PROCEEDINGS

3rd INDONESIA INTERNATIONAL DEFENSE SCIENCE SEMINAR 2019

Jakarta, 8-9 July 2019

INDONESIA DEFENSE UNIVERSITY
Indonesia Peace and Security Center, Sentul, West Java, Indonesia

Volume 5

PROCEEDINGS
3rd INDONESIA INTERNATIONAL DEFENSE SCIENCE 2019

IIDSS 2019

"Enhancing Defense Cooperation to Deal With Terrorism, Cyber Threats and Natural Disaster"

Jakarta, 8 - 9 July 2019

INDONESIA DEFENSE UNIVERSITY
Indonesia Peace and Security Center, Sentul, West Java, Indonesia
Phone: +6221 2961 8757
Fax: +6221 8795 3757
Website: www.idu.ac.id

Volume 5

PROCEEDINGS 3rd INDONESIA INTERNATIONAL DEFENSE SCIENCE SEMINAR

Jakarta, 8-9 July, 2019 **Volume 5st**

Chief Editor : Jonni Mahroza

Editor : Sovian Aritonang, Rudy Agus Gemilang Gultom
Layout : Faishal Irfan
Cover Design : Ahmad Sazrhi
Content : Andoyo Rifky W, Bilqies Kimnilah, Dorothea S. Jasi, Ilham Permadi, Riyadi Juhana, Shinta puspita, Selly Pratiwi

Reviwer :
- Dr. Rodon Pedrason (FSP),
- Dr. Ir Rudy AG Gultom, M.Sc. (FTP)
- Dr. Surya Wiranto, SH., MH. (FSP)
- Nugroho Adi Sasongko, ST., M.Sc., Ph.D. (FMP)
- Dr. Ir. Rudy Laksmono W., MT. (FMP)
- Dr. Ir. Donny Yusgiantoro (FMP)
- Dr. Jonni Mahroza, S.IP., M.Sc.
- Dr. Yusuf, S.Sos., MM. (FSP)
- Dr. Ikhwan Syataria, ST., MM. (FMP)
- Dr. Syaiful Anwar, M.Bus. (FSP)
- Dr. Masita Manessa (FTP)
- Dr. Triyoga Budi Prasetyo, M.Si. (FSP)
- Dr. Agus Adriyanto, ST., MM. (FKN)
- Dr (Can) Drs. Khaerudin, MM. (FTP)
- Dr. Sovian Aritonang, S.Si., M.Si. (FTP)
- Dr. Siswo Hadi Sumantri, S.T., M.MT. (FKN)
- Dr. M. Adnan Madjid, SH, M.Hum. (FKN)
- Dr. IDK Kerta Widana, SKM, MKKK (FKN)
- Romie Oktovianus Bura, B.Eng (Hons)., MRAeS, Ph.D. (FTP)
- Dr (Can). Dani D.A.R., M.Si (Han) (FTP)
- Dr. Djoko Andreas Navalino, S.IP., M.AB (FTP)

Catalogue in Publication: Jonny Mahroza

viii pages + 411 pages + 25 cm x 19 cm
ISBN 978-602-5808-52-4

Phone: +6221 2961 8757
Fax: +6221 8795 3757
Website: www.idu.ac.id

INDONESIA DEFENSE UNIVERSITY
Indonesia Peace and Security Center, Sentul, West Java, Indonesia

TABLE OF CONTENTS

★★★

MINISTRY OF DEFENCE
INDONESIA DEFENSE UNIVERSITY

WELCOMING REMARKS
RECTOR OF INDONESIA DEFENSE UNIVERSITY
LTG DR. TRI LEGIONOSUKO, S.IP., M.AP.
INDONESIA INTERNATIONAL DEFENSE SCIENCE SEMINAR
BOROBUDUR HOTEL, 8 JULY 2019

- Your excelency ambasadors from our friend countries
- Honorable Minister of Defence of Republic Indonesia, General (Retired) Ryamizard Ryacudu
- Honorable commander in chief of TNI or the representing
- Honorable chief of staff of the Indonesian Army or the representing
- Honorable chief of staff of the Indonesian Navy or the representing
- Honorable chief of staff of the Indonesian Airforce or the representing
- Honorable Defense Attaches and defense representataive comunity in Jakarta
- Senior rank officials from the Indonesia Cabinet Ministries, Ministry of Defense and TNI Headquarters, as well as from Army, Naval & Airforce Hq
- Distinguished guest from higher degree and research institutions
- Distinguished speakers and moderators,

Ladies and Gentlemen,

A very good morning to all of you,

It is my pleasure to welcome you to the 2019 Indonesia International Defense Science Seminar which in an or IIDSS 2019, Indonesia Defense University's annual international seminar on defense and security issues.

As an academic institution of defense science, hosting the IIDSS is a part of IDU's contribution to the advancement of both the science and the practice of defense and security. To respond to dynamic strategic environments and challenges, it is paramount for IDU to address these issues, and to help finding the solutions.

Ladies and Gentlemen,

Since the beginning of the 21st century, our region faces several challenges, the old and conventional, as well as new and unpredictable ones. Hence these global issues have generated common interests among countries in the region to anticipate the challeges. These include terrorism, transnational organized crimes, humanitarian crisis, human-made disasters. International community should put their priorities and focus on these real and urgent threats.

Especially, radicalism movement in the southeast asian region as ISIS struggles to have its strong hold in this region, as we could see in Marawi, the Philippines, and a number of attacks lately in Indonesia let me take this opportunity to highlight one specific issue in the contecxt of counter terrorism. One of the most challeging taks for any government now is how to cope with a mindset war, which has been applied by radical-fundamentalism groups. Some studies found that schools and universitie, event government institution, have been very vulnarable to radicalis mindset. At the same time, the rapid development of information technology and social media has changed the way we interact with one another, how we perceive our world. Worse radical-fundamentalism croups also make use of this advance technology to promotion their radical campaigns.

As there is no any government is able to tackle this mindset war alone, all countries have to work together, finding the best strategy to deal with them.

Distinguished guests,

Under such background, this year, the discussions focuses on enhancing defense cooperation to deal with terrorism, cyber, and natural disaster through a number of important defense related topics, such as new conception and strategy in countering terrorism & cyber threats and new ideas and efforts in humanitarian assistance & disaster relief. Furthermore the measures to deal with that have been prepared either domestically in each country and in a frame of bilateral cooperation. Need to be more efective. A particular effort is required among the countries to develop more comprehensive strategies, finding a new applicable concept, management, policy, and new technology innovation in facing these real threats.

The forum is aimed as an academic forum for international practitioners and scholars to discuss selected topics in various security issues and the ways defense cooperation could effectively address them. Prominent speakers, international and domestic, will share their knowledges and views on these topics, elaborating ideas and experiences in which your active participation is also needed.

Understanding the importance of IIDSS, I would like to share the objectives of this academic forum. The objectives of the discussions are:

- ➢ To promote a culture of exchange and share of best practices in policies and strategies, both in terms of soft knowledge and technologies through intellectual engagements in addressing common security challenges.

- ➢ To identify a new development in threats and its anomaly based on country or region.
- ➢ To inspire and encourage policymakers to move more constructively into new or better frameworks of engagements for peace and security.
- ➢ To strengthen the existing international cooperation in common efforts to address global security issues.
- ➢ To contribute with the new ideas and breakthrough to enhance the current cooperation strategy.
- ➢ To identify a possible solution in a specific country with its specific characteristics.

A long with the seminar today, we also conduct "Call For Paper conference tomorrow in IDU main campus in Bogor" that will be presenting a large number of selected papers from experts, and academician as well as students from many universities. You could attend and discuss tomorrow regarding some topics that are related with these seminar's topics.

Distinguished ladies and gentlemen,

Today, we have 1200 Participants, not only from domestic defense and security agencies, but also from National Defense Universities of neighboring countries and defense and security institutes. We are delighted that IIDSS have taken the interest of other countries in the region and beyond.

I hope everyone who attends our forum for the next two days will take part actively in the discussions during the seminar sessions.

And now, it is my honor to formally invite General (Retired) Ryamizard Ryacudu, Minister of Defense of the Republic of Indonesia, to deliver his keynote speech and officially open IIDSS 2019.

Thank you.

Jakarta, 8 July 2019
Rector

LtG. Dr. Tri legionosuko, S.IP., M. AP

Defense Strategy

Defense Management

National Security

Defense Technology

Establishing Regional Security Regime through ASEAN Cooperation in Cybercrime Issue – IIDSS2019

Sereffina Yohanna Elisabeth Siahaan[1]

[1]Master Student of Indonesia Defense University, Sentul, Bogor 16810, Indonesia

E-mail: sereffina.yohanna@gmail.com

Abstract. Cybercrime is non-traditional security issues whose effects to damage all activities by using a computer system. Globally, internet users in ASEAN are the largest with 350 million users in 2018. Losses caused by cybercrime in ASEAN also increase every year. Facing this condition, ASEAN needs to comprehend cyber security and to enhance cooperation thus ASEAN could be able to address common threats. ASEAN has become an institution for all member states to achieve national interests in order to support national security in the cyber field. ASEAN has currently formulated various documents regarding handling cybercrime, but ASEAN has not yet sought concrete agreements that can counter this threat. This paper uses a qualitative method with a descriptive analysis approach. This paper is analyzed by regional security regime theory by approaching on forums and dialogs within ASEAN. This paper aims to provide advice to establish regional security regime through ASEAN in developing cyber cooperation as a new concept of regional collaboration. ASEAN is expected to benefit from maintaining cyber security stability in the region.

1. Introduction

At present the issue of non-traditional security is an important issue because the impact it poses is no less than a threat to traditional security issues. One issue in non-traditional security is cyber threats that are closely related to computer and internet technology. The rapid development of computer and internet technology has created enormous dependence on society. Every activity that is usually supervised by relying on human power is slowly transferred to the computer. Not only that, the internet has simplified human life because all information can be accessed easily only from behind the desk. Dependence on computers and the internet is then disrupted by cyber attacks.

There are 350 million internet users in the Southeast Asia in 2018 and of that number, 150 million of them are from Indonesia, which is referred to as the country with the most number of cyber users in Southeast Asia. Google and Temasek research also found that the use of the Internet through smartphone devices was very large, reaching 90 percent in Southeast Asia. [1] The Hootsuite study found mobile internet users in countries like Indonesia, the Philippines and Malaysia spent 4 hours accessing the internet on mobile devices per day. While mobile internet users in Thailand spend the longest time in Southeast Asia, which is 4 hours 56 minutes per day. [2]

These threats can come from governments, organizations, individuals, or entrepreneurs, whether intentionally or not in order to gain financial, military, political and other purposes. Cyber can be a threat to a country because of its scope that can be used to steal information, disseminate destructive ideas, and attack information systems in various fields in military networks and civil networks such as data theft of companies and agencies. Given the losses that can be caused by cyber attacks, the report of Ponemon Institute in 2018 stated that the average loss due to global data violations this year reached 3.86 million US dollars, an increase of 6.4 percent from 2017. [3]

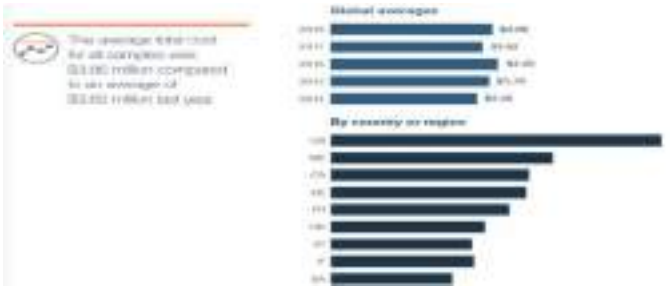


Figure 1. Data Breach Cost (Phenomenon Institute)

The world conditions faced by fourth and fifth generation wars also require different deterrence strategies. If, the concept of the previous generation of war is conventional and involves more physical contact, then the concept of fourth generation war is in communities that are interconnected (networked), cross-country, and information-based. [4] The attacks used vary, both in the form of information interventions through the media and the use of computer viruses that can cause damage to the country's critical infrastructure. In addition, the war of ideas / ideas, the development of opinion through social media can ultimately influence the political, social and cultural conditions of a country as a manifestation of the threat of the fourth generation of war. Without the mastery of cyber space, it is very possible that a country's security and political stability can be disrupted. Therefore, a leader in this generation is demanded not only to master the art of war (traditional) but also technology. [5] Fourth generation war is a new concept that rests on networked, transnational and information based. Tactically, the fourth war involves a combination of international, transnational, national and subnational actors. In contrast to the previous generation of warfare, in this generation of war the state's control of war diminished as it involved non-state actors, so there was no longer a difference between civil and military forces.

Therefore, this paper aims to provide advice for ASEAN to strengthen cooperation in anticipation of this cyberattack. To achieve the above objectives, this paper will explain the complexity of cyber threats in Southeast Asia, analysis of ASEAN cyber cooperation and recommendations and recommendations as conclusions.

2. Cybercrime in Southeast Asia

2.1. Complexity of Cyber Threats in Southeast Asia

In two UN Congress documents cited by Barda Nawawi Arief regarding The Prevention of Crime and Treatment of Offenders in Havana Cuba in 1990 and in Vienna Austria in 2000, two terms related to definition of cybercrime, namely cybercrime and computer related, were explained crime. [6] The cybercrime is divided into two categories, first, cybercrime in a narrow sense is called computer crime, as well as cybercrime in the broad sense which is called computer related breach.

The cybercrime is a type of crime related to the use of an infinite information technology and has strong characteristics with an engineering technology that relies on a high level of security and credibility of information that is delivered and accessed by internet customers. Cybercrime can include things like computer intrusion (hacking) in order to attack property, economic espionage (data theft or confidential transactions, internet extortion, money laundering, identity stealing, and a number of attacks facilitated through the internet) in fact the type continues to grow every day. [7]

Further, cybercrime as mentioned above is not easy to identify, specifically related to the method used, location until the time of occurrence of cybercrime. Internet anonymity, makes cybercrime increasingly rampant with various instruments and forms of crime. In some large cases, cyberattacks that occur not only come from one country or one source. Even cyber attacks, are more often carried out by non-state actors with diverse targets. Unlimited and lawless cyberspace or cyberspace provides various possibilities for how and where attacks originate, so cybercrime is often not handled in an easy and concise way, or only relies on the performance of one actor.

According to the World Threat Assessment 2013 report in the European Commission's proposal of 2.1 billion internet users worldwide, the majority of users are in Asia (922,200,000). Meanwhile, the next most significant area in terms of the number of internet users is Europe with

476,200,000 users. China alone has 485 million internet users - more than other countries or regions (including Europe and the rest from Asia) - and has an internet attack of only 36.3 percent. The growth of ICT in Southeast Asia is actually not too far behind the US, Europe and countries in Northeast Asia such as Japan and the Republic of Korea. [8] According to the ASEAN E Commerce Database Project released in 2010, ASEAN represented 6 percent of Internet users and ASEAN member countries' 20 percent global penetration rate, with Brunei Darussalam, Singapore and Malaysia having the largest share of internet penetration, and Indonesia, the Philippines, and Vietnam has the largest internet user. [9] The Indonesian government even expects companies in ASEAN to potentially risk a loss of US $ 750 billion or Rp.10,000 trillion due to the impact of cyber attacks. [10]

Based on the report of the global consulting company, AT Kearney, ASEAN countries are being used as launchpads in dealing with cyber attacks- either as target for the release of malware attacks. [11] In a cyber-crime operation held by Interpol and investigators from seven countries in Southeast Asia in 2017, it was revealed that nearly 9,000 servers were infected with malware and hundreds of other websites were targeted for attacks in the region. Various types of malware, such as those targeting financial institutions, spreading ransomware, conducting Distributed Denial of Service (DDoS) attacks, and spreading spam, are some of the threats posed by these infected servers. [12] According to a Symantec report entitled Internet Security Threat Report Volume 24 which was released in February 2019, there are 4 ASEAN countries from 10 countries in the world that have presentations on cyber attacks, namely Vietnam, Indonesia, Thailand and Singapore. Vietnam is in the third largest country position after China and India with a 3.54% cyberattack percentage. Cybercrime in the country have increased where in 2017 the number of cyber threats in Vietnam was 2.07%. Indonesia follows next with a percentage of 2.23% cyber attacks in 2018, up from 1.67% a year earlier. Thailand and Singapore sequentially received cyberattack percentages of 1.54% and 0.75%. [13]

2.2 Cyber Security Regimes in ASEAN

According to Krasner, an international regime is an order that contains a collection of principles, norms, rules, decision-making processes, both explicit and implicit, which are related to expectations or expectations of actors, and contain the interests of these actors in International Relations. [14] This study fulfills the need for conceptualization of forces that can enable it to focus on the control of events that are concerned with the problems being faced by international actors. [15] The principle of the international regime is related to the belief in facts, causation, and honesty; norms are standards of behavior that are manifested as rights and obligations; regulation is a clear and specific prohibition on actions taken; while the decision making procedure is a procedure that must be taken in implementing joint choices. Rules, procedures and norms that exist within the regime regulate and become behavioral controls of members of the regime. [16]

Regime is the result of cooperative behavior as an effort to facilitate cooperation. This statement is focusing on the control of events that are concerned with the problems being faced by international actors. The regime can be said is a continuation of the form of cooperation, and encourage better cooperation. The fundamental difference between the regime and the institution is how to view actors in international relations. The regime refers to the influence of behavior generated by international organizations on other actors, especially state actors by focusing on actor expectations. It is different from institutions that look more at what is happening in the organization than to see the influence that international organizations have on other actors. [17] This is especially significant for the Southeast Asia region where ASEAN's centrality in regional architecture has a potential role as a significant "neutral area" in terms of international cyber security cooperation. The ASEAN cyber security regime is a "common" condition formed in Southeast Asia in the face of non-traditional forms of threats that arise in "uncertain" conditions. Regime calculates the results that an actor or State can get in a condition of uncertainty or when there is no specific calculation.

In establishing a security regime in the region, ASEAN needs to make rules, procedures and norms that exist within the regime to regulate and be a behavioral control of members of the regime by strengthening forums and dialogs. ASEAN already forum by ARF (ASEAN Regional Forum) concept to organize interactions among ASEAN member countries in order to combat cybercrime. ARF is different from the concept security cooperation by the North Atlantic Treaty Organizations (NATO) which was formed based on treaty or post-war defense alliance World II. ARF is intended to build taste mutual trust that adopts an approach multilateral to prevent conflicts in the region. ARF is not as identical as NATO with the use of military power, but rather more to dialogue and engagement as a means of preventing conflict. Thus, the concept ARF can be used for major capital in the formation of regional regimes.

In responding to these challenges, since 2001 the issue of cyber security has become one of the agenda of the meeting which resulted in the agreement of AMMTC (ASEAN Ministerial Meeting on Transnational Crime). Member countries in ASEAN agreed to include cybercrime in the working program to be implemented on the ASEAN Plan of Action in order to combat transnational crime.[18] In 2003 at the 9th AMMTC meeting held in Vientiane, Lao PDR, ASEAN Ministers welcomed the new framework of SOMTC Working Group on Cyber Crime which is part of transnational crime (ASEAN Senior Officials Meeting on Transnational Crime). The response from ASEAN is increasingly refined with the ARF Statement on Cooperation in Fighting Cyber Attack and Terrorist Misuse of Cyber Space, in Kuala Lumpur on July 28, 2006, which generally emphasizes the creation of a legal framework (regulation) against cybercrime, encouraging collaboration and collaboration in handling crimes, including cyber terrorism (cyber terrorism), and strengthening increased public awareness in using cyber.

ARF on cybersecurity initiatives was initiated in 2006 through a joint statement at a meeting in Malaysia and reaffirmed at ARF Statement Cooperation in Ensuring Cyber Security, in Phnom Penh, 12th July 2012, as follows: [19]

1. Promoting further consideration of vision and strategies to discuss threats emerging in this field consistent with international law and its basic norms and principles;

2. Promoting forum on confidence building measures (CBM), risk reduction measures and stability to address the implications of ARF external participants' use of ICTs, including exchange of views on the potential use of ICTs in conflict;

3. Encouraging and enhancing partnership in bringing about culture of cyber security in the region;

4. Developing the ARF work plan on security in the use of ICTs, focused on practical collaboration on CBM, which could set out corresponding targets and a timeframe for their implementation;

5. Reviewing a possibility to explain common terms and definitions relevant to the sphere in using ICTs.

The results of the statement was implemented in the form of workshops, seminars, and various training at the level regional. One focus of the workshop that is how a country is inside respond and coordinate when there is something cyber incidents. The discussion includes coordination of national responses, methods of mitigation, how to prosecute perpetrators of crimes between countries, and the perspective on an incident involving actors from other countries and as far as how other countries respond to an incident that emerged from their country.[20]

Since 2003, the Singapore ASEAN Telecommunications and IT Ministers Meeting (TELMIN), and the Telecommunications Senior Officials Meeting (TELSOM) emphasized the efforts to establish an ASEAN Information Infrastructure in order to promote interoperability, inter-connectivity and security integrity. All Ministers of Telecommunications and IT in ASEAN decided that all ASEAN member states need to develop and operationalize the National Computer Emergency Response Team (CERT) in 2005 in accordance with the agreed minimum performance criteria. As the agreement was formed, a virtual forum for ASEAN cyber security is being formed to develop a general framework for coordinating information exchange, establishing standards and collaborating among law enforcement agencies. This effort was enhanced by the establishment of the 2015 ASEAN ICT Masterplan (AIM 2015) which was approved at the 10th TELMIN meeting on 13-14 January 2011 in Kuala Lumpur, Malaysia. AIM 2015 emphasized the development of trust related to cyber security through empowerment and community engagement and infrastructure development efforts with initiatives to promote information security, network integrity, data protection and CERT collaboration.

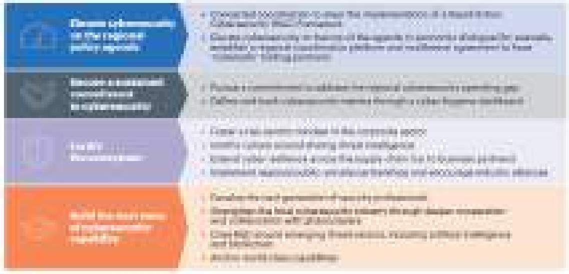
In building a regional security regime, ASEAN must also improve its cyber proactive strategy built on the awareness that cyberspace is a tool that creates economic progress and increases living standards. For example, AMCC in October 2016 has built a discussion platform on cyber issues at the ministerial level to discuss cyber security using a harmonization perspective among stakeholders. The 3rd ASEAN Ministerial Conference on Cybersecurity (AMCC) was convened in 2018, specifically to increase coordination on cybersecurity efforts among various platforms of the three pillars of ASEAN. The AMCC agreed that there is a need for a formal ASEAN cybersecurity mechanism to consider and to decide on inter-related cyber diplomacy, policy and operational issues. It was recommended that the proposed mechanism should be flexible and also take into account multiple dimensions, including economic considerations. [21] ASEAN should strengthen cooperation by enhancing capacity building efforts, thus ASEAN's efforts will be focus, effective, and coordinated holistically on cybercrime issues.

ASEAN should make cybersecurity programs by working together to defend and to take benefit of the region's collective resources. The trust and resilience are the main points for policy makers and non-state actors that should be improved by working together in appearing awareness on cybersecurity and adopting a stance of active defense within ARF and AMCC. Following this is an ASEAN's cybersecurity playbook as a new concept that could be implemented on the upcoming forums:

- Steering the implementation of a Rapid Action Cybersecurity Framework

- Improving cybersecurity issues to the top of the agenda in regional forum within ASEAN framework

Table 1. Regional Cybersecurity Defense Playbook (AT Kearney)



Elevate cybersecurity on the regional policy agenda	[illegible]
[illegible]	[illegible]
[illegible]	[illegible]
Build the next wave of cybersecurity capability	[illegible]

3. Conclusion

The condition of cyber in ASEAN is faced with a dangerous situation. The use of cyberspace has touched various aspects of the nation's life which include social, cultural, economic, politics and security. Internet network penetration in ASEAN continues to expand, even social networking and internet users are one of the largest regions in the world. On the other hand, the trend of cyber threats that increasingly leads to the national interest of a nation is a challenge for each country at the strategic and operational level that has not been fully able to establish a comprehensive cybersecurity system. This unpreparedness of the government in the national scope needs to be addressed by implementing regional collaborative efforts to eliminate or minimize the potential threats. ASEAN needs to use increasing cooperation to become a regional security regime to protect its national security by reducing potential threats and establishing regional stability.

The issue that should be addressed among ASEAN countries is collaboration and information sharing is indeed a vital aspect of cyber security. Without collaboration, cyber security ecosystems are easily compromised. ASEAN must also try to increase capacity through norms, knowledge and information in the field of cybersecurity within ARF, AMCC or other forums. The ASEAN's response to the cybersecurity challenges need to forward-looking, comprehensive, engaging an array of all stakeholders to deal with the cyber threats and support ASEAN's leap into effective platform. ASEAN should use all forums and dialogs such as ARF and AMCC in order to push every stakeholder taking role to play in cybercrime. ASEAN should create security regional regime by building the practices, procedures and processes and establishing military-civil collaboration to address cybercrime issues.

References

[1] Ananda, Rajan. Etc 2018 E-Conomy SEA 2018: Southeast Asia's Internet Economy Hits An Inflection Point. Think with Google. (online), (https://www.thinkwithgoogle.com/intl/en-apac/tools-resources/research-studies/e-conomy-sea-2018-southeast-asias-internet-economy-hits-inflection-point/)

[2] Digital Report. 2018. Global Digital Report 2018 World's Internet Users Pass The 4 Billion Mark. (online), (https://digitalreport.wearesocial.com/)

[3] Ponemon Istitute 2018 Ponemon Institute 2018 Cybersecurity Report. (online), (https://www.gosolis.com/blog/ponemon-institute-2018-cybersecurity-report-information/)

[4] Ali, Alman Helvas 2015 Angkatan Laut dan Peperangan Generasi Keempat. Forum Kajian Pertahanan dan Maritim. (online), (http://www.fkpmaritim.org/angkatan-laut-dan-peperangan generasi-keempat/)

[5] William S. Lind, et all 1989 The Changing Face of War: Into The Fourth Generation. Marine Corps Gazette pp 22

[6] Nawawi Arief, B 2006 Kebijakan Penanggulangan Cyber Crime Dan Cyber Sex. Law Reform, (online), Volume 1(1), pp 24

[7] Govil, Jevish 2007 Ramifications Of Cyber Crime And Suggestive Preventive Measures. (online), (https://www.researchgate.net/publication/4287237_Ramifications_of_cyber_crime_and_suggestive_preventive_measures)

[8] Clapper, JR 2013 Worldwide Threat Assessment. Director of National Intelligence of US Government. (online), (https://www.dni.gov/files/documents/Intelligence%20Reports/UNCLASS_2013%20ATA%20SFR%20FINAL%20for%20SASC%2018%20Apr%202013.pdf)

[9] ASEAN 2015 ASEAN e-Commerce Database Project. (online), (https://id.scribd.com/document/111765095/ASEAN-e-Commerce-Database-Project#)

[10] Ariyanti, Fiki 2018 Serangan Siber Potensi Bikin Rugi Perusahaan ASEAN Capai Rp 10 Ribu T. Liputan 6, (online),

(https://www.liputan6.com/bisnis/read/3337398/serangan-siber-potensi-bikin-rugi-perusahaan-asean-capai-rp-10-ribu-t)

[11] AT. Kearney Report 2018 Cybersecurity in ASEAN: An Urgent Call to Action

[12] Sarkar, Himani and Clarence Fernandez. 2017. Interpol-Led Operation Finds Nearly 9,000 Infected Servers In Southeast Asia. Reuters. (online), (https://www.reuters.com/article/us-singapore-interpol-cyber-idUSKBN17Q1BT)

[13] Symantec 2019 Internet Security Threat Report Volume 24. (online), (https://www.symantec.com/content/dam/symantec/docs/reports/istr-24-2019-en.pdf)

[14] Krasner, Stephan D 1982 Structural Causes and Regime Consequences: Regimes as Intervening Variables. Within: Krasner, Stephan D. [eds.]. International Organization, Vol. 36/2. (New York: Cornell University Press)

[15] Haggard, Stephan and Simmons, Beth A 1987 Theories of International Regimes. Within: International Organization, Vol. 41 (Cambridge: MIT Press)

[16] Keohane, Robert O and Joseph. S Nye 1987 Power and Interdependence. Within: International Organization, Vol. 41 (Cambridge: MIT Press)

[17] Barkin, J.S 2006 International Organization: Theories and Institutions (New York: Palgrave Macmillan)

[18] ASEAN Secretariat 2011 ASEAN ICT Masterplan 2015 (AIM)

[19] ASEAN Regional Forum. 2015. ASEAN Regional Forum on Security of and in The Use of Information and Communications Technologies (ICT's) Cooperation in Ensuring Cyber Security (Phnom Penh: ARF Library) pp 1

[20] Setyawan, David Putra and Sumari, Arwin Datumaya Wahyudi Sumari 2016 Diplomasi Pertahanan Indonesia Dalam Pencapaian Cybersecurity Melalui Asean Regional Forum On Cybersecurity Initiatives (Bogor: Jurnal Penelitian Politik)

[21] Timur, F. G. Cempaka 2017 The Rise of Cyber Diplomacy — ASEAN's Perspective in Cyber Security, KnE Social Sciences. ICoSaPS Conference Proceedings The 3rd International Conference on Social and Political Science The Impact of Information Technology on Social and Political Dynamics, 2016

Indonesia Defense Strategy to Combat Terrorism in ASEAN Region: The Case of Defense Cooperation under ASEAN Defense Ministers' Meeting (ADMM) and ADMM-Plus – IIDSS2019

Aji Widiatmaja[1]

[1] Post Graduate Student in Indonesia Defense University, Sentul Bogor 16810, Indonesia

E-mail: ajiwidiatmaja@gmail.com

Abstract. Terrorism activities in Southeast Asia region possess great threats for Indonesia and other ASEAN members. This situation is worsened by the condition in ASEAN countries that have porous borders, long history of insurgencies, and inequality in defense capability to combat terrorism. Indonesia has long history of terrorism and still deal with the problem today. By understanding phenomena of terrorism that caused by global impact, Indonesia try to enhanced multilateral cooperation in ASEAN region. The establishment of ADMM and ADMM-Plus are used to address such problem multilaterally and comprehensively. It is part of Indonesia Defense Strategy to eliminate terrorism threats from its territory and ASEAN region. Specifically, the strategy in line with Indonesia State Defense Strategy architected by Indonesia Ministry of Defense. The strategy contains ends, means, and ways. It provides guidelines for Indonesia government in joining defense cooperation under ADMM and ADMM-Plus. The result of the research shows that Indonesia success in gain national interests (ends) in combating terrorism supported by strong hard and soft power as the means. Then, the Indonesia government also performed comprehensive application of ways for the strategy. It can be seen from the Indonesia activeness in the forum to guide its national interest.

1. Introduction

Southeast Asia is said as the second front to combat terrorist group activities. This is stated by Smith (1) by seeing the existence of Abu Sayyaf in Philippine and Jemaah Islamiyah (JI) groups in Indonesia that declare wars against state government. The most phenomenal terrorist activity was the first Bali Bombing in Indonesia. This bombing had killed hundreds of people that mostly came from foreign countries. This fact shows that terrorism movement in Southeast Asia region is escalating (p. X). Those terrorism activities done by several terrorist groups that linked to Al-Qaeda. Mokhtar (2) stated that Moro Islamic Liberation Front (MILF) and Jemaah Islamiyah (JI) are the marker of first wave of terrorism in Southeast Asia region. Those groups are responsible for hundreds of casualties and dead victims caused by their bombings.

Today, Southeast Asia region entered the so-called second wave of terrorism. This phenomenon marked by the establishment of Islamic State of Iraq and Syria (ISIS) in 2014. The effect of ISIS came to Southeast Asia and caused serial terrorism activities from 2016 to 2018. This is also can be a marker that terrorism activities in Southeast Asia region is still high. The newest terrorist attack was in Jolo, Filipina. This terrorist attack was done by exploding Catholic Church in January 27, 2019 and caused at least 20 people dead and injured hundreds of people (3). Alkaff and Singh (4) said that ISIS claimed the attack in Jolo, Filipina. This bombing is a clear sign that terrorism still possess great threats for Southeast Asia region. The current condition in Southeast Asia region is in fact worse. The region is known has long history of insurgency, porous border, radical movements, weak regimes, and unequal of defense capability in combat terrorism.

To overcome these problems, a robust and comprehensive cooperation is needed. The ASEAN countries realizes this situation and formed a cooperation platform that specifically address related-defense issues in 2006 namely ASEAN Defense Ministers' Meeting (ADMM). ADMM was formed in Kuala Lumpur by adopting The ASEAN Security Community (ASC) Plan of Action held in the 10th ASEAN Summit. This organization consist of ten ASEAN country members and used as the highest mechanism in ASEAN to discuss about defense and security dialogues (5). In 2010, ADMM broaden its membership by adding eight dialogue countries to strengthen cooperation and capacity building to deal with defense and security problems especially terrorism. Those eight countries are United States, China, Russia, Australia, New Zealand, South Korea, Japan, and India. ADMM specified its cooperation under five issues namely counter-terrorism, disaster relief, peacekeeping operation, humanitarian assistance, military medicine, humanitarian mine action (added in 2013), and cyber security (added in 2016) (6). Each issue has expert working group (EWG) to accelerate the cooperation into real implementation. Indonesia becomes a prominent figure in ADMM and ADMM-Plus. The long history and experiences in combating terrorism since the beginning of its independence makes Indonesia be a natural leader in terms of counter-terrorism cooperation in the region. The former Indonesia Defense Minister, Purnomo Yusgiantoro, stated that Indonesia is a "Big Brother" for other ASEAN countries. This makes insights and inputs from Indonesia are always considered and mostly applied as mechanism (7).

Regarding terrorism phenomena, Indonesia still possess great challenges and threats by looking terrorism activities in its territory. Indonesian Chief of Police *(Kapolri)* Tito Karnavian argued that in 2017-2018 there were at least 39 terrorism activities in Indonesia. By 2018 alone, there were 396 terrorists have been captured by Indonesian Police (8). Indonesia government realize that terrorism is not merely a domestic phenomenon, rather it is an international related. For that reason, Indonesia is very active in regional mechanism in combating terrorism. It can be seen in Indonesia role in ADMM and ADMM-Plus expert working group on counter-terrorism (EWG-CT). Indonesia national interest in ADMM and ADMM-Plus are to develop its defense capabilities in combating terrorism by engaging with other ADMM-Plus members. Also, Indonesia plans to secure the region and its territory from terrorism threats by increasing defense cooperation under ADMM and ADMM-Plus. Moreover, confidence building measure (CBM) can grows among the members through defense cooperation. Indonesia applied its defense strategy to gain national interests in terms of counter-terrorism. The strategy contains three elements namely ends, ways, and means.

2. Discussion

2.1 Indonesia State Defense Strategy

It is important to look back on history by remembering Carl Von Clausewittz, a prominent figure in strategy making. In his book *On War*, he stated that (9) strategy is about the engagement for the purpose of war by focusing the use of power to engage and reach goals. Strategy provides purposes and other elements to support the effort in reaching goals. Also, strategy can do planning to connect all aspects (means) and use it optimally (p. 133). In 2015, Indonesia Ministry of Defense produced Defense White Paper (10) that contains its defense strategy to comprehensively responses all aspects of the dynamics in strategic environment including terrorism threats. Indonesia State Defense Strategy focuses on Global Maritime Fulcrum policy under Joko Widodo presidency. The strategy contains three main elements namely purposes to reach national interest (ends), defense resources (means), and how to use the resources to reach strategic purposes (ways) (p.51-53).

These elements of strategy are very important as guidelines for Indonesia in joining ADMM and ADMM-Plus to enhance its defense capabilities and combat terrorism in the region. Moreover, Indonesia has strong modalities to apply the strategy since Indonesia has experiences, defense infrastructure, and strong multilateral diplomacy. It makes Indonesia becomes a key figure in counter-terrorism cooperation under ADMM and ADMM-Plus. However, even Indonesia has key roles, ASEAN mechanism still need long process of dialogues and consensus mechanism in decision making process. This fact can be advantages or obstacle for its members. The advantages are that consensus mechanism guarantee that every interest from the country members are being considered. The decision-making process involve all the members so that there will be no domination from one country to another. However, the long process of discussion to find consensus sometimes make certain country impatient and act unilaterally by abandoning ASEAN mechanism. These are the classic problems of ASEAN since in the beginning its establishment.

Indonesia, and other ASEAN countries, have succeed in maintaining the organizations for more than fifty years since its establishment in 1967. Archarya and Alastair (11) state that ASEAN is a product from what so-called New Regionalism. This type of regionalism has several markers such as multi polarity in global power, the decrease of United States of America hegemony, the erosion of state system, interdependence, and globalization (p. 9). This type of regionalism also gives power to non-state actor to become a major player in shaping global politics. One of the influential non-state actors is terrorist groups. Their movements are accelerated after the end of Cold War and spread around the world by globalizations. The development of technology also gives big contributions in dissemination of radical ideology around the globe. The prominent examples for the phenomena are Al-Qaeda, Abu Sayyaf Group, Moro Islamic Liberation Front (MILF), Islamic State of Iraq and Syria (ISIS), and Jemaah Islamiyah (JI).

2.2 Element of ends in Indonesia State Defense Strategy

According to Indonesia State Defense Strategy (12), there are several purposes (ends) such as protecting state sovereignty, protecting the unity of Indonesia territory, and protecting the life of the state. Then, those purposes are implemented in five strategic targets, such as:

- Constructing state defense that can eliminate threats
- Constructing state defense that can protect security of maritime, land, and air territory.
- Constructing state defense that contribute to make world peace based on free and active politics.
- Constructing strong, independent, and competitive defense industry
- Constructing *bela negara* awareness from Indonesia people (p.54).

To be specific in ADMM and ADMM-Plus, Indonesia defense strategy is applied well. It has fulfilled the element of ends like constructing defense security to eliminate terrorism threats, protecting is maritime territory, and contribute to make world peace by joining multilateral defense cooperation. Indonesia join ADMM and ADMM-Plus to reach its national interest by maintaining dialogue partners and developing defense capabilities. Indonesia is very active in ADMM and ADMM-Plus since it can contribute to eliminate threats to defense and security in the region. A former Director General of Defense Strategy from Indonesia Ministry of Defense, Lt Gen. (Ret) Yoedhi Swastanto (13), said that the forming of ADMM-Plus was to strengthen ASEAN defense cooperation to maintain regional stability. Also, this cooperation can develop its country members defense capabilities in handling defense and security threats especially terrorism. He added that Indonesia interest is to eliminate terrorism threats in its region. To reach these goals, Indonesia made common perception about terrorism threats that it is a common enemy. For that reason, a robust international cooperation is needed. Purnomo Yusgiantoro, the former Indonesia Defense Minister, also stated that Indonesia National Interest *(Kepentingan Nasional)* is to make sure that Indonesia sovereignty and unity are safe from terrorism threats (14).

Another statement is also conveyed by Head of Security Sub Directorate of ASEAN Politics and Security Cooperation of Indonesia Ministry of Foreign Affairs, Ingen Malem (15). She stated that Indonesia purposes in ADMM-Plus EWG-CT are to enhance its defense capabilities and interoperability among the country members. It is because ADMM-Plus contains several developed countries that can share knowledge, best practices, and joint training to develop Indonesia defense capabilities in combating terrorism. ADMM and ADMM-Plus forums are very important for Indonesia since it can directly contribute in creating zone of peace and stability in Southeast Asia region. It is also in line with the element of ends from Indonesia Defense Strategy. However, in ADMM and ADMM-Plus defense cooperation, issues of defense industry and *bela negara* are still minor comparing other issues such as terrorism, human rights, and maritime security. In the future ADMM and ADMM-Plus cooperation, it is important for Indonesia to enhance defense industry and *bela negara* dialogues and cooperation to complete the five strategic targets of Indonesia Defense Strategy.

2.3. Element of means in Indonesia State Defense Strategy

In this element, Indonesia Defense Strategy employs military and non-military defense. In counter-terrorism cooperation under ADMM and ADMM-Plus, Indonesia has strong modalities. For that reason, Indonesia can be said as a key figure by looking its experiences, defense infrastructures, and defense capabilities. Yerger (16) stated that there are two categories in means that are tangible and intangible. Tangible can be seen from defense forces, military personnel, equipment, and money. In the other hand, intangible assets can be seen from courage, spirit, and intellect (69-70). It is can be said that Indonesia mostly has those both tangible and intangible assets. Those assets will very helpful for Indonesia to reach its national interest which in this context is eliminating terrorism threats. Specifically, in Indonesia State Defense Strategy (17), defense resources (means) transform to element of national power consist of military and non-military defense power. The elements of military defense consist of main component (Tentara Nasional Indonesia), reserve component, and supporting component. In the other hand, non-military defense consists of main element (ministry/institution) and other element of national power (p.107-109).

The former Director of International Cooperation from Indonesia Ministry of Defense, Maj. Gen (Ret) Syaiful Anwar, stated that Indonesia has strong modalities in terms of hard and soft power. For hard power, Indonesia has several special units in its military such as *Komando Pasukan Khusus* (Kopassus), *Detasemen Jala Mangkara* (Denjaka), dan *Detasemen Bravo* 90 (Denbravo 90). Moreover, Indonesia has long experience (soft power) in dealing with terrorism activities and want to share the experiences to develop defense capabilities of ADMM and ADMM-Plus country members (18). In fact, Indonesia have been dealing with terrorism since in the beginning of the country Independence Day. Ltc. Ikwan Achmadi, Chief of Peace Mission Section in Indonesia Ministry of Defense said that Indonesia has resourceful experiences in dealing with terrorism. He added that Indonesia had deal with Darul Islam/Tentara Islam Indonesia (DI/TII), Gerakan Aceh Merdeka (GAM), and the most phenomenal action was in 1981 in Woyla Operation. From these experiences, Indonesia becomes a role model in combating terrorism since Indonesia has strong modalities (19).

By looking the means, Indonesia has strong modalities consist of both hard and soft power. As mentioned above that element of hard power can be seen from the Indonesia special units and military equipments in dealing with terrorism. In the other hand, soft power means can be seen from the non-military aspects such as experiences in counter-terrorism operation, organization maturity, institution structure, and diplomacy competency. These modalities can enhance Indonesia position in defense cooperation under ADMM and ADMM-Plus so its national interest can be fulfilled. Indonesia successfully integrate its military and non-military means in constructing defense strategy. It is applied in defense cooperation under ADMM and ADMM-Plus. Moreover, Indonesia activeness in the defense cooperation, can build positive image as confidence building measure (CBM). The application of the means in ADMM and ADMM-Plus contribute to reach Indonesia national interest (ends).

2.4. *Element of ways in Indonesia State Defense Strategy*

For this element, Indonesia strategy is based on its State Defense Strategy which consist of total defense, defensive-active defense, and multilayer defense. Those items provide guidelines for constituting ways in reaching national interest. The guidelines, according to State Defense Strategy (20), are employing all citizens, territory, and defense resources. Then, strengthen cooperation and diplomacy through active-independent politics by integrating military and non-military resources (p. 51-53). Yerger (20) stated that element of ways in strategy are very important since it will provide platform to employ national power and give role for defense resources to move in terms of when, how, and what aspect. This will give guidelines for means to be employed and reach national interest (ends) (p.1-5). To implement strategy well needs remarkable implementation of means and ways. In counter-terrorism cooperation under ADMM and ADMM-Plus, Indonesia join several activities and agendas as the way Indonesia reach its national interest. Those agendas divided into table top exercise (TTX) and field exercise. TTX agendas are implemented into workshop, seminar, meetings, conferences, and discussion forums. In the other hand, field exercise is done in joint training that employed strategic level, technical level, and operational level. The highest level of meeting in ADMM and ADMM-Plus will be attended by defense ministers from each country members and usually followed by joint statement.

In that agenda, Indonesia is very active and often became speaker to give best practices and experiences regarding counter-terrorism activities. Indonesia also uses the defense cooperation under ADMM and ADMM-Plus to develop its defense capabilities. Indonesia try to protect its territory from terrorism also can be seen through the establishment of Trilateral Maritime Patrol in Sulu Sea. This cooperation established in 2017 consist of Indonesia, Malaysia, and Filipina. The cooperation is used to address the escalation of terrorism and piracy activities in Sulu Sea. Sulu Sea is a porous border and has high terrorism, kidnaping, piracy, and other maritime crime activities. In 2016, Abu Sayyaf group hijacked three Indonesia ship and one Malaysia ship and arrest about eighteen hostages (22). After the Trilateral Maritime Patrol in 2017, the crime in Sulu Sea decrease significantly. Storey (23) in his research said that the joint patrol has significantly decrease the crime activities in Sulu Sea. He added that in 2016 there were ten cases recorded. However in 2017 there were only three cases and only one case in 2018.

Trilateral Maritime Cooperation then followed by establishment of Trilateral Air Patrol in October 2017. This establishment is to strengthen the cooperation and comprehensively address defense and security threats in Sulu Sea. Col. Oktaheroe Ramsi, Chief of Sub Directorate of Multilateral Cooperation of Indonesia Ministry of Defense (24) stated that Trilateral Maritime Patrol is to overcome security threats in Sulu Sea such as piracy, kidnapping, and terrorism activity. The cooperation also in line with Indonesia Global Maritime Fulcrum policy and with national interest to secure maritime, air, and land territory. Indonesia leadership also can be seen when coordinator with United States in EWG-CT became from 2011-2013. In the end of Indonesia and United States administration, a huge multilateral field exercise in counter-terrorism was held in Sentul, Indonesia. This cooperation involving hundreds of participants from ADMM-Plus country members both military and non-military personnel. The field exercise was used by Indonesia to build confidence building measure (CBM), develop its defense capabilities in counter-terrorism, and to send message for terrorist groups that ASEAN has a platform to combat their activities

3. Conclusion

The implementation of Indonesia State Defense Strategy in defense cooperation under ADMM and ADMM-Plus is supported by clear national interest (ends), strong modalities (means), and comprehensive ways. Indonesia has common and specific purposes in its national interest. The common purposes in joining ADMM and ADMM-Plus are to build confidence building measure (CBM), capacity building in combating terrorism, and maintain multilateral dialogues to avoid conflicts. In the other hand, Indonesia specific purposes are to maintain national sovereignty and maintain national unity by eliminating terrorism activities in its territory. Those common and specific purposes are in line with State Defense Strategy.

Indonesia modalities to reach its national interest in counter-terrorism are supported by hard and soft power. The hard power comes from Indonesia military, defense infrastructure, defense institutions, and military employment around Indonesia territory. Then, the soft power comes from Indonesia long experiences in combating terrorism since in the beginning of its Independence Day, maturity of defense organizations, and diplomacy competency. Those modalities make Indonesia as a key player in defense cooperation to combat terrorism in ASEAN. Moreover, those modalities are very helpful to gain Indonesia national interest in eliminating terrorism threats.

The last element of strategy, ways, also well implemented by Indonesia government. The activeness of Indonesia in ADMM and ADMM-Plus forum enhance its bargaining position to insert its national interest be discussed in the forum. Indonesia centrality also can be seen from the first period of coordinator with United States in Expert Working Group on Counter-Terrorism (EWG-CT) in 2011-2013. By seeing ends, means, and ways from Indonesia defense strategy in ADMM and ADMM-Plus, Indonesia strategy in combating terrorism is accomplished.

Acknowledgements

I would like to thank Indonesia Ministry of Defense and Indonesia Ministry of Foreign Affairs to allow me collect the data by interviewing its several ministry officials. The officials were Col. Oktaheroe Ramsi (Chief of Sub Directorate of Multilateral Cooperation of Indonesia Ministry of Defense), Ltc. Ikwan Achmadi (Chief of Peace Mission Section in Indonesia Ministry of Defense), and Ingan Malem (Head of Security Sub Directorate of ASEAN Politics and Security Cooperation of Indonesia Ministry of Foreign Affairs). They gave me comprehensive explanation related to Indonesia roles in ADMM and ADMM-Plus especially in counter-terrorism cooperation. Then, I would like to thank Indonesia Defense University that gave me a permit letter to do research in those two ministries. Also, I would like to thank Mr. Purnomo Yusgiantoro, and Lt. Gen. (Ret) Yoedhi Swastanto as Indonesia Defense University Lecturer and former high rank official in Indonesia Ministry of Defense who gave me deep understanding and facts about ADMM and ADMM-Plus. The last but not least, I would thank to Maj. Gen. (Ret) Syaiful Anwar and Aris Arif Mundayat, Ph.D as my supervisors for this research. They directed me and gave comprehensive understanding in collecting, processing, organizing, and writing the data and finishing the research.

References

[1] Smith, Paul. J 2015 *Terrorism and Violence in Southeast Asia: Transnational Challenges to States and Regional Stability* (New York: Routledge)

[2] Mokhtar, Faris. *The Big Read: Battered in the Middle East, IS eyes Southeast Asia as next terrorism hotspot*. Channel NewsAsia. Available from: https://www.channelnewsasia.com/news/asia/islamic-state-terrorism-extremism-eyes-southeast-asia-11199586 [Accessed 9th March 2019].

[3] Associated Press. *20 Dead After Bombing of Cathedral in Southern Philippines*. The Diplomat. Available from: https://thediplomat.com/2019/01/20-dead-after-bombing-of-cathedral-in-southern-philippines/ [Accessed 9th March 2019].

[4] Alkaff, Syed H, and Singh, Jasminder 2019 2019 Jolo Bombing: Bid to Derail BOL Peace Deal? *RSIS Commentary* No. 025

[5] ADMM. *About the ASEAN Defence Ministers' Meeting (ADMM)*. Monday, 06 February 2017 22:26. Available from: https://admm.asean.org/index.php/about-admm/about-admm.html [Accessed 9th March 2019].

[6] ADMM. *About the ASEAN Defence Ministers' Meeting Plus (ADMM-Plus)*. Monday, 06 February 2017 12:00. Available from: https://admm.asean.org/index.php/about-admm/about-admm-plus.html [Accessed 9th 2019].

[7] Yusgiantoro, Purnomo. Former Indonesia Defense Minister. Personal Communication. 3rd September 2018.

[8] Jurnaliston, Reza. *Kapolri Sebut Terorisme Masih Menjadi Ancaman di Tahun 2019*. Kompas.com - 27/12/2018, 17:39 WIB. Available from: https://nasional.kompas.com/read/2018/12/27/17392661/kapolri-sebut-terorisme-masih-menjadi-ancaman-di-tahun-2019 [Accessed 9th March 2019].

[9] Clausewitz, Carl Von 2007 *On War: Translated by Michael Howard and Peter Paret* (Oxford: Oxford University Press)

[10] Kementerian Pertahanan Republik Indonesia 2015 *Strategi Pertahanan Negara 2015* (Jakarta: Kemhan RI)

[11] Archarya, Amitav, and, L. J, Alastair 2007 *Crafting Cooperation: Regional International Institution in Comparative Perspective* (Cambridge: Cambridge University Press)

[12] Kementerian Pertahanan Republik Indonesia 2015 *Strategi Pertahanan Negara 2015* (Jakarta: Kemhan RI)

[13] Swastanto, Yoedhi. Former Director General Defense Strategy of Indonesia Ministry of Defense. Personal Communication. 7th September 2018.

[14] Yusgiantoro, Purnomo. Former Indonesia Defense Minister. Personal Communication. 3rd September 2018.

[15] Malem, Ingen. Head of Security Sub directorate of ASEAN Politics and Security Cooperation of Indonesia Ministry of Foreign Affairs. Personal Communication. 21st September 2018.

[16] Yerger, Harry R 2006 *Strategic Theory for the 21st Century: The Little Book on Big Strategy* (United States: United States Government)

[17] Kementerian Pertahanan Republik Indonesia 2015 *Strategi Pertahanan Negara 2015* (Jakarta: Kemhan RI)

[18] Anwar, Syaiful. The former Director of Foreign Cooperation from Indonesia Ministry of Defense. Personal Communication 7th September 2018.

[19] Achmadi, Ikwan. Chief of Peace Mission in Indonesia Ministry of Defense. Personal Communication 30th Agustus 2018.

[20] Kementerian Pertahanan Republik Indonesia 2015 *Strategi Pertahanan Negara 2015* (Jakarta: Kemhan RI)

[21] Yerger, Harry R 2006 *Strategic Theory for the 21st Century: The Little Book on Big Strategy* (United States: United States Government)

[22] Abuza, Zachary. *Trilateral Maritime Patrols in the Sulu Sea: Asymmetry in Need, Capability, and Political Will*. Zurich: International Maritime Security (CIMSEC), 2016

[23] Storey, Ian 2018 *Trilateral Security Cooperation in the Sulu-Celebes Seas: A Work in Progress*. (Singapore: ISEAS -Yusof Ishak Institute)

[24] Ramsi, Oktaheroe. , Chief of Sub Directorate Multilateral Cooperation of Indonesia Ministry of Defense. Personal Communication 20th September 2018.

Semesta Cyber Security System Concept: Method to Prevent Data Privacy Violation of Indonesian e-Commerce Customers – IIDSS2019

[1]Adhit Prayoga and [2]Reno Saputro Yandrat

[1]University of Riau, Mutiara Panam Residence H10, Pekanbaru 28293, Indonesia
[2]Center of Energy Security Studies, Puri Park View Apartment AC/10/09, West Jakarta 11620, Indonesia

E-mail: adhit.prayoga@outlook.com; reyszha@gmail.com

Abstract. The aim of this paper is to invent a new conception in dealing with cyber threats, especially towards the hacking activities against e-Commerce customer's personal data in Indonesia by using phishing, malware, botnet, etc. This concept requires cooperation between the government and the private sectors to collect, analyse, disseminate alerts and incident reports, thus cyber security can be guarded more effectively and comprehensively by the Cyber and National Encryption Agency (BSSN) as its national focal point. By using descriptive qualitative research method which the research data was obtained through literature review, this paper invents a new conception which is Semesta Cyber Security Concept. the focus of this concept is increasing the efficiency of BSSN by intensifying its function not only as a formal body which protects the cyber security of the country, but also as an Information Sharing and Analysis Centre (ISAC) to share an indicator of threats, vulnerabilities and cyber incident information to counteract and recover from cyber-attacks. ISAC applies Cyber Threat Intelligence (CTI), Automated Indicator Sharing (AIS), Trusted Automated eXchange of Intelligence Information (TAXII) and Structured Threat Information Expresion (STIX) that will rapidly exchange the indicators in machine speed, thus e-Commerce will be able to minimize the threats.

2.2. Introduction

2.1. Cyber Security in Indonesia

Along with the times, the world has entered the process of globalization in all dimensions of social life. Globalization has removed the limits of human movement by continuously maximizing the use of technology to support the communication and information exchange process. Up to now, globalization has been in the phase of the Industrial Revolution 4.0 which is characterized by the existence of an integrated network system using fibre technology that affects economic activity, from the production process to finally being accepted by consumers. Industrial Revolution 4.0 is a process where the internet of thing becomes a stimulus for economic development which directly increases the effectiveness of actions and connectivity between people in the field of trade. The Industrial Revolution 4.0 has caused a change in the trading system which was initially in the form of barter activities, traditional markets and modern markets, becoming digital markets (e-Commerce).

Indonesia is one of the countries that has been affected by the advancement of technology and information, this is marked by the increase of Indonesian internet users which reached 158,529,932 people in 2018 and become one of the fastest growing internet users in Asia [1]. Through these massive internet users, e-Commerce is a sector that is in demand by the community because of its unlimited reach with high efficiency. Indonesia's e-Commerce transactions are the largest in Southeast Asia, estimated at US $ 5.6 billion in 2016 [2] and in 2018 reaching US $ 12.2 billion [table 1]. This indicates that consumers in Indonesia changed their conventional way of buying stuffs into e-commerce. By the convenience offered, it does not mean that E-Commerce have no weaknesses in its system. Transactions involving individuals and e-Commerce will be able to trigger illegal actions such as the hacking of customer data which leads to the violation of data privacy.

Table 1. Internet Users and e-Commerce Transaction in Indonesia between 2015 - 2018

Information	Year			
	2015	2016	2017	2018
Population (million)	255,01	258,43	261,89	265,40
Internet Users (%)	43%	51%	54,7%	59,73%
Internet Users (million pop)	109,65	131,8	143,25	158,53
e-Commerce Transaction (million $)	1.800	5.600	10.900	12.200

The Government of the Republic of Indonesia has formed a series of policy to prevent and overcome problems that arise on the internet. Indonesia already issued Law No 11 of 2008 concerning about Information and Electronic Transactions [3] and Law No. 19 of 2016 regarding to the Amendments of Law No. 11 of 2008 concerning about Information and Electronic Transactions [4] carried out based on the principle of legal certainty and faith that interception actions on other people's information is a matter that violates the existing law.

In order to strengthen the existence of the law, President Joko Widodo signed Presidential Regulation No. 53 of 2017 regarding to the Cyber and National Encryption Agency (BSSN) which was subsequently refined through Presidential Regulation Number 133 of 2017 concerning the amendment to Presidential Regulation Number 53 of

2017 on December 16, 2017 [6]. BSSN was officially formed to effectively protect cyber security by compiling, implementing and evaluating technical policies in the areas of identification, detection, protection, countermeasures, recovery, monitoring, e-commerce protection control, coding, screening, cyber diplomacy, cyber crisis management center, cyber contact center , information centers, mitigation support, recovery of vulnerability countermeasures, incidents and / or cyber-attacks [5].

The implementation of the law and the Presidential Regulation was in fact still not effective because the violations of law in the internet domain still occur. The case that happened to Bukalapak by Gnosticplayer in the beginning of 2019 exposed the complexity of bringing cases of data theft to the realm of Indonesian law. According to the Acting Head of Public Relations Bureau of the Ministry of Communication and Information Technology of the Republic of Indonesia, Ferdinandus Setu, Indonesia still does not have a law that can penalize the perpetrators of personal data theft. The existing laws are still not effectively regulated hacking cases in detail [3] [4].

2.2. Data Theft Cases in Indonesia

In general, the industrial revolution 4.0 with all the conveniences it offers to the trade sector leads to the growth of Indonesian e-commerce and become the fastest in Southeast Asia with fantastic transaction value. But this also raises the vulnerability to cyber-attack actions, ranging from data theft to carding. This action is carried out in various ways, such as phishing, malware, and skimming.

In 2016, the Indonesian raid hailing unicorn, Go-Jek, experienced hacking on the server section that brought customers to the driver. The stolen data contains customer information ranging from name, email address, password, telephone number, credit card number to its e-wallet service (Go-Pay). Stolen data, especially accounts that have a large amount of Go-Pay balance then sold through sales forums on social media like Facebook [7]. Some of the most massive cases of cyber-attack in Indonesia are phishing [8], carding [9] and skimming [10] which are not only targeting Indonesian people but also tourists who are on vacation in Indonesia. The resulting losses reached hundreds of millions rupiahs, even exceeding that number, considering this case as an iceberg phenomenon.

2.3. Authorities' response on data theft cases in Indonesia

Reflecting on cyber threats that have emerged, several state institutions in Indonesia have created their personal cyber protection agencies until the BSSN was formed in 2017 as a national focal point. In addition, the government through the Ministry of Communication and Information Technology has also made security efforts from cyber-attacks, one of which is "Born to Protect" program [11]. "Born to Protect" program aims to select and train 100 talents from the younger generation each year in order to encounter cyber threats. The government stated that alumnae of this program would help both the government and the private sector in counteracting cyber threats. However, it is not explained in detail whether alumnae of this program are released to be independent or absorbed into the BSSN.

The BSSN itself plans to create a cyber-attack prevention program called Government Computer

Security Incident Response Team (GCSIRT) [12]. But this GCSIRT only focuses on the uniformity and recovery of every government agency and state institution in the center and district area from cyber-attacks. This program is the government's response to cyber-attacks on state institutions which are dominated by web defacement attacks, phishing, and spam and few are brute force attacks or malware. It is unfortunate that the government is still focusing on security on the internal side of the government, even though the problems that afflict the private sector especially e-Commerce also indirectly affect national growth and state revenues.

2.3. Information Sharing

Generally speaking, in order to overcome existing problems and simultaneously create a more reliable cyber security ecosystem for the private sector, collaboration between government agencies and the private sector, especially the e-commerce sector, is needed through the Cyber Threat Intelligence (CTI) and Information Sharing and Analysis systems Center (ISAC). This collaboration is believed to encourage the understanding that cyber security is a shared responsibility so that the handling of cyber illegal actions is not only carried out by the private sector which is attacked, but also the responsibility of the state for the greater good.

3.1. Information Sharing and Analysis Center (ISAC)

ISAC is a third-party entity that functions as an aggregator for the exchange of threat intelligence, vulnerabilities and cyber incidents between each of its partners while maintaining the anonymity of each partner. [13] ISAC main objective is aggregating important information which is accurate, actionable, and relevant to the most comprehensive range of ISAC partners then share the information to all partners. [14] In general, ISAC has the following functions:

- Provide the ability to operate safely in full capacity 24/7 to each partner
- Aggregate indicators and cyber threat intelligence; analyze; and then disseminate threat indicators, warnings, appeals, notifications, and vulnerability assessments to each ISAC partner
- Provide the ability to exchange trusted cyber threat intelligence in machine-speed electronically, and
- Provide a quick response in the event of an emergency through the ability to effectively contact and coordinate with each partner

ISAC can also function as a main secure communication channel in terms of cyber threat intelligence, supporting the dissemination of information between partners and state institutions.

3.2. Cyber Threat Intelligence (CTI)

Cyber Threat Intelligence is intelligence-based threats related to computers, networks and information technology where intelligence is not only in the form of data, but also information and indicators that have been analyzed and actionable. Indicators of attacks such as IP addresses, domain names, and also file hashes are often the focus of the CTI because they are easily actionable [15]. CTI specifically has varied uses, but in general it can be divided into several categories such as the following [16]:

- Proactively stopping, neutralizing, nullifying malware, ransomware and advanced threats;

- Enhancing detection capabilities;
- Threat modeling;
- Prioritizing security incidents and their responses;
- Detecting phishing emails, desktop related targeting and end user application compromise;
- Reusing data for the awareness of security staff.

CTI can provide useful information about emerging or existing threats so that the appropriate response can be taken as defense measure [17]. Network security is no longer adequate to detect and protect from the ever-changing cyber-attack. Intelligence capabilities allow the CTI to identify potential threats and vulnerabilities in order to minimize the threat attack window and limit the amount of time an attacker can gain to access the network before they can be discovered. Through threat intelligence, CTI can make better decisions on how to respond to future threats based on contextual information about the attacks such as the techniques, the tactics, the patterns, the indicators, the actors and also the locations.

CTI can develop depending on the variety of data feed that has been aggregated and analyzed, because conjoined data can provide in-depth insight into attack trends. CTI tries to provide solutions to the following questions, "Who is attacking us?", "Why is there an attack?", "What are they attacking?" "How are they attacking?" and "How can the attack be stopped?". CTI strives not only to comprehend network operations and activities but also the actor, the reason and the aftermath [17]. One of the biggest challenges in adopting CTI is the lack of the ability to integrate into existing systems or build new systems; lack of funds; and lack of competent human resources to be able to run CTI reliably [16].

3.3. Automated Indicator Sharing (AIS)

Automated Indicator Sharing is the aptitude to be able to exchange cyber threat indicators and intelligence between government agencies and the private sector in the broadest range in machine-speed automatically [18]. Threat indicators are pieces of information such as dangerous IP addresses, phishing email addresses, malware, and ransomware. In addition to threat indicators, AIS can also be used as a way to exchange vulnerability; threat attack window; and intelligence about threat indicators counter-measures [13]. Cyber threat indicators are facts that have been identified plus hypotheses about threats. Defensive measure is an effort that is applied to an intelligence system that detects, prevents or mitigates existing and emerging cyber threats and vulnerability.

Partners who share indicators through AIS will not be identified as the source of the indicator to other participants unless they agree to disclose their identity. In other words, they will remain anonymous unless they want their identity to be published [18]. AIS uses industry-standard machine-to-machine communication form such as STIX and TAXII. STIX and TAXII are standards developed in an effort to improve the prevention and mitigation of cyber-attacks. STIX describe threat information securely while TAXII determines how the information is exchanged. STIX and TAXII are machine-readable; therefore they are very easy to be automated. There are three main keys to AIS, namely [13]:

- The purpose of AIS is to share cyber threat indicators machine-readable and defensive measures in machine-speed quickly and broadly;
- Has the ability to automatically receive, process and share indicators;

- AIS is about volume and velocity in sharing indicators automatically, not through human intervention.

In general, the workflow of AIS system is as follows [13]:

- Partners format or encrypt indicators of cyber threats into STIX and then send them via TAXII to the trusted cyber authority institutions e.g. DHS, BSSN, Fireeye, etc;
- Built in program in the server reviews submitted indicators to be validated, anonymized, ensured data privacy and then enrich them through analyst-enrichment process;
- Indicators that need further review are then sent to analysts;
- Finally, validated indicators are sent back to all parties connected to the main server of the cyber authority.

***2.3.1. Structured Threat Information Expression (STIX)* is a standardized language developed by MITER and the OASIS CTI Technical Committee to describe cyber threat intelligence. STIX has been adopted as an international standard by many communities and organizations of cyber security intelligence. STIX is designed to be exchanged through a safe channel from TAXII, but can also be exchanged through other means. STIX is structured in such ways so that users can understand and respond the threat in full manners, from the motivation, the ability, the potential damage and the response [13].**

***2.3.2. Trusted Automated eXchange of Intelligence Information (TAXII)* is a transportation mechanism to share cyber intelligence. TAXII is specifically designed to support STIX format information [13].**

2.4. The Implementation of Semesta Cyber Defense System

In practice, the CTI and ISAC systems can be implemented nationally into the BSSN as the main operator. The e-commerce sector specifically joins the Semesta cyber defense system partner voluntarily with the guarantee of the confidentiality of the data and the sender. Workflow of the Semesta cyber defense system [Figure1] begins with the submission of cyber threat indicators automatically by AIS in order to ensure speed of delivery, optimal range, minimum human error and sender confidentiality. Threat indicators are first converted into STIX Language format then forwarded via TAXII server to ISAC. The submitted indicators then enter the automated process, e.g. filtration and validation; anonymizing data sources; guarantee the confidentiality of data; and forward indicators that require further review to the analyst section.

In the Analyst enrichment process, the indicators that have been entered are then analyzed thoroughly by the analyst team from ISAC. The process of analyzing indicators also be done by leveraging threat intelligence from external sources which obtained by the CTI. The analysis-enriched results are then distributed back to all ISAC partners and also send to the CTI for further analysis. CTI analyzes the indicators sent by ISAC and then looks for the threat attack window that has been used to carry out the attack. Next by utilizing that intelligence, CTI develops the defense measures.

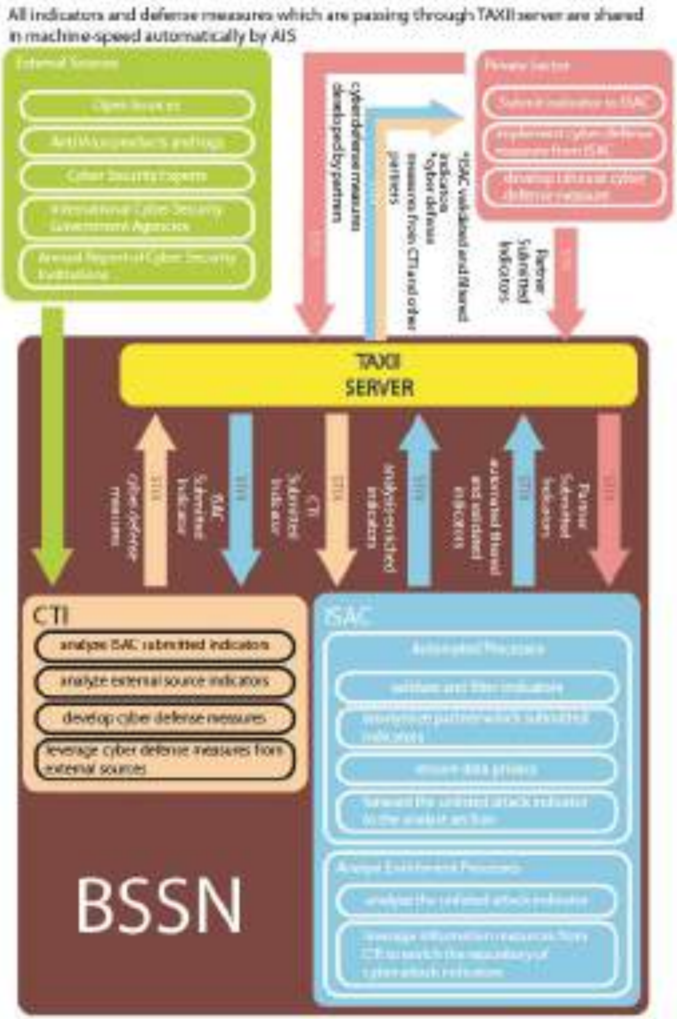

All indicators and defense measures which are passing through TAXII server are shared in machine-speed automatically by AIS
External Sources
Open Sources
Anti-Virus products and logs
Cyber Security Experts
International Cyber Security Government Agencies
Annual Report of Cyber Security Institutions
Private Sector
Submit indicator to ISAC
implement cyber defense measures from ISAC
develop internal cyber defense measure
cyber defense measures developed by partners
*ISAC validated and filtered indicators
*cyber defense measures from CTI and other partners
Partner Submitted Indicators
TAXII
SERVER
STIX
cyber defense measures
ISAC Submitted Indicator
CTI Submitted Indicator
analyst-enriched indicators
automated filtered and validated indicators
Partner Submitted Indicators
CTI
analyze ISAC submitted indicators
analyze external source indicators
develop cyber defense measures
leverage cyber defense measures from external sources
ISAC
Automated Processes
validate and filter indicators
anonymize partners which submitted indicators
ensure data privacy
forward the unlisted attack indicator to the analyst section
Analyst Enrichment Processes
analyze the unlisted attack indicator
leverage information resources from CTI to enrich the reputation of cyber attack indicators
BSSN

Figure 1. Semesta Cyber Security Workflow

The defense measures that have been developed are distributed to all partners. Apart from analyzing the indicators received from ISAC, CTI proactively participates in analyzing cyber threat indicators from external sources and then develops defense measures in order to minimize attacks and the impact of damage received by cyber threats. Finally, the CTI also utilizes external sources in finding efficient defense measures if the CTI could not find or develop their own defense measures for emerging or known cyber threats.

In the Semesta cyber security system, defense measures are not only developed by CTI and external sources, but also defense measures that developed independently by each partner of the Semesta cyber security system. In accordance with what is done with the defense measures from CTI and external sources, this defense measure is also passed on to all partners and also to CTI itself. This is in accordance with the meaning of the Semesta defense itself that a strong defense system does not only rely on government efforts, but also a collective effort by all parties.

2.5. Conclusion

Semesta cyber defense system can resolve known and emerging cyber threats collectively with the government but still able to maintain the anonymity of compromised partners. This system resembles of a semesta defense system that is adopted by the Ministry of Defense of the Indonesian Republic, where all parties play active roles in preventing and fighting the attack that arise from both internal and external. Practically, each partner is obliged to share cyber threat indicators to ISAC and the BSSN which managing ISAC n CTI, is also obliged to maintain the anonymity of the sources.

Theoretically, CTI and ISAC can be placed under the authority of the BSSN such as within the directorate; or they can also become an institution outside the BSSN but still under the direct supervision of the BSSN. The process of exchanging information in the Semesta cyber defense system runs at the engine-speed with the widest range and is carried out machine-to-machine without human intervention. These processes are done to ensure that every attack carried out could only be carried out once and the time the actor gains to break into the network greatly reduced. This makes every attack on the partner of the Semesta cyber defense system very costly and time consuming.

References

[1] Badan Pusat Statistik 2017 Statistik Telekomunikasi Indonesia 2017

[2] Fachryto T, & Achyar A 2018 Effect of Online Behavioral Advertising Implementation on Attitude toward Ad and Purchase Intention in Indonesian E-Marketplace. *Sriwijaya international journal of dynamic Economics and business*, *2*(2), 123-138

[3] Republik Indonesia 2008 Undang-Undang Republik Indonesia Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik

[4] Republik Indonesia 2016 Undang-Undang Republik Indonesia Nomor 19 Tahun 2016 tentang Perubahan atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik

[5] Presiden Republik Indonesia 2017 Peraturan Presiden Nomor 53 tahun 2017 tentang Badan Siber dan Sandi Negara

[6] Presiden Republik Indonesia 2017 Perpres Nomor 133 tahun 2017 tentang Perubahan atas Perpres Nomor 53 tahun 2017 pada tanggal 16 Desember 2017

[7] Aprilia M L, & Prasetyawati E 2017 Perlindungan Hukum Terhadap Data Pribadi Konsumen Pengguna Gojek *Mimbar Keadilan*, 90-105

[8] Rustam S 2018 Analisa Clustering Phising dengan K-means dalam Meningkatkan Keamanan Komputer *ILKOM Jurnal Ilmiah*, *10*(2), 175-181

[9] Malika A 2018 Pengaturan Hukum Internasional Terhadap Kejahatan Carding (Penggunaan Ilegal Kartu Kredit) Sebagai Bentuk Cybercrime

[10] Ekawati D 2018 Perlindungan Hukum terhadap Nasabah Bank yang Dirugikan Akibat Kejahatan Skimming Ditinjau dari Perspektif Teknologi Informasi dan Perbankan *Unes Law Review*, *1*(2), 157-171

[11] Erdianto Kristian 2017 Bagaimana Upaya Pemerintah Menangkal Maraknya Serangan Siber? Kompas (online) 21 Nov 2017 Available at : https://nasional.kompas.com/read/2017/11/21/22411551/bagaimana-upaya-pemerintah-menangkal-maraknya-serangan-siber?page=all [Accessed on 4 May 2019]

[12] Sicca S P 2018 BSSN Bentuk Sistem Penanggulangan Serangan Siber di Pemerintah Tirto.id (online) 9 Aug 2018 Available at : <https://tirto.id/bssn-bentuk-sistem-penanggulangan-serangan-siber-di-pemerintahan-cRgw> [Accessed on 5 May 2019]

[13] Jasper S 2019 Information Sharing Mechanism Cyber Operation Integration Seminar Jakarta

[14] McCarthy C, Harnett K, Carter A., & Hatipoglu C 2014 *Assessment of the information sharing and*

analysis center model No. DOT HS 812 076

[15] Mandt E J 2017 Integrating cyber-intelligence analysis and active cyber-defence operations. *Journal of Information Warfare 16*(1) 31-48

[16] Olivo N J 2017 *Applied cyber threat intelligence techniques for mainframe systems* (Order No 10687904) Available from ProQuest Dissertations & Theses Global: The Humanities and Social Sciences Collection. (1993168002)

[17] Veerasamy N 2017 *Cyber threat intelligence exchange: A growing requirement* Reading: Academic Conferences International Limited

[18] US Department of Homeland Security 2019 *Automated Indicator Sharing Fact Sheet*

THE COUNTER OF RADICALIZATION IN THE SCHOOL ENVIRONMENT THROUGH "*BELA NEGARA*" EDUCATION

Priyanto[1] and Ahmad Wafi Fauzi[2]

[1]Student of Ph.D.Program Indonesia Defense University, IPSC Sentul Complex, Bogor, 16810, Indonesia
[2]Master of Defense in Peace and Conflict Resolution Studies, Indonesia Defense University, IPSC Sentul Complex, Bogor, 16810, Indonesia

*Corresponding author: ahmad.wfauzi@gmail.com

Abstract. This research is motivated by the phenomenon of infiltration of radicalism in the environment of educational institutions, especially secondary education institutions, both at the junior high school (SMP) and senior high school (SMA) level. Radicalism is one of the causes of acts of terrorism. The pattern of acts of terrorism currently uses many children aged 8-18 as executors as to the Surabaya bombings in 2018. This research is intended to answer the problem of how the government's strategy in counter-radicalization in school environment based "Bela Negara" education. This research is qualitative research using the library research method. This study found that radically charged content can be easily accessed by middle and high school students through extracurricular activities, religious studies in the classroom, reading books in the library, and social media. Therefore we need a holistic, integrated, synergy and current strategy for the preparation of the Curriculum of "Bela Negara" which is prepared through coordination between relevant ministries and institutions.

1. Introduction

Terrorism became a common enemy after the September 11, 2001 incident, known as the 9/11 tragedy. Terrorist actions targeting the World Trade Center building followed the Pentagon building not long ago, which has awakened the international community that the threat of terrorism is now increasingly evident. Terrorism became a global enemy together after the statement of US President George Walker Bush on September 20, 2001 stating:

"Our war on terror begins with Alqaeda, but it does not end there. It will not end until every terrorist group of global reach has been found, stopped, and defeated"

Indonesia was also not spared from terror attacks. Terrorism attacks in Indonesia using bombs occurred in Bali on October 12, 2002, known as the Bali Bombing I. In that event 202 people died and the world and hundreds of others were seriously injured. Allegedly the bomb used by TNT and RDX type terrorists. The event that tarnished the name of Indonesia in the eyes of the world also proved that the threat of terrorism had reached Indonesia. In his statement the perpetrators of acts of terrorism since the attacks of 11 September 2001 claimed that what they did was *jihad fi sabilillah* (jihad in the way of Allah) as the testimony of Ali Imron, suspect of Bali Bombing I in the trial that the background of the Bali Bombing I was: dissatisfaction with the government which is not based on the Islamic Shari'ah and the absence of Imamat, the destruction of morality and the faith of the people, protects Muslims, retaliates against the infidels who fight the Muslims.

Based on the information revealed by Ali Imron, the Bali bombing actually happened as one of the answers made by a handful of Muslims who were aware and understood the meaning of a defense and self-esteem over the oppression of the colonial state (the United States and its allies) so that jihad must be carried out. Therefore it is necessary to discuss the roots of radicalism among some Muslims accompanied by efforts to handle and de-radicalization as a step to prevent the development of radicalism.[9]

Radicalism is a view that wants to make a fundamental change in accordance with the interpretation of adopted ideology or existing social reality. To get to these fundamental changes, not always with violent approaches, there are times when using persuasive methods, but sometimes the approach used uses methods of physical and symbolic violence which ultimately identify radicalism with acts of violence to self-sacrifice (suicide) to achieve a goal he believed in.[9]

Understanding of radicalism can come from various doors, one of which is school. The phenomenon of the Surabaya bomb which was the one perpetrator of the family that also involved children aged 8-18 years. The seeds of radicalism were indicated to have entered both public and private schools. The results of research from the Center for Islamic and Community Studies at the Syarif Hidayatullah State Islamic University in Jakarta said that

48,95 percent of students/student respondents felt that religious education influenced them not to associate with other religions. What is even more surprising is that 58,5 percent of student/student respondents have religious views with radical opinions.[4]

The entry of seeds of radicalism in the school environment will certainly be very concerning and tarnish the world of education in Indonesia. Even though it is clearly stated that the national education goals set forth in Article 3 of Act Number 20 of 2003 concerning the National Education System are: "... *developing capabilities and forming dignified national character and civilization in order to educate the nation's life, aiming at developing potential students to be human beings who believe and fear God Almighty, are noble, healthy, knowledgeable, capable, creative, independent, and become democratic and responsible citizens* ". The role of the government, teachers, parents and the community together has a responsibility so that the seeds of radicalism do not enter and develop in the school environment. *Bela Negara* education is one of the solutions to counter radicalization to counteract the massive radical ideas that have now entered the school environment.

2. Theoretical Framework

The arrest of suspected terrorists in Sibolga which led to the suicide bombing in March 2019 then reminded Indonesia of the dangers of the threat of terrorism. Terrorism and radicalism are two things that are mutually related. Both are ghosts that are frightening to most of humanity, including the entire Indonesian citizens. Changes in the patterns of attacks carried out by terrorist groups make the government help change the pattern of handling terrorism in Indonesia. The act of terrorism is not something that can stand alone if it is further elaborated terrorism has a flow of beliefs and ideologies that are embedded in the consciousness of the perpetrators of terrorist acts. An act of terror will quickly develop if society has been infiltrated by religious radicalism.[9]

So that it can be concluded that radicalism is the root of the birth of terrorism. Radicalism comes from the word *radix* which means root. Radicals in the *Kamus Besar Bahasa Indonesia* (Great Dictionary of Bahasa Indonesia) mean changes in a meaningful manner, whereas radicalism has the meaning of understanding or flow that wants a change and renewal fundamentally. While the National Counter Terrorism Agency (BNPT) defines radicalism as an attitude that wants a total and revolutionary change carried out by ignoring drastically embedded values through violent actions and extreme.[9] The mention of radicalism to call the extreme movement is seen as more appropriate than the use of the term fundamentalist because fundamentalism itself has many interpretations. In Islam, fundamentalism means a movement of renewal *(tajdid)* to return to the Qur'an and Sunnah. Whereas in the West's view fundamentalism means people who hold religious teachings rigidly, orthodoxy, and are not reluctant to use violence in defending their ideology. Fundamentalism can also be interpreted as anti-westernization.[3]

Having a radical understanding does not directly make someone participate in acts of terrorism. At least there are several factors that motivate someone who has a radical understanding to join in a terrorist act or network. First, domestic factors or domestic factors, such as disappointment with the government, poverty, discrimination. Second, international factors, such as the emergence of religious sentiments, foreign policy that tends to be unfair, modern imperialism by superpower countries. The third factor is cultural factors related to religious understanding such as textual scriptures.[9]

It needs to be noted in advance that radicalism is a movement carried out by a group of individuals who are sociopolitically and sociohistorically disadvantaged both by the government nationally and globally. Violent actions carried out by a group of Muslims are caused by social and political symptoms compared to carrying out the arguments contained in the scriptures. Consciously the media (especially western media) have pinned radicalism on Muslims because of the practices of violence committed by a group of Muslim communities so as to create the formation of identity that turns into a prejudice. The phenomenon of radicalism carried out by a group of Muslims was exaggerated by the western press so that Islamophobia emerged which made Muslims need to be suspected so that they cornered Muslims. What was captured by the western press about Islam was defined by the international community. The radical movement embedded in Islam for the western press was seen as more attractive than labeling Hindu militant groups in India, IRAs in Northern Ireland, extreme Jewish groups in Israel or the Communist-Marxist movement as a radical movement.[7]

So it appears that the western press uses double standards and behaves unfairly towards Islam. What is done by the west is the restraint of Islamic civilization amid Islamic civilization is in the process of forming its identity in the modern era. So that the radicalism carried out by a handful of Muslim groups cannot justify the radicalism carried out by Muslims. Whatever the reason, acts of violence in the name of religion are a violation of religious norms and abuse of humanitarian norms.

3. Research Method

This study uses a qualitative approach by using library research that focuses on books, journals, and papers that are relevant to the objects to be studied obtained through conventional search and relevant electronic technology with the title "Counter Radicalization in the School Environment Through *Bela Negara* Education.

Data is obtained by studying and reading carefully. Then the data obtained are recorded and grouped according to the existing themes. The next stage of the data that has been grouped is taken to answer the research object.

4. Result and Discussion

5.1. Development of Radicalism in Indonesia

After the September 11, 2001 attacks in the United States, Indonesia became one of the regions in Southeast Asia where terrorism was rife, one year after the September 11, 2001, Indonesia was rocked by the Bali Bombing I, the Incident at JW Marriot Hotel in 2003 in 2004, Bali Bombing II Event in 2005, Bombing Events at Ritz Carlton and JW

Hotels Marriot in 2009, Bomb and shootout at Jalan MH Thamrin Jakarta in 2016, Kampung Melayu Bombing Events in Jakarta in 2017, Surabaya Bombing Events in 2018, and Bom in Sibolga in 2019. From these cases, the perpetrators committed the action is in the name of religion. [1]

The emergence of radical Islam in Indonesia is at least caused by two factors, namely: internal factors, namely factors originating from within the Muslim community, namely the occurrence of deviations (bid' ah) in religious norms. Next is external factors, namely factors originating from outside the Muslim community, such as Western hegemony that displaces Islamic values, so the term jihad arises. Jihad is used as a symbol of effective resistance to rally resistance to Western hegemony.[1]

In the context of Islamic radicalism, Zastrouw divided the radical Islamic movements into two typologies: First, the Critical Radical movement which was motivated by the existence of social pressure on arbitrariness, and social injustice. Second, the fundamentalist radical movement is a radical movement that knows no compromise, anti-dialogue, and is exclusive which does not give space to local traditions and values because it is considered to divert religious values *(bid'ah)*.[5]

The development of Indonesian right radicalism was the result of the post-fall of the New Order in 1998. The form of Islam in Indonesia became very diverse. The development of Islamic diversity is reflected in a large number of organizations patterned in Islam and the organization of interests over Islamic ideas from time to time increasingly diverse and varied. During the New Order, the government at that time always cleared radical movements. For the New Order government radicalism was the number one enemy and became the common enemy of both left radical and right radical movement. The left radical that had developed in Indonesia from 1980 to 1990 which was transformed through the Democratic People's Party, was under pressure from the state and many of its figures were captured, and until now it is unclear how high the fate is now. Likewise, with the right radical movement, the right radical movement that had emerged in Indonesia during the New Order was Command Jihad, many Islamic figures suspected of being affiliated with Command Jihad were arrested and detained by the New Order regime.[5]

But after the fall of the New Order era into the reform era, the left radical movement was in a state of suspended animation, but not so with the right radical movement. With the opening of the door to freedom of opinion and expression, the right radical movement is increasingly flourishing, organizations such as : Majelis Mujahidin Indonesia (MMI), Islamic Defenders Front or *Front Pembela Islam* (FPI), Lasykar Jihad, Jamaah Ansharut Tauhid (JAT), Hizbut Tahrir Indonesia (HTI) and Islamic State Of Indonesia or *Negara Islam Indonesia* (NII). Based on the historical background right radical groups can be categorized into three groups, namely: 1). Local groups, which have no connection with the Darul Islam movement and International Organizations. In this category, for example, the Islamic Defenders Front or *Front Pembela Islam* (FPI) and Laskar Jihad. 2). Groups that have relations internationally but have no connection with the Darul Islam movement, in this category an example is

Hizbut Tahrir Indonesia (HTI). 3). Groups that have relations with the Darul Islam movement but do not have official relations with international networks, for example, Majelis Mujahidin Indonesia (MMI). It was from the Majelis Mujahidin Indonesia group that it gave birth to a regional terrorism activity called Jamaah Islamiyah affiliated to AlQaeda and ISIS.[1]

The history of right radicalism in Indonesia can be traced to the development of the oldest radical organization in Indonesia, namely Darul Islam or the Islamic State of Indonesia or *egara Islam Indonesia* (NII). Then the Salafi jihadi doctrine is also suspected as the red thread of the growth of radicalism in Indonesia. The Islamic State of Indonesia or *Negara Islam Indonesia* (NII) was founded on 7 August 1949 by S.M Kartosoewirjo. The aim of the Indonesian Islamic State is to fully implement Islamic law throughout Indonesia and reject the single principle of Pancasila. Although the Imam of NII, Kartosoewirjo was executed in September 1962, NII's struggle never subsided. The NII struggle was then continued by the *Komando Jihad* group involved in the Talangsari Lampung incident. Now the ideals of establishing an Indonesian Islamic State are still being fought for by the Indonesian Islamic State group Region IX or *Negara Islam Indonesia Komandemen Wilayah IX* (NII KW IX).

Whereas *Salafi jihadi* which is also suspected as the red thread of the growth of radicalism in Indonesia is a movement that is global in nature. This movement is a combination of the harakah of the jihadi (jihadist movement) from the thoughts of Sayyid Qutb and the Wahhabi-style Salafi creed. According to the term *Salafi* meaning ancient people, namely a method in Islam that teaches and practices Islamic Shari'a such as the period of the Prophet Muhammad without any reduction and addition, because for them Islam is a thing in Islam that teaches and practices Islamic Shari'a like the Prophet Muhammad without any reduction or addition, because for them Islam is a *syaamil* and *kaamil* (dynamic and complete) so *ijtihad* (interpretation) is no longer needed. Furthermore, *jihad* means trying seriously. So that *Salafi jihadi* means fighting for the application of the Qur'an and al-hadith according to the understanding of the previous generations of Islam seriously. According to the Salafi jihadi view, every government that is not lawful to Islamic Sharia is an infidel even though its population and government are Muslim. Replacing a government that is not Islamic in nature to a government with Islamic law in the Salafi jihadi view is the biggest jihad. The Salafi Jihadi movement began to develop in Indonesia in the 1980s which was inspired by the pattern of the Ikhwanul Muslimin movement in Egypt spread through Hasan Al Banna's thought books and the momentum of the success of the Iranian Islamic Revolution and the Mujahideen of Afghanistan fighting the Communist Soviet occupation (Sinaga, 2015). Some examples of organizations that adopt the Salafi jihadi ideology include Hizbut Tahrir Indonesia (HTI), Majelis Mujahidin Indonesia (MMI), Jamaah Ansharut Tauhid (JAT), dan Jamaah Islamiyah (JI).

Radical movement activists use several means and media to disseminate their understandings in the framework of internal members' cadre, recruitment of new cadres, and socialization to the public. Some of the tools taken by radicalism activists include:

- Through cadre organization which is usually in the form of training new prospective members and fostering old members. Campuses and schools are the best means to cadre radical organizations by utilizing senior-junior relations surrounded by schools and colleges. Indoctrination of radical notions in schools and campuses can take advantage of a network of Islamic Spiritual activities (Rohis). Student activities are often infiltrated by outside parties invited to fill the activity.
- Through magazines, bulletins or jihad that contain radicalism content.
- Publishing books.
- Spread via the internet
- Through mosques which become the "base" of radical Islamic movements.[6]

5.2. The Impact of Radicalism in the School Environment

The development of the doctrine of radicalism has undergone development both in action, mode, pattern, cadre process and method of socialization. This is also due to the influence of digitalization of information technology that is growing rapidly so that recruitment and cadre have surpassed national borders *(borderless)* which later developed into a network to carry out acts of terror in groups or individuals *(Lonewolf)*.

Now the influence of radicalism has also targeted young Indonesians at the college level, senior high school and even to the junior high school environment. At least there are several factors that make young people easily influenced by radical thinking including psychological factors, national and international political conditions, textual understanding of religion, absence of role models plus the development of science and technology.[7]

Psychologically, Kauffman said that adolescents are very vulnerable to exposure from outside influences because adolescents tend to have prominent behavioral and emotional problems. Furthermore, Loeber explained that behavior problems and emotional problems lead to aggressive behavior that is diverse and a tendency to violent behavior .[7]

Teenagers also tend to be easily exposed to radicalism because of the transition period in the transitional age which causes an identity crisis and enters the search for identity phase. This is what Havighurst calls an interim status, which has escaped childhood but has not yet fully become an adult. This crisis then opened the mind to accept new ideas, including radical ideas. Another pathway that causes young people to easily accept radicalism because there is a moral shock .[8]

In addition to internal factors within the individual youth, external factors originating from formal education institutions also make radicalism understandably influence young people. The limited ability of schools to oversee all activities carried out by their students makes radicalism easy to infiltrate into classrooms. Besides that radical understanding can also be entered through reading books and activities at school. In some cases, the inclusion of radical thinking in schools actually received support from the management of educational institutions. This is due to the lack of the ability of schools to filter out the content taught in extracurricular activities and literature read by students. In addition to activities outside the classroom, teacher factors also influence the entry of radical ideas in the school environment. Sometimes teachers often approve teaching the material in teaching books without taking deeper consideration.[6]

5.3. Counter-Radicalization Strategy Based on "Bela Negara"

One way to prevent the entry of radicalism for the younger generation is education. Education aims to provide skills, knowledge, and values. Skills and knowledge aim to fulfill life needs, and understanding of values is useful as behavioral control. Understanding of good and bad values makes students able to choose a way of life that is dignified and does not justify the way to achieve their goals. State defense education is one way to ward off learners from the influence of radical thinking that increasingly influences the younger generation to classrooms. The implementation of counter-radicalization strategies is a cross-sectoral joint responsibility involving ministries and institutions such as the Pancasila Ideology Development Agency (BPIP), Ministry of National Education, Ministry of Religion Affairs, Ministry of Defense and National Counter Terrorism Agency (BNPT) involving the participation of teachers, parents and the community so that young people students in educational institutions are not exposed to radicalism.

Counter-radicalization is a preventive program with the aim of preventing the public, including students exposed to radicalism. In an effort to deter the danger of radicalism, it includes efforts to prevent early and early detection with the aim of stopping the flow of radical thought in educational institutions so that it can stop acts of terrorism . The counter radicalization that can be built to prevent the entry of radical ideas among middle school students (SMP-SMA) is through *Bela Negara* education.[8]

Bela Negara can be understood as an attitude and behavior and actions of citizens inspired by the love of the Republic of Indonesia based on Pancasila and the 1945 Constitution of the Republic of Indonesia aimed at ensuring the survival of the nation and state. [2]

Indeed the state defense charge has been integrated into Citizenship Education or *Pendidikan Kewarganegaraan* (PKn). But now Citizenship Education (PKn) faces the challenges of issues of radicalism and terrorism that are free to enter into classrooms. A new formula is needed to inject "*Bela Negara*" content in every aspect of the younger generation's life, especially for junior and senior high school students, considering the ways in which activists of radicalism are one step ahead of the methods used to deliver *Bela Negara* content integrated through Citizenship Education (PKn). Among them is the spread of radical content through social media, as known to middle and high school students today can be categorized as Generation Z, the generation born between 1995-2010 where this generation was born when technology was growing rapidly. The characteristics of this generation are more individual and friendly to technology. Because it is individual and friendly to technology, the Z generation tends to complete their curiosity through the internet. At the same time radical movements also massively socialized radical thoughts through internet media. Based on a survey conducted by the Center for the Study of Islam and Society (PPIM) of Syarif Hidayatullah State Islamic University in Jakarta as reported by Tirto.id, Z generation who do not have internet access actually think more moderate than those who have easy access to the internet. This proves that social media contributes significantly to the formation of character in generation Z.[2]

Facing an increasingly massive attack of radicalism, a Grand Design of the *Bela Negara* Curriculum is needed that touches all aspects of education for students, both intracurricular and extracurricular. The *Bela Negara* Education curriculum in question is holistic, integrated, synergetic and up-to date. *Holistic* means to encompass in its entirety, that all subjects taught at the junior and senior high school level contain the contents of the *Bela Negara* such as the history of the nation, the values of patriotism and the love of the country, character, diversity and national plurality. *Integrated* means that the *Bela Negara* Education curriculum is a unified whole both intracurricular and extracurricular, state defense values taught in class are applied in extracurricular activities, one of the extracurricular activities which are full of Bela Negara education is Scouting, in Scouting the application of values countries that are theoretically studied in the classroom are applied in concrete actions that have a benchmark of assessment. Furthermore, the *synergy* that is between subjects loaded with Bela Negara content is a harmonious balance, resulting in optimum results. An example of this synergy can be applied to Citizenship Education or *Pendidikan Kewarganegaraan* (PKn) and Religious Education Lessons. Civics lessons provide examples of the values of *Bela Negara*, while Religious Studies strengthen with the basis of the scriptures of the Holy Book. And the last is the *present value(up-to date)*, which means the pattern of teaching, material, and delivery of material tailored to the conditions of the times and the psychology of students. Therefore the instructor or teacher must also improve their competence, think broadly, understand the psychology of students and be able to keep up with the times and technological developments.

Radicalism is a real threat that is now faced by the whole world, including Indonesia. The threat that will undermine the ideology of the Nation is a non-military threat so that it requires the synergy of Ministries and Institutions to stem the attacks of radicalism in the secondary education environment. The compilation of the Grand Design of the *Bela Negara* Education Curriculum that is holistic, integrated, synergetic and present must involve cross ministries and institutions including 1). The Pancasila Ideology Development Agency or *Badan Pembinaan Ideology Pancasila* (BPIP) whose duties are mandated in Article 3 of Presidential Regulation Number 7 of 2018 concerning the Pancasila Ideology Development Agency are:"*.... to coordinate, synchronize, and control the development of Pancasila ideology in a comprehensive and sustainable manner, and implement the standardization of education and training, conduct education and training, and provide recommendations based on the results of studies of policies or regulations that conflict with Pancasila to high institutions country*". 2). The Ministry of National Education, as a Ministry that oversees formal and informal education from elementary to secondary levels. 3). The Ministry of Religion Affairs oversees formal and informal religious education from the elementary level (madrasas) to universities (Religious Colleges). 4). The Ministry of Defense, as the master design designer for the implementation of the National Customs Awareness Coaching program which is in line with the Ministry of Defense's program to form 100 million *Bela Negara* cadres. dan 5). The National Counterterrorism Agency (BNPT) as a non-ministerial institution is also tasked with coordinating relevant government agencies in implementing and implementing policies in the field of counter-terrorism.

The compilation of holistic, integrated, synergic and current national martial arts curriculum in dealing with issues of radicalism and terrorism is in line with the 8th Nawa Cita agenda proclaimed by the seventh President of the Republic of Indonesia Ir. Joko Widodo namely: "*Revolutionizing the nation's character through a policy of restructuring the national education curriculum by prioritizing aspects of citizenship education, which places proportionally the aspects of education, such as teaching history of national formation, patriotism and love of the country, the spirit of defending the country and character in the Indonesian education curriculum* ".

5. Conclusion

The rise of acts of terror that have occurred in Indonesia signifies the incessant flow of radical thought in Indonesia. The act of terrorism cannot be separated from radicalism. But having radical thoughts does not necessarily mean that someone is carrying out acts of terrorism, there are several other factors that encourage someone who is radical in being able to carry out acts of terror. So before acts of terror occur, an early prevention strategy is needed to suppress acts of terror by reducing adical thinking.

The current pattern of bomb terror attacks makes children as executors, for example, the Surabaya bomb. Children will not want to be executors of suicide bombings if there is no radical doctrine that permeates his thoughts. Besides that, right radicalism has now entered classrooms, library books, and social media. The government needs to form a counter-radicalization strategy to stem the radicalism that has now entered educational institutions to the junior high school level. The strategy prepared is to make the *Bela Negara* Education Curriculum that is holistic, integrated, synergy and present value. Because the threat to the nation's ideology is a non-military threat so that the leading sector that handles is the coordination of relevant ministries/institutions consisting of Pancasila Ideology Development Agency (BPIP), Ministry of National Education, Ministry of Religion Affairs, Ministry of Defense and National Counterterrorism Agency (BNPT). This counter-radicalization strategy in secondary education is certainly aimed at achieving national education goals and the 8th Nawa Cita.

References

[1] Sinaga, Prayitno, and Ian Montratama 2018 *Terorisme Kanan Indonesia: Dinamika dan*

Penanggulangannya (Jakarta: Elex Media Komputindo)

[2] Tippe, Syarifuddin 2017 *Redesain Bela Negara dalam Sistem Penddikan Nasional : Perspektif Manajemen Strategi* (Jakarta:Yayasan Obor Indonesia.

[3] Nur A and Rory O 2014 *Terorisme Insurjensi dan Peperangan Cyber* (Jakarta : Dapur Buku)

[4] Convey Indonesia (PPIM UIN Jakarta &UNDP Indonesia) 2018 Ancaman Radikalisme di Sekolah *Policy Brief Series Vol 1 Serie 4 (2018).*

[5] Moh. Hasim 2015 Potensi radikalisme di Sekolah : Studi Terhadap Buku Pendidikan Agama Islam di Sekolah Dasar *Journal Edukasi* ***14*** pp 255-259

[6] Laode Abdul Wahab 2016 Metamorfosa Radikalisme pada Lembaga Pendidikan di Sulawesi Tenggara *Shautut Tarbiyah* **22** pp 69-70

[7] Rindha W, Sumiyem, and Kuntarto 2017 Kerentanan Radikalisme Agama Di Kalangan Anak Muda *Proc. National Seminar on Human Resources and Village Development* pp 1553-1556

[8] Abdul M 2012 Menangkal Radikalisme Agama di Sekolah *Jurnal Pendidikan Islam Volume 1 Nomor 2* **23** pp 160-161.

[9] Badan Nasional Penanggulangan Terorisme 2015 *Strategi Menghadapi Paham Radikalisme Terorisme – ISIS,* (Jakarta : BNPT)

THE LEVEL OF YOUNG PEOPLE'S PARTICIPATION, MOTIVATION, AND STRATEGY IN ENCOUNTERING PROXY WAR THREAT TOWARD THE INTEGRITY OF THE REPUBLIC OF INDONESIA

Sri Arfani[1], Vera Agustina Yanti[2]

[1]Universitas Bina Sarana Informatika, Indonesia [2]Universitas Bina Sarana Informatika, Indonesia

Abstract. The purpose of this study is to analyze the level of participation and motivation of the young people in anticipating the threat of proxy war on the integrity of the Republic of Indonesia. The study was conducted on the students of the Faculty of Economics and Business majoring in D3 Business Management at Universitas BSI Jakarta during the research period from February to April 2018 with 75 sampling respondents. Based on the analytical data using SPP version 2.1, this study resulted that partially the level of motivation had a significant effect on the threat of proxy war and simultaneously variable X had an effect on the basis of the Y variable, which is the threat of proxy war. Descriptively, the level of participation and motivation in facing the threat of proxy war was in the moderate category. The strategies used were input and output process, one of which provided training and mentoring for young people, and state defense training to equip them.

1. Background

War or conflict that occurs as a proxy war has taken place before World War I and II and during the Cold War, where there were two important actors in a proxy war, in which carried out by a big country to a group of individuals who were non-state actors and state actors. According to Hidayat (2017), all conflicts that occur have a tendency to power, both in the form of soft power and hard power. Soft power in a proxy war is using economic devices and, nowadays, technology and information devices in the form of assistance or donations from donor countries or agencies, while hard power is carried out by the intervention of economically, politically, and militarily well-established countries to the third world countries or developing countries. The intervention was effectuated with military or political instruments.

A set of rules and standards of achievement were also conceived to measure the progress achieved by donor-recipient countries in the form of global policies such as MDGs (Millennium Development Goals), Civil Supremacy, Human Rights, Climate Change, transparency and accountability. According to Nye in Hidayat (2017), there is a difference between hard power and soft power, which is coercive power through military intervention, diplomacy, and economic penalty while soft power is: the power as the ability to influence others to get the desired results.

On the other hand, this set of standards and regulations cannot be rejected because it is an important issue in international politics. In some cases, interventions were carried out to replace the ruling regime (such as the Arab Spring), influence political leaders (Latin America and Africa), and of course ultimately perpetuate the power of major countries on the international political stage both in terms of power and influence. War is carried out by one party to another party by using a third party originating from within the country itself or another actor who operates whether by utilizing local communities.

Meanwhile, the form of proxy war also varies, especially in Indonesia, which can take many forms, one of which is the separatist movement that wants to separate itself from the Republic of Indonesia. The proxy war in Indonesia also manifested itself in the form of mass demonstrations, adverse regulatory systems, terrorism, drug trafficking, and clashes between groups, and the development of Lesbian, Gay, Bisexual, and Transgender (LGBT) groups in Indonesia to destroy Indonesian young generation. In Indonesia, there are five factors that influence and become the cause of the proxy war: (1) Indonesia's natural resource wealth, (2) unstable Indonesian unity, (3) apparatus that are easily lured by power, (4) Indonesian strength in Southeast Asia, and (5) easily provoked society.

The role of participation and motivation of young people as the next generation is needed for the country. In line with Mardikanto (2014) that the participation of every citizen in solving problems for the successful development of the Republic of Indonesia is important. Because of the role of youth as the backbone of the nation, they must be aware of the various challenges and threats of the nation to then unite and work together to maintain the safety of the nation and country. A number of actions that can be taken especially by students to counteract proxy war in the country include always identifying and recognizing problems, experts in their respective disciplines, conducting youth-based entrepreneurial movements and organizing learning communities, and pioneering character building programs. Meanwhile, based on Central Bureau of Statistics (BPS) data in 2017, it is stated that some of Indonesia's population 60 percent are productive young people. Based on the description above, the importance of the motivation to mobilize youth to have awareness and willingness to overcome the threat of proxy war is shown. Therefore, it is important for the young generation to have high enthusiasm to be a generation that is intelligent and has a strong will to build strong character to avoid influences that may lead to any activity related to a proxy war. This is in line with Gibson (1995) that the yield of performance is influenced by several factors, one of which is motivation in the individual.

On the other hand, social media users in Indonesia based on the data from Linkedin in (2017), especially Facebook, are ranked fourth in the world, while according to the Association of Indonesian Internet Service Providers (APJII) internet users in Indonesia in 2016 are around 123 million people or around 51.5% of the total population of Indonesia. The use of social media can have a negative impact, especially when it is very extreme in the case of social media users, such as utterances of hatred, hoax, racial issues, and blasphemy. This is certainly very dangerous for the integrity of the Republic of Indonesia.

As explained above, proxy war has been taking place in Indonesia in various forms, such as intervention from foreign parties in the form of black campaigns, control of assets by foreign parties, foreign-based regulation, and separatist movements that threaten the integrity of the Republic of Indonesia. Based on the facts in the field, one of the proxy wars in Indonesia shows coverage from Liputan 6 (2017) reached 3.5 million people of drug use. LGBT behavior among the productive age according to Jawa Pos (2012) has reached 1 million people in Indonesia. Because of an increasingly high threat of proxy war, threatening the nation's next generation, it is hoped that the behavior of the young people can prevent and overcome this problem so that the integrity of the Republic of Indonesia is maintained. There are gaps in the conditions in the current environment, especially in dealing with proxy war threat. Strategies and efforts are needed to support the role of young people in facing the threat of proxy war through behavior change among young people with a variety of steps and actions to mobilize youth, to have awareness and generate a high sense of motivation to reduce the deviant behavior that is part of the proxy war.

For this reason, the researchers wanted to raise the theme of the level of young people's participation in facing proxy war. The formulation of the problems obtained are: (1) How are the participation and motivation level of the young people in facing proxy war, (2) To what extent the influence between the role of the young people in terms of the level of participation and motivation against the proxy war threat, and (3) Strategy approach in facing threat of proxy war.

2. Theoretical Approach

Referring to the Online Oxford English Dictionaries, proxy war is a war carried out by two or more great powers, but these forces do not directly touch one another. According to Nurmantyo (2018), it can be described that proxy war is a confrontation between two major powers by using substitutes, to avoid confrontation directly with reasons to reduce the risk of fatal conflicts. Since the cold war era, the practice of proxy war has occurred in almost all parts of the world. One of the most famous examples is the proxy war between the US and the Soviet Union in the form of the Vietnam War. The other example, such as the civil war that took place in Syria, until now, even the Indonesian state has entered into the next target of "victim" of proxy war. According to Aymardi Azra, proxy war or more specifically called as "proxy sectarian war" exists because of religious sectarianism. Briefly, proxy war 'is a puppet' war between two or more countries without directly involving countries or citizens themselves in an open war between them.

The understanding according to Born in Mardikanto (2014) stated that participation is an action to take part, namely an activity or statement to take part in an activity with the intention of obtaining benefits. Levels of participation according to Wilcox (1988) have five levels: (1) providing information, (2) consulting, (3) joint decision making, (4) acting together, and (5) providing support. As for the growing participation of the youth's role in preventing the proxy war threats, they are (1) the opportunity, (2) the willingness, and (3) the ability of the younger generation to participate in the fight against the threat of war which disrupts the integrity of the Republic of Indonesia. On the other hand, according to Robin (1996), motivation is an impulse that arises from a person in a direction of behavior that begins with the need that has not been satisfied so as to give rise to an urge to realize desires. Motivation consists of two dimensions, they are intrinsic and extrinsic motivation. The intrinsic motivation factor is a driving factor in young people to have an awareness of the importance of understanding the threat of a proxy war for the integrity of the Republic of Indonesia. The extrinsic motivation is an effort to encourage the younger generation to be able to carry out activities to prevent threats of proxy war which disturbs the Republic of Indonesia.

3. *Framework and Hypothesis*

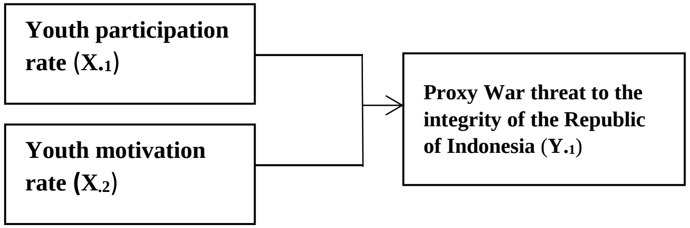

Youth participation rate ($X_{.1}$)
Youth motivation rate ($X_{.2}$)
Proxy War threat to the integrity of the Republic of Indonesia ($Y_{.1}$)

Figure 1. The framework of the level of participation and motivation on proxy war threat

Based on the frame above, the research hypothesis is used as follows: the threat of a proxy war on the integrity of the Republic of Indonesia (Y_1), significantly influenced by the level of participation of the younger generation (X_1), and the level of motivation of the younger generation (X_2).

4. *Research Method*

The method of data analysis on this study used the mixed methods, quantitative and qualitative methods. This research used a quantitative approach, with survey methods, and to deepen data in quantitative analysis supported by a qualitative approach. The survey was conducted in one research location at a university in Jakarta. Qualitative is by searching literature that has relevance and substance to explain the potential phenomena and the role of young people participation in preventing proxy war. The results of the identification of analysis and meaning were then used to draw conclusions and phenomena observed in the study, using quantitative methods. The study was conducted in February 2018 until April 2018 for the students of D3 Office Management program on the Jatiwaringin campus.

The method in selecting the sample of respondents was determined by simple random sampling technique. The determination of the number of samples was using Slovin method by 5% precision. The study population was 93 students with a sample of 75 students who were fulfilling the requirements for respondents from a predetermined population. The data collection techniques of the business actors of UMKM were collected using interview techniques, questionnaires, observations of students in Jakarta and relevant stakeholders, during the study. Interviews with related sources were conducted during the study. Qualitative data were analyzed using descriptive statistics and inferential statistical tests, namely by analysis of SPSS version 2.1. Processing and analyzing data using descriptive and inferencing statistics. Multiple linear regression test with SPSS 21 software.

The collection of data and information is done by looking at the results of research by previous researchers and other researchers who have published scientific papers and scientific publications both in the form of online and reference in the form of periodic books and other sources. Based on data and information collected, the researchers conducted an analysis of the studies that conducted the substance and scope of the relevant problems, based on the review the researcher synthesized to provide understanding and meaning of the information obtained. Furthermore, quantitative data collection was using survey methods for collecting various types of information and interviews using structured questions as outlined in the form of questionnaires. Thus, this study observed the relationship between two independent variables and one dependent variable. That is the variable X is the role of participation and motivation of the young people towards the Y variable, namely the threat of proxy war against the Republic of Indonesia.

5. Result and discussion

5.1 *Description of the young people's participation in facing the threat of proxy war*

Based on the results of descriptive data, the participation rate of the young people was currently in the moderate category. Based on the Likert scale measurement was 2.89. While the number of answers to the average score of answer 3, as much as this illustrates a number of answers to respondents 377. This is because many young people today have a lot of sensitivity and concern for the environment and current conditions of low efforts by young people to face the threat of proxy war. Movements or campaigns related to a proxy war in changing the individual behavior of each young person are driven by the low self-awareness of young people on the importance of efforts to prevent proxy war and the impact of the proxy war threat. The results of the Gardiana's study (2017) show that the proxy war among young people in the need for state defense education and early education will shape their minds by identifying and recognizing problems through character building programs, whereas according to Victor (2016) it is stated that the need for combination the strategy of hard power and soft power is needed by a strong military and strong partnerships and institutions.

5.2 *Description of the young people's motivation in facing the threat of proxy war*

Based on the results of descriptive data, it showed that the motivation level of the young people is currently in the moderate category. Based on the measurement of the Likert scale of 2.89, while the number of answers on the average score of the answer was 3, this illustrates a number of answers to respondents 380. This is because many young people today are low in carrying out actions on efforts made by young people to face the threat of war proxy.

6. Results of the Data Analysis

The data analysis technique in this study used multiple linear regression analysis, the SPSS test version 2.1. The results of the validity test showed that most constructs were stated to be quite good, through field tests with respondents 30 people outside the population with significant value > 0.001. Reliability test shows that the Cronbach alpha value of each construct shows good results of the Cronbach alpha coefficient obtained by most of the required values, namely $Y_1 >$ from the r table value. Cronbach alpha internal consistency testing needs to be tested for instrument reliability with the construct validity and variance extracted obtained, most of which show values above 0.5. This means that all instruments are reliable, namely Y_1=Threats to proxy war, the value of the instrument variables of the young people's participation rate and the level of motivation in facing proxy war threats are quite reliable. The test results of multiple regression analysis are presented in Table 1.

Table 1. Test of multiple regression analysis

	Unstandardized coefficient		Standardized coefficient	T	Sign
Variable	B	Standard of error	Beta		
Constant	11.085	3.337		3.322	0.001
Youth Participation (X_1)	-0.013	0.066	-0.023	- 0.198	0.843
Youth Motivation (X_2)	0.467	0.121	0.442	3.867	0.000
Adjusted R ₂					0.434
F count					8.252
Sign F					0.001

Based on the description of the results of the data above, the equation for the regression model is obtained as follows:

$$\mathbf{Y= 11.085\text{-}0.013X_1+0.467X_2}$$

From the results of the analysis through SPSS statistical test version 2.1, the results obtained were that there is a significant influence on the level of participation and motivation against the threat of proxy war.

Based on the results of the analysis of the threat level of proxy war, it is significantly influenced by the motivation level of 0.467: p = 0.000, and is influenced unrealistically by the participation rate of = -0.013 X1: p = 0.843 and means the threat level of proxy war will be higher if affected by the high and low level of motivation of the young people in anticipating the threat of a proxy war that disrupts the integrity of the Republic of Indonesia.

Based on the results of hypothesis testing and the level of probability of the causal relationship of hypotheses between the factors sub-variable $\mathbf{X_1\text{-}X_2}$ to $\mathbf{Y_1}$, level of participation of the young people variable **(X_1)** and variable $\mathbf{X_2}$ which is the level of motivation simultaneously influences the participation and motivation in facing the threat of proxy war has a positive effect in facing the threat of war proxies. It is based on the value of **F table** shows the coefficient of **8.252 > F table**, through partial participation rate does not significantly affect **0.843** > sign value; (2) the level of motivation has a positive effect and on the threat of proxy war of **0,000** <value of **0.005**, through a test of the value of determination $\mathbf{R^2}$ indicates the threat level of proxy war is **43%** influenced by motivation factors and participation levels, while **57%** threat of proxy war is

influenced by other factors which were not included in this study.

Based on the results of the above test it can be stated that the dominant influence on the threat of proxy war is the X_2 variable, namely the motivation of the young people in facing the threat of proxy war. Motivation is an effort made by individuals to generate an impetus to take action to motivate the young generation to prevent and have awareness in facing the threat of proxy war by forming good character and defending the Republic of Indonesia. The strongest motivation driver is his own desire with the help of encouragement and support from the environment so that he can help overcome the threat of proxy war. The young people in facing the threat of proxy war were influenced by extrinsic and intrinsic motivation.

7. Efforts to Implement Strategies for Young People in Facing Proxy War Threats on the Integrity of the Republic of Indonesia.

Strategy according to Mintzberg (1998) is a program or planned step to achieve a set of goals or ideas that have been determined. Strategic efforts for the younger generation in facing the threat of proxy war are carried out using the Input, Process, and Output, and Impact approaches. The main effort that needs to be implemented is a strategy to change the behavior of the young generation into a generation that is active and caring and sensitive to the threat of a proxy war that threatens the integrity of the Republic of Indonesia. Based on the results of the analysis test, the level of motivation of the younger generation has a significant effect on efforts in facing the threat of proxy war, while the level of participation does not significantly influence the threat of proxy war. Efforts are made to strengthen the level of motivation of the younger generation to actively take action in anticipating the threat of proxy war. Strengthening motivation includes: building effective communication strategies for the younger generation and supporting internal and external environments. The strategy process is divided into 4 stages, namely:

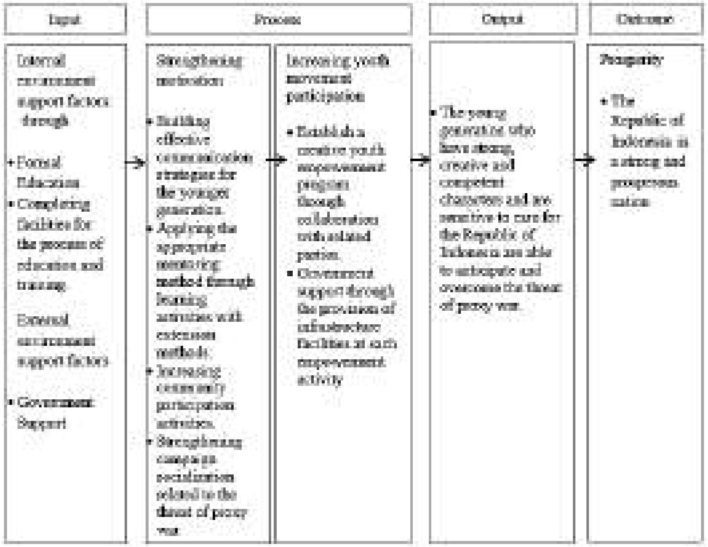

Input
Process
Output
Outcome
Internal environment support factors through
• Formal Education
• Completing facilities for the process of education and training
External environment support factors
• Government Support
Strengthening motivation
• Building effective communication strategies for the younger generation
• Applying the appropriate mentoring method through learning activities with extension methods
• Increasing community participation activities
• Strengthening campaign socialization related to the threat of proxy war
Increasing youth movement participation
• Establish a creative youth empowerment program through collaboration with related parties
• Government support through the provision of infrastructure facilities at each empowerment activity
• The young generation who have strong, creative and competent characters and are sensitive to care for the Republic of Indonesia are able to anticipate and overcome the threat of proxy war.
Prosperity
• The Republic of Indonesia is a strong and prosperous nation

Figure 2. Strategy for the young people in anticipating proxy war threat

8. Conclusions and Recommendations

8.1 Conclusions

The level of motivation and participation of the younger generation is on the average in facing the threat of proxy war that threatens the integrity of the Republic of Indonesia. Based on the results of the multiple regression analysis outlined from the two independent variables, there is one variable that must be considered a priority, namely motivation because of these factors that affect the level of threat of the proxy war towards the integrity of the Republic of Indonesia. The motivation level of the younger generation is partially the dominant variable that significantly influences the anticipation of the younger generation at the threat of a proxy war on the integrity of the Republic of Indonesia, a variable level of participation does not significantly affect the threat of war proxy. The entire independent variable has a simultaneous influence on the threat of proxy war, it can be seen from F count > F table, the whole independent variable X_1-X_2 affects the threat of war proxy by 43%, the remaining 57% percent is influenced by other variables that have not entered the model. Increasing the role of the younger generation in the face of the threat of proxy war is carried out with a strategy with an input process output approach through: (a) increasing motivation (b) increasing youth participation through learning activities with methods of mentoring or counseling for the younger generation in the academic environment (c) Support The government through the provision of facilities, provision of teaching staff, and partnerships with related parties to strengthen empowerment programs for youth.

8.2 Recommendations

The importance of increasing government support in improving facilities, and establishing a network of partnership with related parties to support the success of youth empowerment programs to produce a young generation who have a strong and intelligent strong character, so as to counteract the proxy war movement that threatens the integrity of the Republic of Indonesia. The importance of community support, and the role of the private sector, as well as the environment, in contributing and participating in the state defense movement with the youth to anticipate the threat of proxy war. Applying the intensity of the method of mentoring to the generation of youth, especially related to training on counseling to defending the country, so that the threat of proxy war on the Republic of Indonesia can be suppressed.

References

[1] Azra A 2015 Ancaman proxy war. *Jurnal Toddopolly.wordpress.com*. Retrieved on August

[2] Gunawan W, and Gunawan H 2017 Proxi War dan Keamanan Nasional Indonesia: Victoria Concordia Cresit *Jurnal Pertahanan dan Bela Negara vol (7) 2*

[3] Mardikanto T 2014 Penyuluhan Pembangunan Pertanian Sebelas Maret Surakarta University Press

[4] Mitzberg, H. and Quin, J. B. 1998. T*he Strategy Process Concept, Context, Cases, 2nd Ed* Englewood Cliffs NJ Prentice HallInternational Inc.

[5] Nurmantyo 2018 Bahaya Proxi war Mahasiswa harus antisipasi tantangan masa depan Retrieved from http://nasional sindonews.wordpress.com on November 17, 2018

[6] Nye J 2004 Soft Power: *The means to Success in World Politic. New York: Public Affairs*

[7] Robins 2014 Organizational Behaviour Global Edition

[8] Wilson E J 2008 Hardpower, Soft power Smart Power *ANNALS of the American Academy of Political and Social Sciences . Issue 616*

Strategy for Prevention of Use of Virtual Currency in Cyber Crime with Government Perspective – IIDSS2019

Mawidyanto Agustian[1], Mohammad Ulir Ro'yi[2] and Nurul Hasani[3]

[123]Badan Siber dan Sandi Negara, Jl. Harsono RM No.70 Ragunan Pasar Minggu, Jakarta Selatan 12250, Indonesia

E-mail: mawidyanto.agustian@bssn.go.id[1], mohammad.ulir@bssn.go.id[2], nurul.hasani@bssn.go.id[3]

Abstract. New technologies drive change in the global economy, including how to exchange goods, services, and assets. The development of money and various payment systems throughout history has helped make exchanges more efficient and safer. An important development in the process of this change was the emergence of virtual currency (VC). The issue of VC that we want to examine in this paper regarding misuse of user privacy, related to privacy and anonymity that can (facilitate) criminal activity, the large number of anonymity provided by the VC system helps prospective cybercriminals to carry out various prohibited activities such as ransomware, tax evasion, under market, and money laundering. VC abuse can occur because it is supported by the ease of transfer of funds and saving transfer fees. Based on the 2018 survey VC document, Indonesia is still in the category of Implicit Banned against VC. Based on the survey the authors say that the government component was still not integrated with responding to the issue of VC abuse in Indonesia. There need to be strategic steps that can be taken from the government's perspective to see this momentum so that financial technology innovations can be optimized by various components of the government.

1. Introduction

New technologies drive change in the global economy, including how to exchange goods, services, and assets. The development of money and various payment systems throughout history has helped make exchanges more efficient and safer. The rapid spread of internet-based trade and cellular technology supported by advances in encryption and network computing has led to the development of several innovative technologies. Companies like Uber and Airbnb have developed radical new business models.

Secure online payment systems (for example, PayPal) and cellular payments and transfer solutions (for example, M-Pesa) change the way in which payments for goods and services are carried out. An important development in the process of this change was the emergence of virtual currency (VC). VC, in principle, questions the currency paradigm supported by the state and the dominant role played by central banks and conventional financial institutions in the operation of the financial system. Currently, VC is issued without state involvement or support. Some VC schemes use distributed ledger technology that provides complete and safe transaction records without using the central registry, therefore this technology allows for direct peer-to-peer transactions and eliminates the need for clearing houses, it is not surprising that private sector interest in this new technology has grown, but the attention of regulators and policymakers are far behind.

The first progress towards VC was made by cryptographic researcher David Chaum, who used tokens that were cryptographically signed. These proposals and subsequently, give significant attention to non-traceable anonymous currencies that are issued centrally and supported by banks or other institutions (which will enjoy a number of trust by users).

Issues regarding VC that we want to examine in this paper regarding abuse of VC User privacy, related to privacy and anonymity that can (Facilitate) Criminal Activity, The large amount of anonymity provided by the VC system helps prospective cybercriminals to carry out various prohibited activities such as ransomware, embezzlement taxes, down market, and money laundering.

VC abuse can occur because it is supported by the ease of transferring funds and saving transfer fees. In addition, the transfer can be done quickly. Based on the 2018 survey VC (cryptocurrency) document, Indonesia is still in the category of Implicit Banned against VC. Based on the survey the authors say that the government component was still not integrated with responding to the issue of VC abuse in Indonesia. There need to be strategic steps that can be taken from the government's perspective to see this momentum so that financial technology innovations can be optimized by various components of the government.

2. Problems

How does Indonesia face the abuse of VC against TPPU and Terrorists based on the Government's perspective as a Regulator?

3. Theoretical foundation

3.1. Virtual Currency

3.1.1. What is a Virtual Currency Virtual Currency is digital money issued by parties other than monetary authority obtained by purchasing, transferring (reward) or mining (the process of producing a number of new virtual currencies, involving complicated mathematical processes). Digital money is issued or controlled by the developer community and used and accepted by members of the virtual community.

3.1.2. Type of Virtual Currency Currently, in the world, there are 1300 types of virtual currencies, but there are only 5 major virtual currencies in the world that are often used for transactions, among others, Bitcoin, Ethereum, Ripple, Bitcoin Cash, Cardano.

3.1.3. Advantages and Weaknesses of Virtual Currency VC advantages:

- You can do transactions using VC whenever and wherever you don't know the limits and without binding rules;
- Transaction costs with VC are lower when compared to transactions with third parties as intermediaries such as financial institutions that have relatively higher transaction costs, especially if they make transactions to different countries.
- You can do every transaction with VC more safely. You will not experience things like counterfeiting money and minimizing the mode of fraud.
- Transactions using VC are transparent because all users without exception can see all information about the VC.
- VC value is not affected by inflation, but is influenced by a large number of requests and offers on the market.
- You can use VC without having to include personal identity, so you tend to be more comfortable in making transactions.

VC Weaknesses:

- VC is still not fully accepted as a currency and means of payment.

- Exchange rates that go up and down can be influenced by the amount of bitcoin in circulation, the number of traders more than users, the presence of various news about VC, and the possibility of hacking.
- VC software continues to develop so that it can experience changes at any time.
- Providing significant opportunities for criminal offenders, caused by transactions that can be carried out without intermediaries so that financial institutions or even the government will experience difficulties in tracking transactions.

3.2. *Money laundering*

Money laundering gets its name from Al Capone 'laundering' money through the laundry. In short, that means making criminal assets appear legal, which all involve hiding the origin of money. This is usually done in three stages:

3.2.1. *Placement:* for example, cash obtained from drug trafficking is stored in a bank account through what is called a money mule.

3.2.2. *Hiding*: money is obscured by transactions such as buying and selling real estate and becoming increasingly difficult to trace.

3.2.3. *Integration*: money cannot be easily traced to crime again and is now used to buy, for example, Ferrari. Criminals have a seemingly legitimate explanation: he got his money in real estate.

3.3. *The Virtual Currency issue is related to Money Laundering and Terrorism*

There are several cases where virtual currency is used as a means of cyber laundering crime. One of them is a case that occurred in 2013, Liberty Reserve, a provider of money transmitting services which claim to be the oldest, safest and most popular online payment system that serves millions of users worldwide. To transfer money using Liberty Reserve, users only need to provide their name, address, and date of birth. But users are not required to authorize their identity.2 Account holders to convert their cash to digital currency provided by Liberty Reserve, an "instant" transfer is made and the digital money is converted back to cash. Every time a transaction the company gets $ 2.99. The United States Department of Justice said that the scheme had been used to process 78 million combined value transactions of up to $ 8 billion related to hiding proceeds from credit card theft, identity fraud, hacking and Ponzi investment schemes, a Ponzi scheme is a mode of investment fraud where the perpetrator pays profits to investors in the form of investor's own money or money paid by the next investor. The Shavers case is the first federal securities fraud case involving Bitcoin.

In 2015, a French man, Mark Karpelès, was arrested and charged with fraud and embezzlement of money. He embezzled money totaling 390 million US dollars (equivalent to Rp.5 trillion) belonging to the Bitcoin currency exchange company, Mt. Gox, which has now been closed.

Case of Terrorist Bombing Alam Sutera Mall. October 2015, Indonesian people were shocked by the bombing of Alam Sutera mall. Leonard Wisnu Kumala, the perpetrator of the bombing of Alam Sutera Mall reportedly threatened and blackmailed mall management by asking for 100 Bitcoin coins equivalent to Rp.300,000,000. Alam Sutera Mall responded by giving only 0.25 Bitcoin, equivalent to Rp. 700 thousand. Annoyed by Alam Sutera's Mall response, which only sent a small portion of its request, Leonard placed a bomb that finally exploded in Mal Alam Sutera's women's toilet.

Case of a Ransomware Virus Attack, WannaCry. Mid-May 2017, a ransomware virus attack, WannaCry, which locks documents from corporate computers and Windows-based government globally. The perpetrator requests a number of ransoms in the form of a Bitcoin currency to return the documents. As reported by Quartz, from the extortion, a total of 101,000 US dollars was collected in the form of Bitcoin sent to hackers. Some of the large organizations that were attacked by the WannaCry virus in Indonesia are the Dharmais Cancer Hospital and Harapan Kita Hospital.

4. Discussion

4.1. Impact of VC Issues in Indonesia related to Money Laundering and Terrorism

Jakarta Chief Executive Officer of Bitcoin Indonesia, Oscar Darmawan, said the online currency of bitcoin is very vulnerable to being used for money laundering. "The possibility of money laundering is huge," Oscar said a while ago when visiting the Tempo office. According to him, since bitcoin was launched in 2009 until now there is no central bank in the world that regulates the circulation of the virtual currency. Central banks in China, the United States, and other countries prohibit the circulation of Bitcoin involving banks. They allow Bitcoin as an investment medium, but not as a measurement standard. "In Indonesia, Bank Indonesia has not regulated and has not banned Bitcoin," All transactions in Bitcoin, said Oscar, are noted that everyone on the internet can see bitcoin user transactions through bitcoin digital wallets. Every bitcoin user has a wallet and can have more than 100 wallets. Then, where is the potential for money laundering? Oscar gave an example, on November 22, 2013, there were 199,993 BTC of transactions from unknown countries. Until now, it was not known who the person was. in transactions, bitcoin users do not necessarily include their real identity. "Usually if someone has a bad intention, the wallet doesn't want to be exposed on the internet," Bitcoin currencies can basically be used for various transactions. For example for legal transactions such as on wordpress.com, virgin galactic airways, republikhost.com, and various social donations such as Wikileaks. But it can also be used for illegal purposes, the portion of which is greater in the international community. Illegal actions include money laundering, gambling, drugs, and even prostitution.

4.2. Conditions of Regulation concerning VC in Indonesia

Virtual currencies present significant and difficult hazards to navigate but can be minimized through comprehensive technology, education, regulatory approvals, insurance, alliances, and risk management. One of the six problems we will reveal is the use of virtual currency in money laundering and acts of terrorist funding. Indonesia should prepare strategic steps to prevent the use of VC from becoming a negative commodity. Based on data obtained through data from the Coordinating Ministry for Economic Affairs of the Republic of Indonesia, Indonesia does not yet have a regulation that manages the existence of VC to be used in Indonesia. This is also reinforced by the results of a study from the RAND Corporation in the Study of the National Security Implication of Virtual Currency, saying that every government in any country must pay attention to the existence of VCs, especially policymakers related to Technology, Counterterrorism, Intelligence, and Law Enforcement.

If you look back in 2018, On January 13, 2018, Bank Indonesia (the Indonesian central bank) released a statement warning against buying, selling, or trading virtual currencies. The statement includes: Bank Indonesia affirms that virtual currencies, including bitcoin, are not recognized as legal tender, therefore they are not allowed to be used for payments in Indonesia. This is in accordance with Law No. 7/2011 concerning Currency, 666 which states that currency is money issued by the Republic of Indonesia and every transaction that has the purpose of payment or other obligations that must be fulfilled by money or other financial transactions carried out within the territory of the Republic of Indonesia must be fulfilled with Rupiah.

The next statement said that ownership of virtual currencies is "very risky," "vulnerable to bubble risk," and "vulnerable to use for money laundering and terrorism funding." Therefore, Bank Indonesia considers that the currency "has the potential to have an impact on financial system stability and cause financial losses to the community." 668 This also refers to Bank Indonesia Regulation No. 18/40 / PBI / 2016 concerning the Implementation of Payment Transaction Processing and Bank Regulations Indonesia No. 19/12 / PBI / 2017 concerning the Implementation of Financial Technology in asserting that, as a payment system authority, the Bank prohibits all payment system operators and financial technology operators in Indonesia from processing transactions using virtual currencies. 671 The statement was supported by the Minister of Finance who, at a press conference on January 23, 2018, warned that virtual currencies are high-risk and speculative investments and said that "we will also continue to function as a government that expresses views that are not in accordance with the law. transaction. The World Bank statement follows a previous press release in 2014, in which it encouraged caution regarding the virtual currency and stated that the views in Law No. 7 of 2012 concerning Currency and Law No.23 of 1999 [673] which has been amended several times, most recently by Law No. 6 of 2009, [674] Bank Indonesia states that bitcoin and other virtual currencies are not currencies or legal payment instruments in Indonesia.

4.3. Strategies offered related to VC issues in Indonesia

We have seen that with VC there is no opportunity to benefit in Indonesia, however, the shared concern that will occur is that VC is not used as a means of payment but as an asset exchanged between interested parties in its efforts to disrupt the stability of the political economy and national defense. lifting how prevention strategies are appointed by the author from a government perspective, by strengthening the joints that intersect with the VC itself. The financial era that is supported by digital technology is minimal financial transactions with face-to-face processes, loan applications, and various financial assistance facilities that can be done at this time. This can also be done between cities, between provinces and even between countries. With the support of a complex system in operation between financial service provider sectors, VC also saves the potential vulnerability that was mentioned at the beginning of this paper. But again VC offers an investment position that promises to collectors, which we cannot know about them business background and activities are undertaken.

Authors who see this problem from a position as a government or regulator, where its presence guarantees the community inevitably the presence of VC in Indonesia. The author feels that the existence of a concocted strategy is expected to guarantee the existence of VC in Indonesia and anyone who will later abuse it will be able to be dealt with decisively.

SMART Regulation by prioritizing 4 main principles in its application, among others :

- Shared Responsibility
- Rules Of Law and Creating Legal Clarity
- Flexibility to Accommodate New Technology
- Fairness and Transparency

With four (4) principle points that must be supported by the objectives and intentions that must be understood by policy stakeholders, among others, regulations that will be compiled and implemented do not impose the components of the regulator itself. Or in other words, every policy and regulation issued by each regulator does not tangle one another. In addition, regulations that are present in the VC ecosystem are able to facilitate positive business, not to hinder the digital economic ecosystem, but also to be able to detect and minimize risks from. Abuse of VC. The last point is the need for special attention to periodically evaluate each of the VC regulations and policies and the entire evaluation mechanism can be made as easy as possible.

After with clear principles, accompanied by the aims and objectives of the strategy, then the next is how to apply it in the world of bureaucracy and cooperation between lines of government. The author details in the following steps :

- *How To Proceed How Much Uniformity Is Necessary*
  The importance and urgency of uniformity of understanding and translation of VCs in a policy, sitting in a Joint forum is one of the right commitments to establish an appropriate and targeted component of policy for current or future VC stakeholders.

- *More Harmonization Or Cohesion Policy Is Vital*
  Harmonization and integration between the policies and regulations that were born by the units in the government will be able to recognize threats and potential threats from VC, but also not exclude the benefits of VC that can be explored into the digital economy community in Indonesia.

- *Public, Private, Civic Stakeholders Partnership*
  The last is no less important role Together from every business sector that will later use, develop VC, both from the technological aspects, the media and the form of the VC

must build good cooperation and mutual benefit from each other.

5. Conclusion

From the perspective of the writer who has elaborated on how VC develops, as well as the threat of abuse that may arise and finally how the strategies that can be present in preventing VC abuse in Indonesia, it can be conveyed in the following main pointers :

5.1. There needs to be a SMART Regulation that is understood by each line of stakeholders and regulations by prioritizing 4 main principles SMART Regulation by prioritizing four (4) main principles in its application including :

- Shared Responsibility
- Rules Of Law and Creating Legal Clarity
- Flexibility to Accommodate New Technology
- Fairness and Transparency

5.2. In the implementation of SMART REGULATION, three (3) strategic steps were carried out, among others :

- *How To Proceed How Much Uniformity Is Necessary.*

  The importance and urgency of uniformity of understanding and translation of VCs in a policy, sitting in a Joint forum is one of the right commitments to establish an appropriate and targeted component of policy for current or future VC stakeholders.

- *More Harmonization Or Cohesion Policy Is Vital.*

  Harmonization and integration between the policies and regulations that were born by the units in the government will be able to recognize threats and potential threats from VC, but also not exclude the benefits of VC that can be explored the digital economy community in Indonesia.

- *Public, Private, Civic Stakeholders Partnership.*

  The last is no less important role Together from every business sector that will later use, develop VC, both from the technological aspects, the media and the form of the VC must build good cooperation and mutual benefit from each other.

Thus this paper was made as a means of contributing to the community and stakeholders in responding to changes in the use of VC in the digital financial era (Economic Digital Movement).

Acknowledgments

Authors wishing to acknowledge assistance or encouragement from colleagues, special work by technical staff or financial support from organizations should do so in an unnumbered Acknowledgments section immediately following the last numbered section of the paper.

References

[1] Joshua Baron, Angela O'Mahony, David Manheim, Cynthia Dion-Schwarz RAND_1231: National Security Implication Of Virtual Currency; Examining Potential Of Non-State Actor Deployment, 2015.

[2] Bank Indonesia Regulation Number 18/40 / PBI / 2016 concerning the Implementation of Payment Transaction Processing, http://www.bi.go.id/id/peraturan/sistem-pembayaran/Documents/PBI_184016.pdf (in Indonesian), archived at https: //perma.cc/JBX8-44U7

[3] Minister of Finance: Bitcoin is Not in Line with the Law, MINISTRY OF FINANCE, (Jan. 25, 2018), https://www.kemenkeu.go.id/en/publications/news/minister-of -finance-bitcoin-is-not-in-line-with- law /, archived at https://perma.cc/3MEJ-HHUP

[4] Act No. 23 of 199 Bank Indonesia Concerning, http://www.bi.go.id/en/tentang-bi/uu-bi/Documents/act2399.pdf (unofficial English translation), archived at https://perma.cc/ 6S8P-FFZH

[5] Act No. 6 of 2009 Concerning Stipulation of Government Regulation in Lieu of Act No. 2 of 2008 Concerning Second Amendment to the Act No. 23 of 1999 Concerning Bank Indonesia into Act, http://www.bi.go.id/en/tentang- bi / uu-bi / Documents / BIact_0609.pdf (unofficial English translation), archived at https: // perma. cc / FRZ5-ZZG5

[6] Press Release, Bank Indonesia, Statement of Bank Indonesia Related to Bitcoin and Other Virtual Currency (Feb. 6, 2014), http://www.bi.go.id/en/ruang-media/siaran-pers/Pages/SP_160614 .aspx, archived at https://perma.cc/3MEJ-HHUP.

Papua Youth in Mindset Threat
(Cyber Propaganda 4.0 and Defense Strategy 5.0)

Steve Rick Elson Mara

Afiiliation : Indonesia Defense University, Bogor West Java 16810, Indonesia

E-mail : stevericelsmara@gmail.com

Abstract. The young generation of Indonesia or often referred to as generation Y is the future generation of the Indonesian nation. Generation Y currently faces many threats both from domestic and abroad. The threat of mindset changes is one of the biggest challenges currently faced by youth in Papua. This threat is increasingly evident through propaganda by certain parties to change the mindset of young Papuans who oppose Indonesia's integrity. This is a challenge for the government to develop a defense strategy in the face of this threat. Defense strategy itself is very important for the existence of a country. So it is necessary to have a calibration of the concept of defense strategy in the face of the threat of propaganda in the era of 4.0 carried out by the Indonesian government especially through the ministry of defense. This article will contain the generation Y in Papua in the face of the threat of a mindset and a study of Indonesia's national defense system and a calibration of defense strategies to become a strategy for defense against the threat of a mindset. This paper use the method of literatur study and get the data from book, jurnal, and internet then make some comparison to get maximum result. As a result, this paper will provide information about variables that are emphasized in the national defense system, the threat of minnets experienced in Indonesia.

Introduction

In the life of nation and state, the Defense System is very fundamental. The defense system is the main factor for the existence of a country. If a country is unable to defend itself against various threats that come from within and outside the country it means that the country fails to maintain its existence.

Indonesia has a defense system prepared by considering sharing factors in the development of the strategic environment and geographical conditions, domestic and foreign politics, culture, economic conditions and social welfare in the country. Indonesia's defense system is a universal defense system. Literally, the universal defense system is a system that involves all Indonesian citizens in accordance with their roles and functions which are based on the value of love for the homeland. The Indonesian defense recorded in the Indonesian defense white paper in 2015 states that the universal defense system has 3 (three) main features, namely: Population, Equality, and territoriality that involve all components.

"Indonesian state defense is held in a universal defense system. The form of defense developed involves all citizens, regions, all national resources and infrastructure, prepared early by the Government, and organized in a total, integrated, directed and continuous manner "[1].

There are 3 components in the national defense system, namely: Main components, backup components and supporting components. While the threat itself is divided into three spectrums, namely military threats and non-military threats and hybrid threats (a combination of military and non-military threats). If the threat that comes is a military threat, then the main component to deal with the threat is the military and the backup is non-military. Meanwhile, if the threat that comes is a non-military threat then the main component is non-military and the supporting component is the military.

In the characteristics of Indonesia's national defense which is of course certainly the Indonesian defense system involves the Youth as Agent of Defense. If observed the threat of threats today is an unconventional threat, where non-military threats are more likely to occur than military threats such as direct war that occurred in World War 1 and World War 2. Industrial development 4.0 has also changed the dimensions of Cyber threats, wars are carried out in cyberspace by using technology as the main weapon. This encourages state defense education to continue to be carried out at various levels of society, especially for youth. Propaganda is currently one of the real threats that occur in Papua. Propaganda is done as a cyber crime to turn the mindset into a national disintegration mindset.

2. Discussion

2.1 Industrial Revolution From Time to Time

Of course industrial development is inseparable from technology. This is clearly seen when there are technological developments there will be industrial development. Technology and Industry are 2 different fields but present to influence each other.

The industrial revolution first entered industry 1.0 in 1784, and that resulted in changes in several fields such as agriculture, manufacturing, mining, transportation. The first time it happened in the United Kingdom and then spread to other parts of the world. It started with a Steam engine, and then applied for the sake of production.

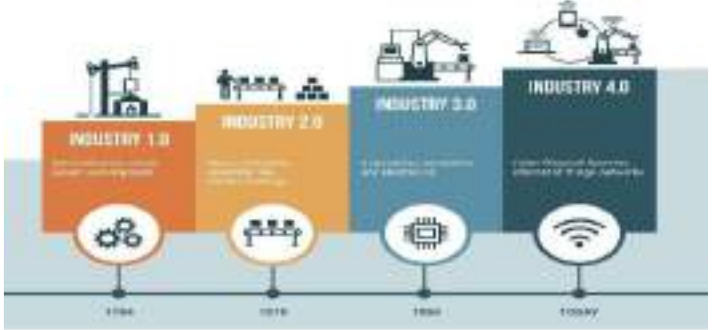


Figure 1.
Source: Global Uncertainties in Digital Era: Issues, Challenges, and Policies, Dean, School of Management and Administrative Sciences Chair, Department of Economics, 2018. Dikutip dari website Bank Indonesia

The development of the industrial revolution 2.0 began in 1870, marked by technological developments gaining momentum with the development of steam-powered and rail boats and continuing to burnt engines and power plants. Industrial Revolution 3.0 in 1969 when the use of computers and electronic devices began to be used in various parts of the world to communicate.

At present, the industrial revolution is entering a higher point, namely the Industrial Revolution 4.0 where the use of internet networks is very high, the increase in the use of syber and access to information is very easy to obtain. This is certainly a challenge for every country, where industrial development has brought the country into an era of unlimited openness and everything can be easily accessed.

As well as other developing technological developments such as automated robots, syber security, System Integration, and Simulation. This revolution has had a positive impact but also a negative impact on the existence and sovereignty of a country. The threat to a country is through crime such as Cyber Warfare. This threat is categorized as a non-military threat and a real threat currently faced by the Indonesian people.

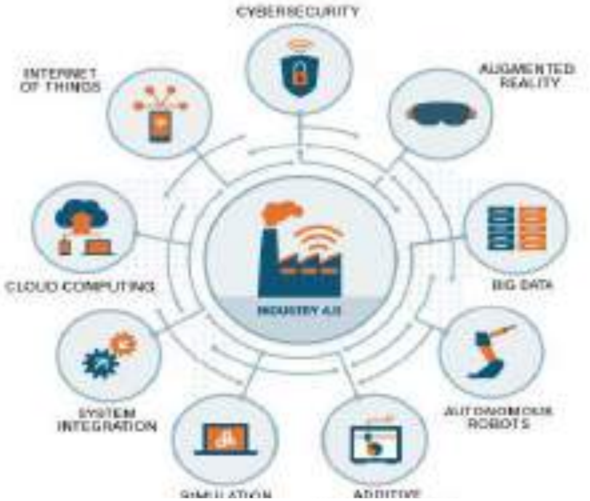
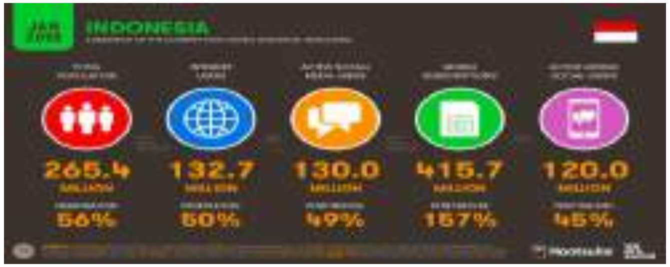


Figure 2.
Source : "Prospects and Challenges of Digital Technology in Indonesia: A socioeconomic perspective", CSIS 2018 dikutip dari website Bank Indoesia, 2018

2.2 Generasi Y in The Grip Cyber Propaganda 4.0

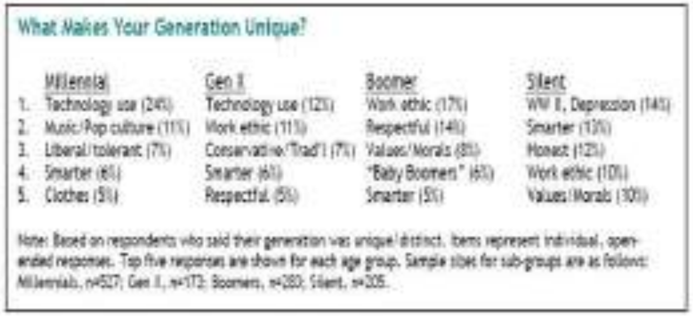
Changes that occur in the era of globalization also threaten the sovereignty of a country, it is caused by the many new ideas that come from outside the country then



penetrate the thinking of the people. The ideas that come are often in conflict with the values that apply in a nation state. At present the Indonesian government is anxious about the tendency for the development of trans-national culture in the younger generation which is feared that nationalism will decline. Indonesian people, especially Indonesian youth, are more globally aware than nationally aware, this is evidenced by the use of social media.

Figure 3. The Country's Key Digital Statistical Indicators

The data in the table (above) is the result of research conducted by *We Are Social* in collaboration with *Hootsuite*. Based on these data, Pupolasi Indonesia reached 265.4 million, while internet users in Indonesia reached 132.7 million. When viewed from internet users, it can be said that all internet users in Indonesia also access social media[2].



What Makes Your Generation Unique?

	Millennial	Gen X	Boomer	Silent
1.	Technology use (24%)	Technology use (12%)	Work ethic (17%)	WW II, Depression (14%)
2.	Music/Pop culture (11%)	Work ethic (11%)	Respectful (14%)	Smarter (13%)
3.	Liberal/tolerant (7%)	Conservative/Trad'l (7%)	Values/Morals (8%)	Honest (12%)
4.	Smarter (6%)	Smarter (6%)	"Baby Boomers" (6%)	Work ethic (10%)
5.	Clothes (5%)	Respectful (5%)	Smarter (5%)	Values/Morals (10%)

Note: Based on respondents who said their generation was unique/distinct. Items represent individual, open-ended responses. Top five responses are shown for each age group. Sample sizes for sub-groups are as follows: Millennials, n=527; Gen X, n=173; Boomers, n=283; Silent, n=205.

Figure 4. What Makes Your Generation Unique?

Millennial generation, or generation Y, is a generation born from 1980 to 2000, so that what is referred to as the milineal generation is currently in the age range of 19-38 years. When compared with several previous generations Gen X, Boomer, and Silent. then the millennial generation has a unique tendency. Millennials are more interested in using technology, especially internet usage. The need for internet users is mentioned as a basic requirement of this generation.

In a survey conducted by the Alvara Research Center (table above) in 2014, the millennial generation preferred the topics of music, sports, technology, and only a few were mature people who liked social, political and economic talks[3].

Based on data from We Are Social in collaboration with Hootsuite and compared with data from the alvara Research Center which states that 132.7 million Indonesians are active internet users and millennials prefer technology. So the authors conclude that Indonesian youth today is a generation of technological literacy and are in the grip of propaganda 4.0 which is done to change the nation's mindset of integration. Propaganda 4.0 is propaganda carried out through internet networks to form the mindset of the younger generation. Propaganda carried out in Papua is one of the threats of national disintegration because it is carried out by disseminating messages and images of support for independent Papuans coming from abroad. Like the example image below that can be easily accessed on the internet and distributed via social media like whatsapp and facebook :

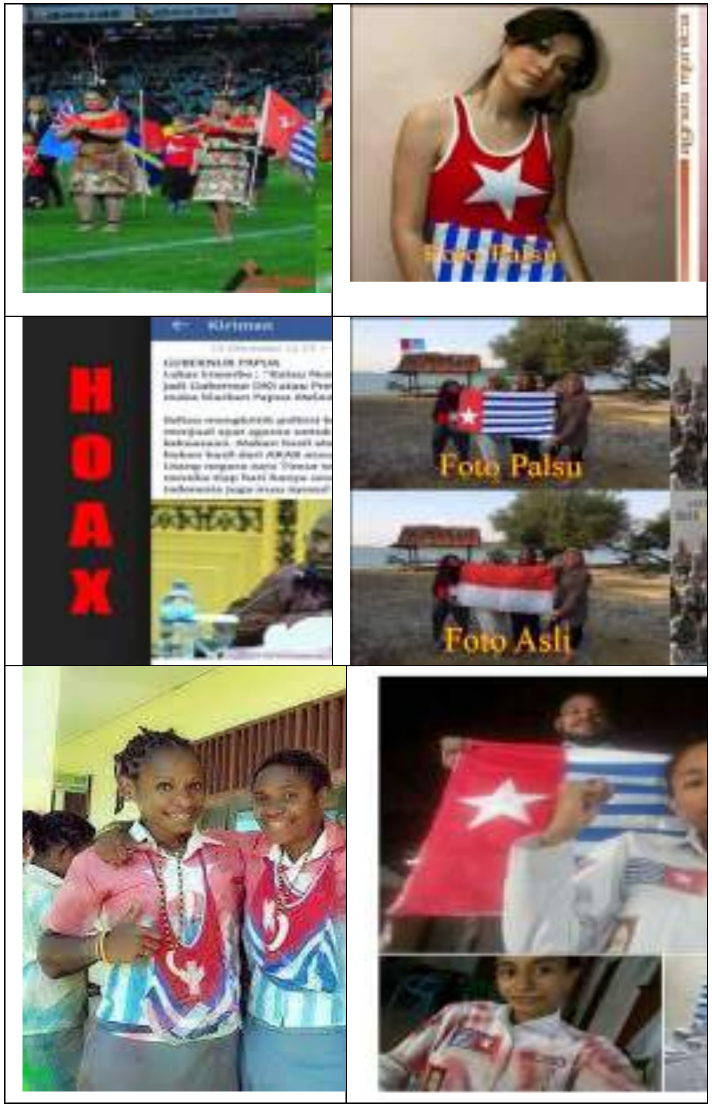


Figure 5. Example photos

The writer said that This propaganda as a proganda 4.0 because it was done through a massive internet network to change the mindset of the young generation of Papua and make a categorization of US vs Them. This is done by generation Y that we are not them and they are not us, they are our enemies and we are demons to them. The results of 4.0 propaganda have formed a national disintegration mindset by describing the Papuan flag on school clothes, can be seen in the picture above.

2.3 The Role of Young People 4.0 In the 5.0 National Defense System

In development, the younger generation is demanded to face every revolution that occurs. Indonesian youth in the universal defense system are also required to face threats that come from within the country and abroad. So that Youth must be a point of movement in the national defense system. The role of the young generation must be re-optimized through the education of state defense cadres carried out by the Indonesian Ministry of Defense in order to create an attitude of love for the homeland and be willing to sacrifice for the nation.

The role of youth 4.0 can also be formed through the dissemination of positive content through internet technology in the form of literacy about awareness of the nation and state. Planting a patriotic soul defending the country as one of the bases for having the initial ability to defend the country. In addition, the planting of 4 national consensus values, namely: Pancasila, UUD 1945, NKRI, and Bhineka Tunggal Ika are also important to do in improving the integrity of youth.

Youth 4.0 also have to have the skills to be creative and innovative, think creatively, communicate, and collaborate to increase positive activities. If the role of the youth is optimal then the national defense system, namely the universal defense system will be stronger and the interests of the nation will be more optimal to run in achieving national goals. This is in line with the 4 pillars of Indonesia's development direction in 2045, namely: (1). Human development and mastery of science and technology, (2). Sustainable Economic Development, (3). Fair development, (4). Strengthening resilience and National Government.

The solution that the writer gives is to calibrate the national defense system that was made 20 years ago into a defense strategy 5.0. Industrial Revolution 5.0 has the concept of two waves, the first wave has been used in industrial revolution 4.0, which is very massive internet use, while the second wave is to restore human glory. If the two waves are collaborated, then it will combine physical, digital and biological and be equipped with a spiritual presence.

If the calibration concept planned by the minister of defense, namely: "returning the compass direction to zero" is done by paying attention to wave 5.0, it will become a force to change the archipelago, by returning the values of past struggles and enthusiasm to give special pride to identity archipelago. This is key in facing the threat of a mindset. If youth in Papua can easily be influenced by propaganda, then with a defense system 5.0, Papuan youth can return to their mainsets to feel more of having Indonesia as a whole

3. Overview

4.0 young people have a very fundamental role in the national defense system. Especially in the 4.0 Industrial Revolution Youth have an important role in facing threats. However, Youth is also a victim of the threat of a mindset carried out through cyber propaganda to change the mindset of integration into disintegration.

In dealing with these threats, the Government through the Ministry of Defense needs to carry out a calibration of the concept of national defense which was made in the past into a defense strategy concept 5.0. the concept consisting of two waves will again shape the mindset of Indonesian youth in Papua as a statesman who respects the noble values of the nation and the identity of the archipelago. with the skills possessed by youth 4.0, the defense system will run more optimally and Indonesia will run brilliantly towards the direction of development in 2045.

References

[1] Kementerian Pertahanan, Buku Putih Pertahanan Indonesia, 2015

[2] https://inet.detik.com/cyberlife/d-3912429/130-juta-orang-indonesia-tercatat-aktif-di-medsos. Haryanto Agus, 130 Juta Orang Indonesia tercatat aktif menggunakan media sosial, 2018

[3] Generasi milenial, tantangan dan peluang http://alvara-strategic.com/generasi-millennial-indonesia-tantangan-dan-peluang-pemuda-indonesia. diakses pada tanggal 05 April 2019, Pukul 17:48

[4] Cecep Darmawan, " Pendidikan Bela Neagara dalam Konteks Keamanan Nasional", dalam muradi (ed), penataan kebijakan keamanan nasional, (bandung: Dian Cipta, 2013)

[5] Indrawan Jerry "Jurnal Pertananaan dan Bela Negara" , Membangun Komponenn Pertahanan berbasis kemampuan bela negara sebagai kekuatan

pertahanana Indonesia menngghadapi ancaman nir-militer, UniversItas Pertahanaan, (Agustus, 2012)

Soft Power Approach to Overcome Radicalism and Extremism in Indonesia – IIDSS2019

Yulia Fadillah[1]

[1] Indonesia Defense University, Bogor 43210, Indonesia

E-mail: yuliafadillah27@gmail.com

Abstract. Radicalism and extremism are understandings of direct individuals act on terror. Radicalism and extremism began to be created as a tool to incorporate the ideology of terror into society. Therefore, in tackling and counteracting terrorism in Indonesia, it is necessary to consider counter-radical and deradicalization actions that are submitted to the social system in communities that are vulnerable to radicalism. This paper will discuss the Indonesian government's strategies through the National Agency for Combating Terrorism to overcome radicalism and extremism through the soft power approach. The soft power approach is then used to shift radical and extreme understandings so as not to follow-up with violence as the root of terrorism. The social dominance theory in this study will be used to analyze individual changes as part of the dominance social system to be given the deradicalization and counter radicalisation treatment. The soft power approach concept will be used to analyze modern government strategies in counteracting and overcoming terrorism into the society and militants that will be introduced globally.

1. Introduction

The 9/11 tragedy became the beginning of the terrorism phrase to be known and evolved as a terrorist act based on religion to attack the state's sovereignty and spread the fear in society. The global war against terrorism is a signal of the open war existence of open war between countries in the world as a form of escalation of conflict against acts of terrorism that justifies the US invasion of the Middle East to overcome terrorism which is assumed to originate from the Middle East.[1] Since 2001 (the 9/11 terror attack) acts of terror against society have created global fear and Islamophobia in the midst of the social system of society. The community shows its choice to stay away from Muslims and condemn acts of terror which most claim to be Muslims to ask for Westernization by the West. Priority after serving terror in Indonesia as a continuation of 9/11.

Bombing terror in Indonesia begins with the Bali Bombing 1 tragedy conducted by Imam Samudra who joined Jamaah Islamiyah (JI) as an affiliate of the Al-Qaeda network in 2002. This terrorist attack was carried out under the pretext that westernization was being carried out even though Indonesia is dominated by Moslem. He argued that the character of contemporary jihad had transformed conflict no longer between Moslems and Non-Moslems but became the United States and Israel as objects of attack.[2] Regarding that, everything that is closely related to the United States or Israel, it will be the target to be moved by global westernization. This then began as a demand to make Indonesia an Islamic state that supported the agenda of Al-Qaeda's global jihad to gather global Muslim forces.

The demands of the establishment of the Indonesian Islamic State and anti-westernization were then ended with the Bali Bombing 2 in 2005, which was a series of bombs made by themselves to provide a tourist spot for Westerners. Although the scale of the Damage and Victims of Bali Bombing 2 is not the same as the Bali Bombing 1, but the scale of the community increases along with the increasing number of foreign tourists to Bali and other tourist objects in Indonesia. The escalation of terror then escalated by launching a suicide bombing at JW Mariot Hotel, Ritz Charlton Hotel, Kuningan, and the Jakarta Stock Exchange.[3] The movement of Jamaah Islamiyah is increasingly widespread and developing along with the development of technology and information making it easier for JI to recruit, especially among young people. This shows that JI is a dynamic development that is able to instill radical ideology for young people with various challenges that occur in the territory of Indonesia. The growth of Islamic radical groups increased with the emergence of Jamaah Ansharut Tauhid (JAT), Laskar Jihad, and Mujahidin Indonesia Timur (MIT).[4] These groups increased the escalation of radicalism in Indonesia which threatened the government because it spreads its understanding to young people and students.

The threat of terrorism in Indonesia began to develop more by diverting ISIS as a new actor in the issue of global terror. ISIS then launched its influence in Indonesia through the spread of fundamental and radical Islamic ideologies by the Faksi (Islamic Shari'a Activist Forum). The ISIS movement has the basic goal of purifying Islam in the world through the establishment of the Islamic

Khilafah in Syria and Iraq. The movement of ISIS in Indonesia was carried out through radical penetration in youth groups and campus areas so that religious-based groups and organizations emerged that were stated that the Pancasila is *thogut* thus reject the concept of the NKRI (Negara Kesatuan Republik Indonesia). Especially with the expansion of *takfiri* doctrine with the concept of *tauhid* which considers everything that is contrary to their understanding can be destroyed in the context of *hijrah*.[5] This is what raise the challenges because of the radical notions that are widely disseminated to youth, so that they can triggered radicalism and extremism that lead violence's acts. ISIS is an advanced form of old Islamic radical with a new label because ISIS also makes Moslems as enemies and targets if they do not agree and don't have similar understanding about Islam also *jihad* with them. ISIS considers Islamic groups outside of them is not Islam so they must be combated, thrown out, and destroyed.

A series of bombings that occurred in Indonesia proved that there was a degradation of the Indonesian national security with the freedom of radical groups to influence the social system of Indonesian. Radical and extreme notions related to terrorism are not only a means to achieve demands on westerinization and the government, but are made instruments of self-existence to facilitate and increase their influence in society.

2. Concept and Theory

2.1. Social Dominance Theory

Radical and extreme actions are based on the belief that individuals and groups are the most correct and dominant. This understanding is justified on the basis that the group becomes dominant in quantity and views on a concept of truth itself according to its thoughts, as expressed by the social dominance theory. The social dominance theory shows that every person and group in society, inherently, has a tendency to form hierarchies in society. The hierarchy will be built and maintained through various forms of oppression and discrimination, such as ethnocentrism, sexism, racism, and nationalism in society.[6] The basic postulate of social domination theory is oppression, discrimination, and inter-group prejudice which is a community structure strategy to regulate the system of social order by forming a hierarchy based on the groups within the system.[7] The social dominance theory also emphasizes that the attitudes that individuals have towards the spread of social ideologies, policies related to social groups, and about social groups themselves, will be influenced by how much the individual's preference for group domination and social inequality in general. In this case, social dominance theory is demonstrated through the existence of social domination orientation as a form of impression of oppression feeling so that the tendency to do the same thing is very high through racism, sexism, support for aggression (war), prejudice, anti-egalitarian and discriminatory behavior.

The social dominance theory shows that terrorism uses the spread of radicalism and extremism to mobilize the masses to have the same ideologies like them. Deployment targets are mapped through stability analysis in the community based on psychological and culture conditions. Terrorism shows their tendency as the dominant oppressed group, in this case it can be mapped that terrorists consider themselves to be the dominant Moslem group in the Middle East and some countries in the world but feel oppressed by westernization so that they cannot grow and develop as other non-Muslim groups.

2.2. Soft Power Approach

Counter-terrorism since the 9/11 tragedy has always been overcome through military action or hard power. The use of hard power is intended for law enforcement that has significant achievements. However, it is considered not to be a long-term solution because it is compelling and is considered irrelevant in responding the current dynamics global constellation. Therefore, the concept of soft power began to be used in providing long-term resolution and reduce threats not to follow by violence act.

Soft power approach is the anti-thesis of hard power with actions through armed and military forces. The soft power approach is introduced by Joseph Nye as a concept to observe the contemporary international relation constellation which is no longer concentrated in military aspect only. The soft power approach is more than just persuasion or the ability to order others using the power of arguments. The soft power approach is the ability to make other parties interested so they will give his consent as means as willingness to accept.[8] Psychologically the party those treated by soft power approach does not realize that if there were being controlled by the soft power approach, it would depends on the ability of the state, group or individual to organize the agenda of issues related to the concept of culture, institutions and even ideology. The concept of soft power approach with culture shows the existence of a cultural orientation that becomes a basic value in society so that emotional and psychological attachments are the target. The soft power approach concept using institutions to show the orientation of individuals or groups with feelings of ownership and loyalty. Whereas soft power approach uses ideology is an approach by moving and shifting understanding rooted through understanding of attitudes, characters and actions. In this case, the soft power approach model used is soft power approach with ideology as a basic concept in the form of deradicalization.

Deradicalization becomes a strategy based on conceptual understanding to deal with problems related to the development of ideologies and radical acts.[9] Deradicalization which means de-ideologization is a program aimed at all levels of society, especially those who are vulnerable to radical and extreme ideologies. Indicators of the success of deradicalization can be seen through the growth of the ability to detect and prevent the threat and danger as early as possible that spread by radical leaders, supporters or sympathizers, conventionally or using social media as part of rapidly information technology growth.

3. Discussion

Terrorism is an action that is always synonymous with terror, violence, extremism and intimidation, so that it often creates negative consequences. Every terrorist always connect their actions as jihad because acts of terrorism are still a stigma that is an act by Muslims to form a global Khilafah Islam. The act of jihad is then interpreted independently as a form of degrading, humiliating the enemies of Islam and terrorizing them. This can also be seen from the statement of Imam Samudra, who acknowledged that Islam forbids killing women and children, obedient parents and Muslims, is also prohibited from destroying property. However, he stressed that this prohibition only applies when the enemy does not commit a similar violation.[10] In defense, Imam argues that the United States and its allies are responsible for the deaths of thousands civilians Moslem in Iraq, Afghanistan, Kashmir and other locations. Religious identity forms the basis of terrorism movements and acts as a form of defense against humanity.

Religion is not only related to peace, but also violence. It becomes a dichotomy when religion is used as an ideological foundation and symbolic justification for acts of violence perpetrated by terrorists. The function of religion as an ideology becomes a society unifier as a form of religious meaning to human relations, social systems and God. In this function, religion becomes a unifier in the social system of society because it provides a framework of interpretation in the meaning of relations between humans, thus the extent to which social order is considered as the religious representation as desired by God.[11] Furthermore, this unifying function can produce many contradictions, especially concerning issues of injustice and inequality that lead to acts of violence through religious identities. So that religion is specifically identified and attached in certain individuals or groups that provide stability, status, view on life, ways of thinking, ethos and so on. It can crystallize if it is associated with other identities such as gender, ethnicity or nationality that have the potential to produce a dichotomy due to ethical, groups, and nations conflicts that can lead to violences, including religious variables. Religion can be the legitimacy of relations between humans, so this is the basis of the dichotomy of terrorists who separate themselves from others while having the same religion, but are considered different because they are not part of their group. Religion which is used as an ideology directs the actions and treatment of terrorists towards violence as a form of legitimacy for their dominant social identity.

Along with its growth, terrorism began to use soft approach to spread influence and ideology in society. The existence of ISIS which has become a real threat in international security constellation shifts their threats and disturbances to the threat of radicalism and extremism which spread by sympathizers and militant groups after obtaining education in Syria, Iran and other countries in the Middle East. Not to mention the arrival of immigrants and migrants from Middle Eastern countries to Indonesia who spread their ideology amid the social system of society under the guise of religion.

Radical Islamic groups spread their ideology to form opinions in the community that their groups are the dominant group with the most correct truth values among other Moslem groups. So if the community does not participate in the group it is considered a part of the minority who must be embraced to become dominant like them.[12] The dominance of groups hierarchically requires more attention from the government, when the government is unable to accommodate their interests, the government has neglected and ignored them for taking care of other groups that have been declared radically incorrect. So that the government is included in the object that must be attacked. It is become the concern of deradicalization to shift the notion of hierarchical dominance towards what should be in accordance with the values of nation state. Subjects exposed to radical understandings of social domination were given deradicalization treatment for penetration so that the presence of the people as part of a sovereign state is constitutionally absolute with the same rights and obligations, regardless of race, class, ethnicity or religion. Deradicalization rooted in the notion that human beings with their human rights will be respected and protected by the state, so that the values of their beliefs become a personal basis that is respected without the formation of a social hierarchy in society. Thus, the concept of domination is biased because everyone has the same values in the eyes of law and constitution as well as beings have faith.

The existence of a social hierarchy formed through radical Islamicism shows a tendency that a social system based on hierarchy gives legitimacy to form moral and intellectual truths. The moral truth then gives confidence in persecuting certain groups with their groups. So that even though Islam is the basis of their beliefs, but the social hierarchy system that is formed does not make the religious value as guideline, even the hierarchy forms its own ideology in evaluating the social conditions in society. This shows that terrorism forms a new understanding by incorporating religious values from Islam to penetrate in achieving its power on the basis of the Khilafah. Even though Islam itself clearly states that every human being has the same value in the eyes of God and the obligation of every individual to protect each other and is not justified to use violence.

Radicalism is an understanding or sect which requires drastic change in the form of fundamental reform.[13] Radicalism directs individual thoughts to act with violence and coercion orientation. Radicalism in this case is a movement based on religion that seeks to overhaul the social and political order by using violence. Radicalism in the act of terrorism seeks to provide a radical understanding of state, government and social order based on religious values in this case is Islam. Radicalism rooted the understanding of Islam in statehood, so politics must be based on Islamic law. The state system that is not based on Islam is the *thogut*, so the Indonesian Government based on Pancasila is the target to be fought. Even though, Pancasila has accommodated religious values that are recognized and protected by the state. This can cause social system instability in the community because of the clash of thoughts which if neglected will lead to violence and terrorism acts. While extremism is an excessive view of an object or something that leads to extreme and radical actions.[14] Religious extremism is usually shown through hate speech which aims to show that those who are not part of the group are wrong and misguided. More extreme actions are taken using the media so that the spread process is more massive. So that the media become the main instrument in extremism so that the goal can be effectively achieved. The overcoming of religious extremism is still considered relativly because its form is still in the realm of information, communication and technology. So that the law in Indonesia still enforces the use of technology and information in religious extremism through the ITE law (Information, Technology and Electronics). So that in general, government policies towards extremism are accommodated through overcoming radicalism, because religious extremism will directs to radicalism and acts of violence in the basis of radicalism.

Radicalism and extremism are the alterations of terrorist strategies in giving the concept of *jihad* to individuals and groups. Radicalism and extremism are genealogical actions for the game of power in achieving its goal of establishing the Khilafahan Islam in Indonesia by opposing the government's system. Radicalism and extremism attack the vulnerability of unstable societies both culturally, educationally and prosperitically so that such communities are the main targets. Therefore, the government through BNPT (National Counterterrorism Agency of Indonesia) in collaboration with the private sector, in this case the social and religious based foundation, made a soft power approach to shift radical and extreme behavior so as not to lead to violence as a form of deterrence and overcome the terrorism in Indonesia.[15] This is used as a state foundation to accommodate the orientation of terrorism that have robbed citizens right by using soft methods, because in the right of individuals to freely ask for the Khilafah Islam from the government through violence acts, there are state rights which accommodate the rights of millions Indonesian citizens seized in them.

Soft power approach is carried out through a religious, cultural and ideological approach so that the radical notions inherent in potential terrorists can be directed not end in violence. The soft power approach model used by BPNT combines the values of Indonesian nationality and culture by adjusting the background of subjects who will be given deradicalization treatment.[16] BNPT works with various private parties as an integral part of deradicalization programs that have a psychologically adaptive approach. The approach which will be given is accommodated by expert groups religiously, culturally, socially and psychologically so that the subjects do not feel they are being given deradicalization treatment. The main objective of the deradicalization program through the soft power approach approach is counter terrorist strategies through the inlet of radicalism in their mind. So that the program's strategy is specifically limited to directing radical and extremes notions in society so that they are directed to the general social systems not to lead of violence acts.

Deradicalization with the concept of soft power approach reduces the belief of the subject (prospective terrorist) as the dominant and most correct group of its belief. The subject's desire to continue his actions towards violence is reduced not to join the hierarchy of dichotomies of the dominant group in general. The soft power approach gives a soft treatment so that the subject does not feel interrogated in depressed to make it becomes a psychological justification for fighting against the government as a result of injustice to his treatment.[17] This is inseparable from the fact that efforts to define terrorism cannot be separated from various interests, including ideological and political interests to create global justification in providing spaces of its movement. Nevertheless, the definition of terrorism is quite important, not only for academic purposes, but also for practical purposes on how to overcome it. Combating organized terrorism is having to have clarity about the defining the organizations itself are includes terrorists or not. Such clarity must of course come from clear definitions. Without clarity the efforts to combat it can have counter-productive effects. So the definition of terrorism must be very carefully understood not to be an instrument of propaganda. Therefore, it is important to provide a clear definition of terrorism by government in order to design appropriate sentences in law for terrorists.

The soft power approach process is carried out intensively through effective communication with various religious leaders, the community and social and psychological leaders. The soft power approach coordinates with the private sector as a productive form so that subjects do not feel the involvement of the state as an inherent part of opposing their movements. The state positions itself as part in accommodating social and economic problems so that its citizens do not feel abandoned and ignored. This feeling is psychologically built through cultural and religious values that explicitly show the role and function of the state towards its people.

Indonesia's deradicalization model then began to show significant results, especially in an effort to respect the right of potential terrorists who want to being part of the Indonesian again. Through deradicalization, the government provides opportunities for prospective terrorists who have realized that they have made a mistake with their actions to become terrorists to be accepted again in their environment and uphold the values of the Pancasila as a guideline for nation state of Indonesia. Through bilateral, regional and even multilateral cooperation, Indonesia starts introduce soft power approach strategies to the international system as a strategy to shift counter-terrorism from military to non-military methods. Indonesia even received several visits from Japan and the Vatican and signed an MoU with Australia and Morocco regarding strategies to deal with radicalism and extremism with violence that led to acts of terrorism.[18] This shows that Indonesia began to build confidence building measures in the defense system to overcome the threat of terrorism through radicalism and extremism by counter-terrorism with international cooperation and seminars. It shows that Indonesia has advanced in countering terrorism so it can be an example for other countries to use the same strategy. Therefore, it will increase the multilateral cooperation as global strategies to protect global citizen from terrorist attact and threat through international or domestic violence nor radicalism and extremism.

4. Conclusions

The dynamic of the global system has shifted the form of acts of terrorism which began to use soft methods in spreading influence and ideology in society. The existence of terrorist has become a real threat in international security shifts the form of threats and disturbances to the threat of radicalism and extremism.

Radicalism and extremism are the alterations of terrorist strategies in giving the concept of jihad to individuals and groups. Radicalism and extremism are genealogical actions for the game of terrorist attact in achieving its goal of establishing the Khilafah Islam in Indonesia. Radicalism and extremism attack the vulnerability of unstable people both culturally, educationally and prosperously so that such community groups are the main targets. Therefore, the government through BNPT (National Counterterrorism Agency of Indonesia) in collaboration with the private sector, in this case is the social and religious based foundation made a soft power approach to shift radical and extreme behavior so not to lead to violence as a form of deterrence and overcome the terrorism in Indonesia.

Soft power approach is carried out through a religious, cultural and ideological approach so that the radical notions inherent in potential terrorists can be directed so that they do not end in violence. The soft power approach model used by BPNT combines the values of nationalism and Indonesian culture by adjusting the background of subjects who will be given deradicalization treatment through soft power approaches. BNPT works with various private parties as an integral part of deradicalization programs that have a psychologically adaptive approach. The given approach is accommodated by expert groups religiously, culturally, socially and psychologically so that the subjects do not feel like they are being given deradicalization treatment. The main objective of the deradicalization program through the soft power approach is counter terrorist strategies through the inlet of radicalism in their mind. Therefore the program's strategy is specifically limited to directing radical and extremes notions in society so they are directed to the general social systems not to lead of violence acts. This model shows that Indonesia start advance in overcoming terrorism by their soft act through radicalism and extremism. It can be reference strategies by countries in countering terrorism as part of global act adjusted to their local value both nationally and culturally.

References

[1] Amy Zalman and Jonathan Clarke 2009 The Global War on Terror: A narrative in Need of a Rewrite *Journal of Ethics & International Affairs 23 (2)* pp 101-113.

[2] Arabinda Acharya. The Bali Bombing: Impact on Indonesai and Southeast Asia. *Center for Eurasia Policy Occasional Reseacrh Paper, Series II (Islamism in Southeast Asia), No. 2.* Hudson Institute. Pg. 2. From: https://www.hudson.org/content/researchattachments/attachment/517/acharyathebalibombings.pdf (Accessed on 25 April 2019).

[3] Muhammad A.S. Hikam 2016 *Deradikalisasi: Peran Masyarakat Sipil Indonesia Melawan Radikalisasi* (Jakarta: Kompas).

[4] Fransisco Galamas 2015 Terrorism in Indonesia: An Overview. *Research Paper 04/2015: The Militant Groups of Radical Ideology and Violent Nature Series Area: Indian Subcontinent and Southeast Asia* (Madrid: IEEE) pp 1-16.

[5] Debora Sanur L. 2016 Upaya Penanggulangan Terorisme ISIS di Indonesia dalam Melindungi

Keamanan Nasional *Jurnal Politica, Vol. 7 No. 1 Mei 2016 DPR RI* pp 32-33.

[6] M. Himawan T. Arifianto 2017 Orientasi Dominasi Sosial sebagai Alternatif untuk Melihat Sikap Implisit Terhadap Sistem Sosial yang Timpang: Adaptasi Skala Orientasi Dominasi Sosial (SDO Scale) *Jurnal Psikologi Sosial, Vol. 15. No. 2* pp 108-109.

[7] Felicia Pratto, Jin Sidanius and Shana Levin 2006 Social Dominance Theory and the Dynamics of Intergroups Relations: Taking Stock and Looking Forward *European Review of Social Psychology, 2006, 17* (Paris: Psychology Press of Taylor and Francis Group) pp 271-320.

[8] Joseph S. Nye 2002 *The Paradox of American Power: Why the World's Only Superpower Can't Go It Alone* (New York: Oxford University Press).

[9] Muhammad A.S. Hikam 2016 *Peran Masyarakat Sipil Indonesia Membendung Radikalisme: Deradikalisasi* (Jakarta: Kompas).

[10] Muhammad Nursalim 2014 Deradikalisasi Terorisme: Studi Atas Epistemologi, Model Interpretasi dan Manipulasi Pelaku Teror *Jurnal Studi Agama dan Pemikiran Islam, Vol. 8, No. 2, Desember 2014* pp 337-338.

[11] Haryatmoko 2000 Agama: Etika Atasi Kekerasan (*Harian Kompas Edisi 17 April 2000*) in Muhammad Nursalim 2014 Deradikalisasi Terorisme: Studi Atas Epistemologi, Model Interpretasi dan Manipulasi Pelaku Teror *Jurnal Studi Agama dan Pemikiran Islam, Vol. 8, No. 2, Desember 2014* pp 329-346.

[12] Jim Sidanius and Felicia Pratto 1999 *Social Dominance* (Cambridge: The Cambridge University Press).

[13] Agus SB 2016 *Deradikalisasi Nusantara: Perang Semesta Berbasis Kearifan Lokal Melawan Radikalisme dan Terorisme* (Jakarta: Daulat Press).

[14] Aan Aspihanto and Fatkhul Muin 2017 Sinergi Terhadap Pencegahan Terorisme dan Paham Radikalisme *Jurnal Hukum Volume 3 Nomor 1 Tahun 2017* pp 73-90.

[15] Concluded from National Counterterrorism Agency of Indonesia.

[16] Times Indonesia 2017 *Soft Power Approach Cara BNPT Lakukan Deradikalisasi* from: https://www.timesindonesia.co.id/read/152481/20170721/193441/soft-power-approach-cara-bnpt-lakukan-deradikalisasi/ (Accessed on 25 April 2019).

[17] Joseph S. Nye, Jr. 2004 *Soft Power: the Means to Success in World Politics* (New York: Public Affairs).

[18] Concluded from National Counterterrorism Agency of Indonesia.

Terror Management, Economic Growth and Islamic Perspective toward the World Peace – IIDSS2019

Taufik[1] and Sri Lestari Prasilowati[2]

[1]STIE IPWIJA, Jl Letda Natsir No 7 Cikeas Nagrag, Bogor 16967, Indonesia
[2]STIE IPWIJA, Jl Letda Natsir No 7 Cikeas Nagrag, Bogor 16967, Indonesia

E-mail: alwitaufik@yahoo.com

Abstract. This research purposed to enrich a study about the strategic peace building based on terror management, terror impact on economic growth and Islamic perspective toward universal peace in the world. The concept proposed in this study is expected to be one of the basic global challenges the peace development in partially Islamic majority countries and toward universal peace. The method of this research is descriptive qualitative research based on research in the field of terror management, political economy and the perspective of peace in Islamic teachings. The policy makers can enrich the absorption of information and develop strategies to deal with terrorism by applying approaches in Islamic perspective. Some important things that can be developed from Islamic values such as: Spread of peace, the equality of all human beings, the call for goodness, the prohibition of committing crimes, competing in goodness, justice and being the enforcer of justice, tolerance, brotherhood, social solidarity, and conveying the truth wisely. Based on the dominance of terror victims in Muslim countries need to emphasize peace building policies enriched with approaches obtained the perspective of Islam toward creating the universal peace in the world.

1. Introduction

National resilience is crucial for Indonesia, which has a population of 269,536,482, which is the fourth largest in the world, and the first largest in the ASEAN region. Based on the composition of religion, Indonesia is the largest Muslim country in the world. National resilience is faced with the dynamics of transnational crime such as terrorism, drugs, and human trafficking. Based on the 2018 Global Terrorism Index, Indonesia is ranked 42 (score 4.54) on the level of medium-scale terrorist impact. Generally of average the trend of terrorism is prevalent in Muslim-populated countries. The trend must get high attention for stakeholders in Indonesia to minimize the spread and development of ideas, teachings and acts of terrorism in Indonesia.

Specifically, there are several variables that cause terrorism, including: clash of identities/dispute with identity aspect, dispossession, exclusion, inequality, repression, violent, and negative economic impact (Newman 2006). On the other hand, terrorism has an impact on defense, social, cultural and economic aspects.

In the economic aspect, terrorism has an impact on the micro economy and macro economy, both in the short term (Llussá & Tavares 2011), and on long periods (Robinson *et al* 2017). The impact of terrorists on the economy as in aspects: ratio of Private consumption growth Public expenditure growth, Private investment growth, and Output growth. This was caused by acts of terrorism in the form of attacks on the interests of civil society, public sector, political and military, injuries, and killing. The sequence of events that accompany it besides being felt by the community in general also has an impact on the economic and political policies of the country that is a victim of terrorists.

The background of terrorism can be motivated by ideologically, religious, personally, ethnically or state-sponsored. Terrorism can directly target the public sector and private sector (Llussa & Tavares 2011). Research and Scholarly publications on terrorism have increased after the 11 September 2001 attacks in USA (Aly & Striegher 2012). The 11/9 attack was linked to perpetrators affiliated with Al Qaeda. Later ISIS emerged on June 29, 2013 calling for the establishment of an Islamic State, where actions other than fighting the Iraq and Syrian government, also became victims of the community which damaged infrastructure and economic impacts. What is shown from the presence of ISIS increasingly raises Islamophobia. On the other hand there is a pro-contra trend in some people who are curious, and finally learn about what and how the true teachings of Islam.

This research focused on the case of non-state terrorism, based on previous research studies and current data on terror management, the impact of terror on economic growth and Islamic perspective in realizing world peace through efforts to minimize acts of terrorism and empower productive economic activities and the spread of universal peace. This paper, which on strategic management field especially terror management, aims to find out the strategic role of terror management by enrichment with economic growth aspect and Islamic perspective in peace building toward universal peace.

2. Research Purpose

The purpose of this article is to enrich a study about the strategic peace building based on terror management, terror impact on economic growth and Islamic perspective toward universal peace in the world. The concept proposed in this study is expected to be one of the basic global challenges the peace development in partially Islamic majority countries and toward universal peace.

3. Research Methodology

The method of this research is descriptive qualitative research based on research in the field of terror management, political economy and the perspective of peace in Islamic teachings in realizing world peace.

4. Results and Discussion

4.1. Terror Management

Terror management provides an increase in ideas, creativity, innovation and experience in handling behavior, actions, impacts and preventive, detective and corrective stages that can enrich the design of the strategy of peace building. Terror management concerning with the anticipation or preemptive, detective and corrective of the negative background of live or the way of live and how to solve the problem in to the common positive perspective. (Greenberg, Vail, & Pyszczynski 2014).

There is plenty of evidence that shows that the terror management process is also able to encourage positive behavior, attitudes and the harmony human interaction. The positive effects of terror management are inseparable from the breadth and scope of science and the development of branches of terror management theory dynamically related to several aspects, namely: politics, religion, love, death, rules of interaction between children and parents, social interactions, health and even neuroscience.

Some research from evaluating counter terrorist strategies that put forward efforts to fight terrorists, when evaluated, found several cases that the strategy for counter terrorism or strategy for combating terrorism did not stop the action and development of terrorism. Some researcher discover the benefit evaluation toward terrorism minimize impact (Lum, Kennedy & Sherley 2006). Especially in the context ideology background of terrorism should be faced by wisely approach (Sukabdi 2015). The research shows that this strategy needs to be continually evaluated along with the development of terror management alternatives through the building peace approach. Peace building strategies and policy involve more efforts to increase a positive of human interaction, norms, attitude, and human being value in personally or socially scope from local, national, regional, and global interaction.

4.2. Terror Impact on Economic Growth

The impact of terror can destroy a variety of facilities, property, historical sites and archeology, the death of humans, disabled victims and injuries, the emergence of public fear and cessation of community activities and economic stagnation as a direct or indirect result of acts of terror. Some examples of Terror attacks such as terror 9/11 2001, 2002 Bali Bombing, terror on mosque attacks in Christchurch, New Zealand 2019, churches and three luxury in Sri Lanka terror 2019. Some conclusions from previous research, such as the conclusion of researcher in Somalia proposed peace-building strategies to build a comprehensive sector in public and private sector including economic sector (Elmi & Barise 2006). Many things indicate economic backwardness such as illiteracy, poverty, poor health, low income, high unemployment and crime. in principle, efforts to minimize economic impacts can reduce the subsequent effects of terrorism. This phenomena should ideally be a consideration for policy makers (Piazza 2006). As stated earlier, that an increase in positive attitudes and high humanity is expected to further strengthen harmonization with the increasing welfare side in the economy.

Research in Turkey, showed us the negative impact for the economic development by the terrorism attack (Bilgel & Karahasan 2015). In similarly cases and research in Pakistan, suggests that terrorism has negatively affected the economic growth (Hyder, Akram, & Padda 2015). In the other cases, increasing of terrorism has negative impact to decreasing of foreign investment (Powers & Choi 2012 Shah & Faiz 2015).

4.3. Peace in Islamic Perspective

In principle, Islam means peace. Islam teaches various aspects comprehensively and integrally. Starting from spiritual and physical activities, individual and social, relations with humans, nature and the environment, the world and aspects of the hereafter. Muslims will be the second of the biggest of world's population based on religion (Desilver & Masci 2017).

Besides various developments in Islam, there are also issues of negative issues regarding Islam which cause some people to perceive Islam as a bad thing. (Bleich 2011). This, raises the presumption of even accusations and physical actions on some innocent Muslims..

Islamophobia is partly due to the massive coverage of acts of terrorism which are often perpetrated by Islam. In principle, a variety of terror attacks associated with individuals are not teachings from Islam. Because in Islam an attack that causes death in a human is a great tyranny (Armstrong 2001). Islam do not justify any acts of violence against followers of the same religion or different religions. There are many prejudices and misperceptions that claim that Islam teaches barbaric action and terror. This prejudice strengthened with the occurrence of a civil war involving Muslim countries (Iran vs. Iraq, Saudi vs. Yemen), acts of terror in the name of Islam, and certain doctrines in Islamic teachings such as takfir, tending to display the image of Islam who are rude, violent and cannot coexist and respect each other (Toft 2007). In principle, religion has an impact on human behavior, interaction and social relations (Abuznaid 2006).

Basically Islamic teachings aim to bring peace. Quran affirms that Prophet Muhammad PBUH (peace be upon him) was sent to spread affection: "We will not send you, but to (be) a mercy to the universe" (Quran 21:107). "and peace is the best" (Quran 4:129). Islam strongly promotes true peace, which calls for basically all human beings to come from one ancestor, and are called to compete in goodness. Peace that is connected with servitude to the creator. Who saved one soul as if saving all humanity, and vice versa (Quran 5:32). Islam teaches help to help in kindness and advise one another to avoid crime (Quran, 5:2).

There are many restrictions on realizing peace. like there is no forced in religious affairs (Quran 2: 257, 18:30, 109:7), Killing (Quran 5:32), help in sinning and hostility (Quran 5:2), conspiracy related to cases of sin, hostility and crime (Quran 58:9), disseminate information without checking and rechecking (Quran 49:6).

Islam calls for continuing efforts in the actions and development of a variety of positive things in realizing universal peace. Some things that can be obtained from Islamic teachings such as: spreading peace (Quran 8:61), love for humans (Quran 4:37) the equation of the degrees of all man (Quran 49:14) send to those who speak and prevent from evil (Quran 3: 105) Race in kindness and piety (Quran 5: 2, 2:148).Justice and being the enforcer of justice (Quran 5:8), (Quran 4:135, 16:90), Tolerance and check and recheck (Quran 49:6) respecting other, Islamic brotherhood (Quran 49:10) Social Solidarity (Quran 34:39) Deliver the truth wisely (Quran 16:125)

There is no religious moral principle that is more emphasized in Quran and Sunnah besides the principle of justice, establishing the law fairly, honesty, equality and simplicity, against oppression at interpersonal and structural levels (Quran 16:90, 4:58, 4: 135, 5: 8, 60:80). Islamic tradition calls for the establishment of justice and resistance to injustice, there is a close link and interdependence between peace building and justice (Quran 60:80).

This notion of ideal and comprehensive justice can facilitate the development of an Islamic peace-building strategy with a broad emphasis on individual responsibility and the main moral obligation to fight against injustice. In addition, Barazangi (1996) notes that methods of promoting justice and other economic equality are carried out through various Islamic rules that encourage mutual support and cooperation. Examples: (1) the law of mutual help); (2) public treasury; (3) diyah (blood money), (4) hospitality law, (5) al-musharakah (the law of distribution), (6) al-ma`un (the law of doing good), and (7) al-irth (Islamic inheritance law).

Various studies, generally do not discuss terrorism based on state actors (Primoratz 2003). Some researchers even find that the state can carry out acts of terror, but the research is limited. this is in line with the lack of further development of systematic research (Jackson , 2008).

Negative perceptions of Islam can arise because the world community through mass media exhibited the deaths of more than 10,000 people carried out by groups affiliated with Islam such as: Boko Haram, ISIL, AlShahab and the Taliban or Al-Qaeda. The economic impact of terorism 2017 amount $52 billions : property destruction (2%), injuries (1%), GDP Loss (25%), Death (72%).

Table 1. Global Rankings Terrorism Index 2018

No.	Country	Score	Very High	High
1	Iraq	9.75	√	
2	Afghanistan	9.39	√	
3	Nigeria	8.66	√	
4	Syria	8.32	√	
5	Pakistan	8.18	√	
6	Somalia	8.02	√	
7	India	7.57		√
8	Yemen	7.53		√
9	Egypt	7.35		√
10	Philippines	7.18		√
11	Congo	7.06		√
12	Turkey	7.04		√
13	Libya	6.99		√
14	South Sudan	6.76		√
15	Central African	6.72		√
16	Cameroon	6.62		√
17	Thailand	6.25		√
18	Sudan	6.18		√
19	Kenya	6.11		√
20	USA	6.07		√
21	Ukraine	6.05		√
22	Mali	6.02		√
23	Niger	6.00		√

Source: Institute for Economics & Peace. Global Terrorism Index 2018: Measuring the impact of terrorism, Sydney, November 2018. http://globalterrorismindex.org/

The frequency of terrorist attacks on countries with a very high scale of impact is experienced by Muslim-majority countries, namely: Iraq, Afghanistan, Nigeria, Syria, Pakistan and Somalia. Likewise on the impact of terrorism at a high level - with the exception of India, USA, Ukraine, Philippines, Thailand, Mali, it is still dominated by Muslim majority countries such as Yemen, Egypt, Libya, Turkey Sudan, Mali and Niger.

Basically, the efforts to realize peace contribute positively to economic development. Globally, both regionally and world population, various activities affiliated with acts of terrorism have affected economic conditions in general and people's purchasing power, especially in countries with high levels of terrorism. This arises because of the effects of fear, damage and other economic impacts which have negative aspects of business and economic turnaround. The economic impact of violence has increased with the start of war in Syria and various types of violence in the Middle East and North Africa. Cases in Afghanistan, Iraq and Syria, caused the three countries to bear the biggest costs among the ten countries that have the highest impact of terrorist attacks. Some research found that the ten countries that were highest exposed to terrorism attacks had assumed 19 times more costs compared to the ten countries that were the lowest exposed to terrorism attacks. Some research also found that in the 20 most peaceful countries it turned out that costs of violence were far smaller than the global average (Institute for Economics & Peace 2018). (Institute for Economics & Peace 2018).

Various findings from terrorist phenomena in carrying out their actions, they appear to depend on the costs they incur, utilization, attack opportunities and opportunity costs of each plan and execution. This should be the entry point in developing strategies and policies for handling terrorism that can minimize terrorist activities (Frey & Luechinger 2008).

Activity and various forms of terrorism cannot be completely overcome by patterns and models of violence such as the role of contra terrorism because some policies like this have not maximally eliminated terrorism. Nor can it be fought through a strategy that ignores the great danger of terrorism. In principle, terrorism must be condemned on the basis of the values and moral principles of humanity as well as the values of all religions in the world that provide a strong foundation in designing terror management governance based on long-term beneficial strategies and effectively minimize their subsequent impacts (Primoratz 2003). This is in accordance with the findings in this study where the approach with attention to negative and devastating impacts on the economy of all victims of terrorism and structured and strategic approaches through religious and humanitarian moral values will bring enrichment to the minimization approach to the development and impact of terrorism toward creating the world peace.

5. Conclusions

- Terror management can be used as a basis in designing control strategies as well as minimizing the development of terrorism. Strategies and policies in the form of counter terrorist actions or fighting terrorists are considered not always effective in reducing the development of terrorists.
- Based on the understanding the negative impact of terrorism on micro and macroeconomic activities (especially in countries affected by terrorism at very high and high levels), demanding that policy makers can enrich the absorption of information and develop strategies to deal with terrorism by applying approaches in perspective Islam.

- Some important things that can be developed from Islamic values such as: Spread peace, love to humans. The equality of all human beings, the call for goodness, the prohibition of committing crimes, competing in goodness, justice and being the enforcer of justice, tolerance, check and rejection, Islamic brotherhood, social solidarity, and conveying the truth wisely.
- The minimize the terror victims in Muslim-majority countries has become a matter of special importance to emphasize peace building policies enriched with approaches and practical matters obtained from the perspective of Islam in minimizing acts of terror, minimizing victims terror, and creating the universal peace in the world.

Acknowledgements

We would like to thank the IIDSS (Indonesia International Defense Science Seminar) for guidance and support with this issue. We are incredibly grateful for its diligence and insight.

References

Abuznaid S, 2006 Islam and Management What can be Learned? *Thunderbird International Business Review* 48 pp 125-139

Aly A, Striegher J L 2012 Examining the Role of Religion in Radicalization to Violent Islamist Extremism *Studies in Conflict & Terrorism* 35 pp 849-862

Armstrong K, 2001 *The True Peaceful Face of Islam* Retrieved from content.time.com/time/printout/0,8816,175987,00.html

Barazangi N H, Zaman M R Afzal O 1996 Islamic identity and the struggle for justice pp 47-63 (Gainsville University Press of Florida)

Bilgel F, Karahasan B C 2015 The Economic Costs of Separatist Terrorism in Turkey *Journal of Conflict Resolution* September pp 1-23

Bleich E, 2011 What is Islamophobia and How Much is There? Theorizing and Measuring an Emerging Comparative Concept *American Behavioral Scientist* 55 pp 1581-1600

Desilver D, Masci D 2017 *World's Muslim Population more Widespread than You Might Think* Pew Research Center, Retrieved from https://www.pewresearch.org/fact-tank/2017/01/31/worlds-muslim-population-more-widespread-than-you-might-think/

Elmi A, Barise A. 2006 The Somali Conflict: Root Causes, Obstacles and Peace-Building Strategies *African Security Review* 15 pp 32-54

Greenberg J, Vail K Pyszczynski T 2014 Terror Management Theory and Research: How the Desire for Death Transcendence Drives Our Strivings for Meaning and Significance In *Advances in Motivation Science* Academic Press 85-134

Hyder S, Akram N Padda I U H 2015 Impact of Terrorism on Economic Development in Pakistan *Pakistan Business Review* January pp 704-722

Institute for Economics & Peace. *Global Terrorism Index 2018 Measuring the Impact of Terrorism* (Sydney) Retrieved from http://globalterrorismindex.org/

Jackson R, 2008 The Ghosts of State Terror: Knowledge, Politics and Terrorism Studies, *Paper prepared for the International Studies Association (ISA) Annual Conference* 26-29 March, (San Francisco USA) pp1-17

Llussá F, Tavares J 2011 Which Terror at which Cost? On the Economic Consequences of Terrorist Attacks, *Economics Letters* 110 pp 52–55

Lum C, Kennedy L W Sherley A 2006 Are Counter-Terrorism Strategies Effective? The results of the Campbell Systematic Review on Counter-Terrorism Evaluation Research *Journal of Experimental Criminology*

Newman E, 2006 Exploring the Roots Causes of Terrorism *Studies in Conflict and Terrorism* 29 pp 749-772

Piazza Z A, 2006 Rooted in Poverty? Terrorism Poor Economic Development and Social Cleavages *Terrorism and Political Violence* 18 pp 159–177

Powers M, Choi S W 2012 Does Transnational Terrorism Reduce Foreign Direct Investment? Business-Related Versus non-Business-Related Terrorism, 49 pp 407-422

Primoratz I, 2003 *State Terrorism and Counterterrorism*, Centre for applied philosophy and Public Ethics, Working paper Number 2003/3 (Australia)

Quran 2019 Retrieved from https://www.alquranenglish.com/

Robinson E, Egel D Johnston P B Mann S Rothenberg A D Stebbins D 2017 *The Economic Impact of Islamic State Governance in Iraq and Syria*, RAND Corporation (Santa Monica, California)

Shah M H, Faiz M 2015 Terrorism and Foreign Direct Investment an Empirical Analysis of SAARC Countries, MPRA (Munich Personal RePEc Archive) Paper No 82008 pp 1-21

Sukabdi Z A, 2015 Terrorism in Indonesia a Review on Rehabilitation and De-radicalization, *Journal of Terrorism Research*, 6 pp 36-56

Toft M D, 2007 Getting Religion? The Puzzling Case of Islam and Civil War, *International Security* 31 pp 97-131

Preventing the growth of terrorism based on local wisdom through friendship in nyadran- IIDSS2019

Apriles Lusein S[1)]

[1)] Peace and Conflict Resolution, University of Defense, Indonesia Peace Security Center, Bogor 16810, Indonesia

E-mail: rinodwipa@gmail.com[1)]

Abstract. Terrorism is one of the real threats faced by Indonesia today. Rooted in the radical movement both ideologically and understanding based on religion evolved into the terror threat that threatens people's lives extensively so dangerous for national security and defense. Terrorism is categorized as asymmetric warfare in which more priority to psychological pressure in the form of terror in the form of violence and threats of violence intended to frighten the victim. Therefore, the need for public awareness through moral values of local wisdom that has been planted and rooted in the community to prevent and counter the threat of radicalism that led to acts of terrorism. Local knowledge as a bid strategy in the face of terrorism by focusing the study on the reality of the territory that could potentially be the target of terror. Moral values positively contained in the local wisdom among others the teachings of moral norms are actualized in the lives of everyday people, for example, the relationship Nyadran in doing the Javanese community to establish bonds of brotherhood and cultivate compassion of the heart between people regardless of religion, ethnicity, race and class. Human nature is basically the same, so the relationship is not only important for individuals and families, but also for the community or the nation in general in order to achieve harmony of life associated with the living, the dead and their attachment to God Almighty. Moral values positively contained in the local wisdom among others the teachings of moral norms are actualized in the lives of everyday people, for example, the relationship Nyadran in doing the Javanese community to establish bonds of brotherhood and cultivate compassion of the heart between people regardless of religion, ethnicity, race and class. Human nature is basically the same, so the relationship is not only important for individuals and families, but also for the community or the nation in general in order to achieve harmony of life associated with the living, the dead and their attachment to God Almighty. Moral values positively contained in the local wisdom among others the teachings of moral norms are actualized in the lives of everyday people, for example, the relationship Nyadran in doing the Javanese community to establish bonds of brotherhood and cultivate compassion of the heart between people regardless of religion, ethnicity, race and class. Human nature is basically the same, so the relationship is not only important for individuals and families, but also for the community or the nation in general in order to achieve harmony of life associated with the living, the dead and their attachment to God Almighty. Hospitality Nyadran example in doing the Javanese community to establish bonds of brotherhood and cultivate compassion of the heart between people regardless of religion, ethnicity, race and class. Human nature is basically the same, so the relationship is not only important for individuals and families, but also for the community or the nation in general in order to achieve harmony of life associated with the living, the dead and their attachment to God Almighty. Hospitality Nyadran example in doing the Javanese community to establish bonds of brotherhood and cultivate compassion of the heart between people regardless of religion, ethnicity, race and class. Human nature is basically the same, so the relationship is not only important for individuals and families, but also for the community or the nation in general in order to achieve harmony of life associated with the living, the dead and their attachment to God Almighty.

1. Introduction

Terrorism remains a serious problem in Indonesia, which not only includes actors in the country, but the cross-country network, roughly terrorism is a term used for the use of violence against civilians / non-combatants to achieve political ends, on a smaller scale than the war. Terrorism is made of fear or horror to intimidation or threats to scare (Merriam-Webster, 1996). Acts of terrorism at the beginning of the 21st century since the events of 9/11 in 2001 that occurred in the United States. Terrorism is spreading throughout the world like a virus that attacks and develop ways and patterns are constantly changing. In Indonesia itself an act of terrorism occurred again in 2018, this pattern is different from previous actions where previously only be done by a man, but that occurred in 3 (three) Church in Surabaya, The main perpetrators of the act with his wife and children (one family). Some new patterns of development led to efforts to counter terrorism is becoming increasingly difficult to anticipate. Acts of terrorism carried out at random, uncompromising, victims could be military or civilian, men, women, old, young and even children, rich and poor, anyone can be attacked. Terrorism is not a question of who the perpetrators, groups and networks. However, more than that terrorism is an act that has its roots beliefs, doctrines and ideologies that can attack the public consciousness. Flourishing of terrorism depends on the land where he grows and develops. If he lived in the land of arid, then terrorism is difficult to find a place, otherwise if he lives in fertile land then he will quickly develop.

In Indonesia, in the era of globalization and technological developments make a tendency for people to be prosecuted following the advances in technology and changing times continue to rise. It affects the lifestyle and values of togetherness among people, where people increasingly busy with a variety of facilities that enable them to live a life, but on the other hand makes them even further away from the emotional connection is physically among humans, causing attitude indifferent and do not care about surrounding environment. This has become one of the great opportunities for radicalism to enter and affect community life became the seeds of terrorism. History records that most acts of terrorism occurred in Indonesia, on the island of Java, which happened in the big city that has a variety of economic, social and cultural rights. Actually, the public in general has had a strategy to prevent terrorism through the development of a culture of life that is inherited from ancestors but with the advancement of age and globalization that many of these values began to fade even forgotten. Various inherited ancestral culture with positive values become the basis of community care in strengthening brotherly relations and establish friendship among people in an area. These values into local wisdom in people's lives. S Various inherited ancestral culture with positive values become the basis of community care in strengthening brotherly relations and establish friendship among people in an area. These values into local wisdom in people's lives. S Various inherited ancestral culture with positive values become the basis of community care in strengthening brotherly relations and establish friendship among people in an area. These values into local wisdom in people's lives. Synergetic all components of society, accompanied by the strengthening of the values of local wisdom and local culture is very important for us. Local knowledge is of course relies on the role of traditional leaders, religious leaders, community leaders and youth leaders as the frontline in the face of the threat of radicalism and terrorism. Local knowledge can also support the existence of the state (nation state) specific. Even in formulating a nation state, always coloured by local wisdom that grows in a society that shape and aspire to the nation state. Local knowledge stems from the idea or ideas, which are then applied in the practice stage, and the creation of cultural material.

Culture is an idea in the form of models of knowledge used as a basis or reference by a person as a member of society social activities, creating a culture material in the element of universal culture: religion, science, technology, economics, social organization, language and communities, and the arts.[2] Indigenous already exist and live in society as hereditary as a mirror of the religiosity of the local community, namely the customs rooted in the teachings of their religion. There are also indigenous presence had been established for the area which is home to the community is led by chiefs or traditional leaders who have long been not altered by the progress and developments of the age.

2. Definition of Terrorism

Before discussing how the values of local wisdom through the culture of friendship in Nyadran to prevent acts of terrorism, here are some definitions of terrorism. Terrorist acts is not new. Since the beginning of independence until the reform of terrorism is always present in the form of, motives and movements are different and with different coping strategies also vary. Global terrorism today there are two kinds of state terrorism and the terrorism network. State terrorism is the impact of public mistrust of the political system of democratic ethics that should be upheld and terrorism terrorist network that carried out the third network in the form of a supranational network. [3] The method used third-generation terrorists are moving on their own, without the control of a significant organization.

Hendropriyono said that terrorism in Indonesia broken grew missing tubs changed. If the terrorists assume as leaves, then tying them into the organizational structure are the branches, twigs, branches, and trunk of a tree. The terrorists like the leaves of a tree that always sprout and regenerate prolifically, each time preceding autumn leaves or chopped. [4]

In a book entitled "De radicalisation Terrorism: Humanist, Soul and Touches Grassroots Approach". Terrorism is defined as any act that is against the law by sowing terror widely to the public with threats or violence, whether organized or not, as well as the consequences in the form of physical pain and psychological or within a prolonged categorized as a crime outstanding (extra ordinary crime) and crimes against humanity (crime against humanity). (Glose, 2014).

In the context of Law No. 5 of 2018 on the Amendment of Act No. 15 of 2003 on Stipulation of Government Regulation in Lieu of Law No. 1 Year 2002 on Combating Criminal Acts of Terrorism Become Law, Article 1 (paragraph 2) explains that terrorism is an act the use of violence or threat of violence that have caused the climate of terror or fear widespread, which can cause the victim that is mass, and / or cause damage or destruction to vital objects strategic, environmental life, public facilities, or international facilities with a pattern of ideology, political and security disturbances.

Acts of terrorism can be committed by an individual, group of individuals or countries as an alternative to the declaration of war openly. Terrorism is not part of an act of war, so it should still be regarded as a criminal act. In general, civilians are the main targets of terrorism, thus attacks against military objectives cannot be categorized as acts of terrorism.

Have the attitude and understanding of the radical alone does not necessarily make someone fall in the understanding and terrorism. There are other factors which motivate someone to join in terrorist networks. The motivation is caused by several factors. First, the domestic factors, namely domestic conditions such as poverty, injustice or feel disappointed with the government. Second, the international factor, namely the influence of external environment provide the impetus growth of religious sentiment as global injustice, that arrogant foreign policy, and the modern imperialist superpower. Third, cultural factors were strongly associated with religious understanding is shallow and narrow interpretation of scripture and lexical (literally).

3. Definition Local Wisdom

The term local wisdom (local wisdom) can be seen as a form to find a format values that develop in a society. The idea of local wisdom can be understood as a form of "indigenous ideas" that are indigenous. Even this issue spread to various issues such as identity, religious, social and political. Therefore the issue of local wisdom was sticking to the surface, but rarely appears study that could explain aspects of what exactly the meaning contained in the matter of local knowledge. That is, whether the value of local wisdom that appear in the public trust? Or local knowledge as a form of resistance against the "global knowledge" that has been formed with the face of globalization. [5]

Local knowledge can be understood as the result of local people thought that shrouded discretion, be positive, and then followed and believed by all members of society without coercion. Each region will likely have local knowledge are different from each other. [6]

Local knowledge is a cultural identity or personality of a nation that causes it is able to absorb, even cultivate the culture that comes from outside / other nations became his own character and abilities. The identity and personality certainly adjust to the views of community life around in order to avoid a shift of values.

Local knowledge is a way of life and science as well as various life strategies that intangible activities undertaken by the local community in responding to various problems in the fulfillment of their needs. In foreign languages often also conceived as a local policy or local knowledge of local wisdom "local knowledge" or local intelligence local genious. Various strategies undertaken by local communities to preserve their culture. [7]

Local knowledge can be understood as the result of local people thought that shrouded discretion, be positive, and then followed and believed by all members of society without coercion. Each region will likely have local knowledge are different from each other. [8]

Local knowledge, according to John Haba as quoted by Irwan Abdullah, "refers to a variety of cultural richness that grows and develops in a society that is known, trusted and recognized as important elements capable of reinforcing social cohesion among citizens'. At least six of the significance and function of local knowledge if used in refolusi conflict. First, as a marker of identity of a community. The second element (cohesive aspect) cross residents, interreligious and trust. Third, local wisdom was not coercive but rather an awareness from the inside. Fourth, the local knowledge gives color together a community. Fifth, the ability of local wisdom in changing the mindset and the interrelationships of individuals and groups and put it on common ground. Sixth,

4. Friendship in Nyadran

1871 EB Taylor defined culture is a complex which includes knowledge, belief, art, morals, law, custom and other capabilities as well as the habits that were made by humans as members of society. Java community in general also has customs that are still doing their community. As done by the whole village community.

In the implementation of Nyadran or thanksgiving tradition of all faiths joined together in places where the implementation of this tradition is in one of the village which is said to be trusted by the local community as petilasan, even some that believe most of the tombs. This ritual, is one culture that is still often done by some communities in Indonesia in particular by Java community is still very strong with the cultural heritage of our ancestors.

This ritual held annually by the Java community, the majority in Java has a tomb figures considered sacred although many do not know exactly how the history of the beginning of the character until in their area. Even if they know, they cannot be proved with certainty because there is no written proof and concrete evidence. Nyadran in general can be said as a form of ritual through prayer and alms (uba rampe / food) intended to pray for the souls of the deceased. This tradition is widely known by the Java community as the village clean activity and alert the inclusion in Sura. [9]

Nyadran tradition has the goal of implementation that can be seen from the aspect of social, cultural, social and economic aspects and aspects of religion. Socio-cultural ritual execution of Nyadran not limited to cleaning the tombs of ancestors, selamatan make apem cake, sticky rice and compote as well as platform offering element of ritual prayer. Nyadran also be silahturohmi media as well as a transformation of family and social, cultural and religious (Remy, 2008: 80). On the implementation of Nyadran tradition many people who came even people living in another city deliberately return to follow the implementation of Nyadran tradition. Even people who are not present and the poor are given gadhulan (default) containing rice, dumplings and side dishes are then sent by the committee to their homes. [10]

The activities carried out in accordance with the opinion Nyadran ceremony Department of Education (1994: 20) that in a complex ritual system contains many important elements among other offerings, pray, eat together, and parade. Nyadran of activity illustrates that humans cannot cater to individual needs his own without the help of others. Therefore man is called a social being. With cooperate to improve the sense of community among residents and tighten the relationship between citizens. Besides, we can know each other between the citizens of the other residents who initially had never known.

5. Terrorism Versus friendship in Nyadran

Acts of terrorism is a non-traditional threat which makes the human threat as an object of focus of attention, but also has an impact threat to the traditional threats that make threats against the sovereignty of a country that maintained by military force. Current human individual has been placed as the object and purpose of the effort to create security threats that are specific, which raised a concept of human security which deals with the human individual as an object that is protected from threats as well as subjects that can protect and eliminate the threat.

See definition above, it can be interpreted that the role of the human individual as the object of a threat by an individual therefore also be subject to eliminate or prevent the threat. Therefore, why the author would like to provide a strategy to prevent the spread of terrorism through the culture of local wisdom that has been passed ancestors to individuals the Java community, especially through friendship Nyadran, and can also be developed for Indonesian society in general with local knowledge possessed respective areas.

All this to prevent and confront the threat of terrorism occurred, countries are still prioritizing military strength by deploying elements of strength and capacity of the various elements of intelligent to the deployment of Special Forces. but with the threat of terrorism that are real are the main factors that become the basis for preparing the design of this strategy as well as changes in the pattern of the threat of terrorism makes the country must involve the general public to prevent and confront the threat of terrorism is already contained in the national defence system. National defence system is universal that involve all citizens, regions, and national resources more, as well as prepared earlier by the government and held in total, integrated, directed, and continues to uphold the country's sovereignty, territorial integrity, and safety of the entire nation of all threat. (Article 1, paragraph 2 of Law No. 3 of 2002). National defence system is universal characterized by democracy, the universality and territoriality. Democracy means that the orientation of the defence enshrined together with the people and for the benefit of all people. [11]

Thus in addition to the power and military capabilities, the need for strong support from the community to prevent the threat of military outside, such as the threat of ideology and radicalism that led to acts of terrorism. Because this threat is born and rooted in the community, so that as early strategy to prevent this threat into an action, then the public should be concerned and mutual maintain national unity through the culture of local wisdom that has been attached.

Sibarani (2012), local knowledge is knowledge of the local community are used to improve the well-being and create peace for the people in a community. This means that with their local knowledge among the people, make people's lives and create a prosperous peace, that peace is a strategy to prevent the threat from the outside.

The tradition of friendship in Nyadran become part of the tradition. One of the main objectives is to connect the rope friendship. It aims not only to add a friend or friends, but more than that friendship ultimate goal is to strengthen the bond of brotherhood. [12] In the tradition of friendship through Nyadran creating horizontal relationships are harmonious in the social life of Javanese society cannot be separated from the actualization of the values of peace will find through unity, mutual assistance and care for each other, besides maintaining harmony vertical relationship with God Almighty and ancestors. In a broader perspective,

The government as the policy holder, both in the field of culture and religion must needs be made a motion regarding acculturation program and relations with regard to both of these. Instead there should be a dialogue between religious leaders were there with local cultural figures to discuss the form of recognition of the autonomy of religious and cultural autonomy, so that religious and cultural region territory is not mixed up. However, it should be noted that in case the relationship (relationship) between cultures and religions does not mean religious values derived sacredness. Likewise, the value of culture is not the same degree of purity to be lifted with religious values.

According to Renan Ernast in theory ethnicity, nationality is a unified solidarity, unity composed of people who each feel solidarity with one another. Nationality is a soul, a spiritual principle that is a great solidarity unity, created by the feeling of the sacrifices that have been made in the past and that the people concerned are willing to be made in the future. Nationality has a past, but she goes on her today with a fact that is clear, that the agreement, which stated with a real desire to live together. The presence of a nationality as if a deal happens every day. [13]

Local governments have authority in implementing an early warning system should be judicious, fair and coordinated in support of cultural activities of local wisdom in order to prevent the growth of terrorism in society. It really depends on the wise decisions of local leaders from the governor, regent, mayor, local council and other supporting isntansi.

References

[1] AM Hendroprioyono, Terrorism: Fundamentalist Christianity, Judaism and Islam (Jakarta: Compass Books, 2009), p. 13.

[2] Rusmin Tumanggor, et al, Social and Cultural Association, (Jakarta: Kencana Prenada Media Group, 2010) hlm.25.

[3] Tito Karnavian, 2011. "Terrorism Generation III" in Magazine Slot, page 23, the March 2011 issue, Jakarta.

[4] AM Hendropriyono. 2014. "Intelijent Philosophy" (Jakarta: PT Kompas Media Nusantara, 2013), p 142.

[5] Piotr Sztompka, Sociology of Social Change, Matter 3rd, Alibahasa Alimandan, Jakarta: Prenada Media Group, 2007, p. 70-71.

[6] Bambang Wahyudi, Conflict Management. Local Wisdom approach (Jakarta: Pustaka Twilight, 2018), p. 37.

[7] Irawan. 2015 "Local Wisdom" in http://eprints.umm.ac.id/35955/3/jiptummpp-gdl-irawansatr-48429-3-babiip-f.pdf, downloadable on May 18, 2019.

[8] Bambang Wahyudi, Conflict Management. Local Wisdom approach (Jakarta: Pustaka Twilight, 2018), p. 37.

[9] Bambang Wahyudi, Conflict Management. Local Wisdom approach (Jakarta: Pustaka Twilight, 2018), p. 42.

[10] Mita Astria, Wakidi and M. Basri. 2004. "Toward Tradition Nyadran In Ramadhan In the village Triharjo Merbau Mataram District of South Lampung regency" Journal of Culture.

[11] Ministry of Defense. 2015 Defense White Paper. Jakarta: Ministry of Defense of Indonesia.

[12] Aqua Dwipayana, 2018. "The Power of Friendship" Jakarta.Taushia.

[13] Bantarto Bandoro, J.Kristiadi, Reflection Half a century of Indonesian Independence, CSIS, Jakarta 1995, p 1

Pancasila and Bela Negara to Counter the Threat of Mindset War in the Asymmetrical Warfare Perspective – IIDSS2019

Luh Putu Ika Primayanti[1]

[1]Asymmetric Warfare, Indonesia Defense University, Bogor 16810, Indonesia

E-mail: primayantiputu@gmail.com

Abstract. This paper aims to analyse the Pancasila as the basis of the Indonesian state and the concept of State Defence 'Bela Negara' as a strategy in counteracting the threat of a mindset war in Indonesia. Mindset war is one part of asymmetric warfare that uses soft power in attacking its opponents to achieve interests. So that strengthening the values of Pancasila and the implementation of the concept of state defence are the best strategy because they carry out ways that soft power also. This study uses a qualitative method that is descriptive analysis, namely explaining the phenomenon under study based on data collected and processed, then analysed using a theory that is relevant, so that a conclusion can be drawn. This paper is reviewed by using the concept of Pancasila, the concept of Martial Arts, the concept of mindset war and the concept of asymmetric warfare. The results of this study are that the basic values of Pancasila should be strengthened and implemented because these values are mutually supportive values, becoming unity that cannot be separated and conforms to national identity. As well as the use of the concept of defending the state in counteracting the threat of a mindset war because defending the country contains five important aspects, namely the love of the homeland, willing to sacrifice for the nation and state, awareness of nation and state, Pancasila as the state ideology, and the ability to defend the country. The goals of the planting of Pancasila and Bela Negara values are all components of society in general and the young generation in particular. Besides that, Pancasila and Bela negara include Patriotism and Nationalism which are effective to build national character. The role of media and technology is very necessary to carry out propaganda on the values of Pancasila and Bela Negara.

1. Foreword

The dynamics of the development of the strategic both globally, regionally and nationally today have signaled a large and complex challenge to national defense both physically and non-physically which leads to potential threats to state sovereignty; the integrity of the unitary state of the Republic of Indonesia and the safety of the nation and will increasingly develop into a multidimensional, physical and non-physical nature and originating from outside and from within the country. The threats that have occurred in Indonesia have undergone a change from military threats to non-military threats.

Indonesia is facing three dimensions of threat, namely real threats, unreal threats, as well as real threats and non-physical threats to the mindset of all Indonesian people. The real threats and main threats that we are facing right now are from the threat of terrorism and radicalism, separatism and armed rebellion, natural and environmental disasters, violation of border areas, piracy and theft of natural resources, epidemics, cyber warfare and intelligence and drug trafficking and abuse. While the threat is not yet real is the presence of military aggression carried out by other countries. [1]

The real threat and non-physical threat to the mindset of the entire Indonesian people are the phenomenon of the mindset war in Indonesia. The threat of a modern mindset war will continue to influence the hearts and minds of the people with the aim of deflecting an understanding of the country's ideology. The operational methods of this war are carried out through infiltration into the dimensions of intelligence, military, education, economics, ideology, politics, socio-culture. Culture and religion, assistance, cooperation in various fields and media or information. In addition, the threat of this mindset is massive, systematic and structured which continues to strive to influence and destroy not only the mindset but also the identity of the Indonesian goose through the influence of foreign ideologies that are not in accordance with our culture. This was one of the wars that used the method of asymmetric warfare. [2] At present time we are facing the threat of ideological ideologies which impose the will to change the Pancasila through foreign penetration or Khilafah, which wants to replace the state ideology of Pancasila.

In order to deal with the threat of mindset war, the government through the ministry of defense makes a universal state defense strategy. However, strengthening the Pancasila and the State Defense program is the right strategy in counteracting the threat of mindset war. Pancasila is the identity of the nation and Defense of the Country is a way to shape the character of the nation, especially the young generation of the nation's successor.

2. Methodology

This study uses an approach with qualitative methods. Qualitative research is research conducted to understand the meaning of individuals or groups regarding the social problems studied. Qualitative research is descriptive because the collected data is in the form of words and images, so it does not emphasize numbers. The data collected is inductive in that it builds information from specific themes to the public. [3] Meanwhile, according to Bungin, the qualitative research process includes collecting data, reducing and making research reports. While secondary data sources consist of writing in the form of reports from other people's research, namely, through literature studies such as books, theses, journals, official documents, newspapers, official websites. [4]

This research is descriptive analysis, namely explaining the phenomenon under study based on data collected and processed, then analysed using a theory that is relevant, so that a conclusion can be drawn. [5] So, in conducting this research, researchers collected data, then grouped it based on the material of the discussion. After that, the relationship between one data and another will be searched and analysed using theory to find answers to the research questions. The results of the research answers are drawn into a conclusion.

3. **Theoretical Review**

Pancasila

Pancasila is the ideology of the Indonesian nation that is upheld as a national identity. Pancasila literally consists of two syllables namely Panca and Sila. Panca means Lima and Sila means principle or basis. So that Pancasila is interpreted as the five basic principles of the Indonesian state. [6] The values of Pancasila have been applied since the time of the archipelago kingdom even though they do not have concrete rules like today.

Pancasila was formulated by nine national leaders who became known as the Committee of Nine consisting of Ir. Soekarno, Drs. Mohammad Hatta, Mr. A A. Maramis, Mr. Muhammad Yamin, Abikusno Tjokrosujoso, Abdul Kahar Muzakir, H. Agus Salim, Mr. Achmad Soebardjo, and KH. Wachid Hasyim. [7] The resulting formula was rejected by the Indonesian envoy from the East regarding the First principle which was deemed not to accommodate all the beliefs or religion contained in Indonesia. However, in the PPKI session on August 18, 1945 the formulation of the legitimate and official Pancasila was adopted as the basis of the state contained in the opening of the Constitution of the Republic of Indonesia in 1945. The five precepts are Almighty Godhead, Fair and Civilized Humanity, Indonesian Unity, Popularism led by Wisdom of Wisdom in Representative Consultation and Social Justice for All Indonesian People.

Literally, Pancasila has many functions for the Indonesian people. Not only as a nation's ideology and state foundation. But also, Pancasila as a source of philosophy of the nation and state of Indonesia, Pancasila as the nation's worldview, and Pancasila as the nation's personality. Pancasila is a consensus and agreement to build Indonesia without questioning heterogeneous background differences in religion, race, culture, language and others. [8]

Bela Negara (State Defence)

Bela Negara is defined as an orderly, comprehensive, integrated and continuous determination, attitude, and action of citizens based on love for the homeland, awareness of Indonesian nation and state, and belief in Pancasila as the nation's ideology and willingness to sacrifice to eliminate any threat both from abroad and from within the country that threatens national independence and sovereignty, national unity and unity, territorial integrity and jurisdiction, as well as the values of Pancasila and the 1945 Constitution. [9]

Bela Negara is the rights and obligations of citizens. This is stipulated in the 1945 Constitution article 27, paragraph 3 of the 1945 Constitution which reads "Every citizen has the right and obligation to participate in the defence of the state". Meanwhile, the defence of the state cannot be separated from the defence and security of the state mentioned in article 30 paragraph 1 of the 1945 Constitution which reads "Every citizen has the right and participation in the defence and security of the state". At present, defending the state can be adjusted in its application with programs through adaptive values to the present. Adjustments are made so that they are more interesting and can foster an attitude of state defence for the younger generation.

The basic values of defending the State are further explained in five aspects, namely: [10]

1. Love the country. The love of the nation for the homeland in its real form is knowing the history of Indonesia, preserving Indonesian culture, protecting the environment and the good name of the State of Indonesia.
2. Willing to sacrifice for the nation and the State. This is indicated by raising the good name of the nation and the State through achievements both academic and non-academic.
3. Awareness of nation and state. The attitude of the Indonesian people should be in accordance with the national personality that is associated with the ideals and goals of the nation.
4. Pancasila as the ideology of the State. Pancasila must be practiced by safeguarding it from foreign threats that want to replace Pancasila.
5. Having the initial ability to defend the country. The initial ability to defend the State was aimed at maintaining discipline, tenacity, and hard work of its citizens in facing military and non-military threats.

Mindset War

The mindset war is a threat that occurs in Indonesia that attacks the mindset of the people to get their interests. The mindset war is a non-physical threat that is massive, systematic and structured. This has disrupted national defence, especially the Pancasila ideology (Ryamizard Ryacudu in the War of Threats Ideology of State Ideology, 2019). [11] The operational methods used are through infiltration into intelligence, education, military, economic, ideological, political, social, cultural and religious aspects.

Literally, the mindset war consists of the word's 'war' and 'mindset'. According to Carl von Clausewitz in his book "On War", war is an act of violence intended to force opponents to follow our will. [12] While the Mindset is defined as a mindset consisting of beliefs or ways of thinking that affect one's actions. In theory, according to Gollwitzer (2016), the action phase of further mindset is based on clear differences between the motivational phases (i.e. the predisposing and post actional phases, where the pursuit of goals becomes a problem) and the will phase (i.e. the pre actional and actional phase, the pursuit the goal is the main question). So that it can be concluded that the notion of mindset war is an action that can force the opponent to follow the will by attacking the mindset. [13]

Asymmetric Warfare

Asymmetric warfare is "unconventional methods of exploiting our strengths, or confronting us in ways we cannot match in kind." [24] When referring to this definition, asymmetric warfare itself can be called a war that uses a non-approach. Conventionally then exploit the vulnerability of actors in unusual and irreversible ways. Asymmetric warfare prioritizes political methods (soft power) such as those carried out in the name of an identity (ethnic, religious, ideological, or tribal) in order to gain access to certain countries to the achievement of the country's war objectives. [25]

According at the definition and correlation with current global issues, it can be concluded that asymmetric warfare is an unusual or non-conventional form of war involving non-state actors who use unusual strategies and ways of thinking. Asymmetric warfare also has characteristics to be regarded as unusual warfare, namely the emerging actors are non-state actors, different strategies and areas of war, and how "the weak" can win in a war. The last feature is interesting because in conventional warfare, a country can be said to win a war if its military capability is very strong, but this does not happen in asymmetrical warfare. "The weak" can win the war with effective strategies and tactics, even more effective than conventional warfare.

It can be concluded that asymmetric warfare is how actors (state and non-state) act, organize, and think of something different from their opponents in order to maximize their personal benefits, exploit the weaknesses of their opponents, achieve their own initiatives or increase their freedom of action. Such actions can be political strategies, military strategies or a combination of both. These things require methods, technology, values, organization, the right time and a combination of all.

4. Result and Discussion

4.1 Mindset War as Threat in Indonesia

The threat to the "mindset" that is very real and is one form of defamation of religion, state and the Indonesian nation which greatly influences the integrity and unity of the nation is terrorism and radicalism. This threat does not only raise material losses and lives and creates fear in the community, but also has torn the integrity of the nation and state.

The mindset war starts from the infiltration of certain elements of society by provocations and propaganda that trigger ethnic, religious, racial and intergroup (SARA) conflicts. In addition, various ideologies seek to divide the nation and incorporate its interests into a new government so that it can trigger Indonesian security and defence instability. There are three patterns of the spread of the notion of terrorism through the media. First, the initial stage was only in the form of the dissemination of ideology through the website facilities. Second, the use of media interaction features such as the creation of forums and chatrooms. Third, the use of social media such as Facebook, Twitter, Instagram etc.[16]

The mindset war that occurs is a form of asymmetric warfare that prioritizes unusual patterns so that people often don't realize it. The use of mass media and information technology accelerates the threat of this mindset war. Local and international factors that influence the emergence of mindset wars in Indonesia, namely the heterogeneity of the people in Indonesia and the abundance of natural resources contained in them are domestic factors. While international factors are the number of foreign penetrations in all aspects of life.

Domestically, Indonesian people consisting of various tribes and ethnicities are easier to fight especially using the issue of SARA when compared to a homogeneous society. With ethnic and ethnic differences, the mindset of people in Indonesia is different, so the threat of mindset war easily invades society. In addition, abundant natural resources make it easy to attack mindset wars because of the many conflicts involving both foreign investors and the Indonesian people in fighting over natural resources to achieve prosperity. This can trigger national divisions and security and defence stability.

While factors that originate internationally are the presence of foreign penetration in all aspects of life. Foreign penetration as a threat originating from abroad towards the ideology of the State can result in disruption of various aspects of community, national and state life which have implications for the existence of sovereignty, territorial integrity and national security. The ideological power of the State is directed at forming a mindset, attitude pattern, and pattern of action in the elaboration of community values. Pancasila as a national ideology is used to unite, guard the stability and progress of the nation.

Especially in Indonesia, the mindset of the young generation is changing and experiencing a cultural shift. Ideology and socio-culture are part of the national strategic environment focus on which development will determine how to make a national defence strategy. Foreign penetration can cause degradation in the implementation of the Pancasila. The loss of Pancasila values which emphasize multiculturalism, diversity, and the value of justice with narrow primordialism tendencies are indicative of a decline in understanding of the values of the Pancasila ideology. [17] Meanwhile in the field of socio-culture, foreign penetration has caused a change in mindset, attitude pattern, and the pattern of future generations' actions to be unconcerned in addressing various national problems.

4.2 Strengthening Pancasila Values as a Counter to Mindset War

The ideology of Pancasila is a formula and guideline for the life of the nation and state for all the people of Indonesia. Pancasila as the nation's ideology is the result of extracting values that live in society, must be conveyed and taught to the community. While the Caliphate as an invitation to form a state based on religion for the state of Pancasila seems less relevant. This can be viewed from the historical, normative and philosophical side of the Indonesian nation.

Likewise, in terms of politics, Pancasila is the result of a diversified Indonesian nation's compromise, a national consensus that is able to mobilize and guarantee the unity of the nation towards the realization of common ideals of a just and prosperous society. The population of Indonesia is a majority of people who are Moslem. Laying the Pancasila as a state ideology does not conflict with sharia. Thus, it is seen as the formation of the basic principles of philosophy of his home country or the spirit of the Pancasila ideology.

The Pancasila Philosophy can be defined briefly as a critical & rational reflection on Pancasila as the basis of the state and the reality of national culture with the aim of obtaining the points of understanding. Pancasila as a System can be seen from two things:

- Deductive: looking for the essence of Pancasila and analysing and structuring it systematically into a comprehensive viewpoint
- Inductive: observe the symptoms of social, cultural, community, reflect it.

Pancasila is essentially a system of philosophy because it is a unit. The basic philosophy of the State of Indonesia consists of five precepts, each of which is a principle of civilization. Each precept is an element (an absolute part) of the unity of Pancasila, then the basis of the Pancasila State Philosophy is a single compound entity. Consequently, each precept cannot stand alone. The principles of Pancasila which is a philosophical system are essentially an organic unit. Pancasila as a system can also be understood from the basic thoughts contained in Pancasila about humans in relation to God, himself, fellow human beings and with the people of the nation.

Strengthening the implementation of Pancasila values can be done in several ways. First, Pancasila should be well socialized so that it can be implemented. One way is to use media and information technology. Both aspects are the best means of propaganda. Propaganda is a message designed to influence and invite the mindset of the community to think and act in accordance with certain attitudes.[18] Specifically, propaganda is disseminated institutionally and systematically specially to promote political interests or religious views.

Second, it can be done through learning or curriculum in schools so that the younger generation is more sensitive to national identity and is not easy to accept foreign penetration. Even though it requires a large budget, citizenship and Pancasila education are important things that are still taught at school. Learning methods in the curriculum is one form of psychological operation (Psyops). Planned operations to convey selected information and indicators to foreign audiences to influence the emotions, motives, objective reasons, and ultimately the behaviour of governments, organizations, groups, and foreign individuals. The purpose of psyops is to make certain pressure on other countries' government organizations, politicians, foreign economies and other aspects to achieve the national interests of a country. [19]

Third, strengthening of ministries and government institutions that are responsible for strengthening the implementation of Pancasila in Indonesia. Indonesia basically has an institution specifically tasked with assisting the President in formulating Pancasila Ideology coaching and carrying out coordination, dissemination and control of the development of Pancasila ideology in a comprehensive and sustainable manner. [20] The agency is the Pancasila Ideology Development Agency (BPIP) which is a change from the Presidential Work Unit for the Development of Pancasila Ideology in accordance with Presidential Regulation (Perpres) No. 54 of 2017 concerning the Presidential Work Unit for the Development of Pancasila Ideology. Several activities have been carried out, but the lack of news in the mass media has made the community mindset think that this institution must continue to be improved in performance and synergize with other institutional ministries in the process of planting Pancasila values in Indonesia.

The values of Pancasila as a dynamic ideology that reflects the openness of thought that is able to accept all the climate changes that occur in order to be able to carry out the values of the Pancasila are fundamentally described as follows. [21]

First, *Ketuhanan Yang Maha Esa*. The Indonesian nation expresses its belief and devotion towards the Almighty God. Religion and trust are problems that concern human relationships with God, but still based on humanity and fostering harmony between religious groups.

Second, *Kemanusiaan Yamg Adil dan Beradab*. This is understood and applied by recognizing and treating humans according to their dignity and dignity as God's creatures. And recognizing equality without distinguishing ethnicity, ancestry, religion and so on.

Third, *Persatuan Indonesia*. Described as the means of emerging unity, unity and interests and safety of the nation and state as a common interest above personal and group interests. Then it is in accordance with the state's goal of maintaining world order based on freedom, eternal peace and social justice.

Fourth, *Kerakyatan Yang Dipimpin Oleh Hikmat Kebijaksanaan Dalam Permusyawaratan Perwakilan*. It is explained as the relationship among citizens in a deeper sense on which every Indonesian human being has the same position, rights and obligations. Prioritizing deliberation in making decisions for common interests. As well as decisions taken must be morally accountable to the Almighty God, uphold human dignity and values, values of truth and justice prioritize unity and unity for the common good.

Fifth, *Keadilan Sosial Bagi Seluruh Rakyat Indonesia*. Described as the development of a noble deed which reflects the attitude and atmosphere of kinship and mutual cooperation. And like to appreciate the work of other people that are beneficial for progress and mutual prosperity.

In order to deal with the influence of mindset war, all components of society should prioritize the actualization and purification of the implementation of Pancasila values as the basis of the ideological power of the nation and state. The ideology of the Pancasila is an ideology based on philosophy of idealism. The values contained in the ideology of idealism will never change since the past now and in the future. Idealism is an inner nature and materialism is an outward nature. Therefore, this concept of Pancasila idealism is the most effective in preventing influences of ideological materialism.

4.3 *Bela Negara as a Concept of Counteracting the War of Mindset*

'Bela Negara' or State defence concept is needed in national defence. In the implementation of universal state defence, there are three components of national defence, namely the main components, reserve components, and supporting components. The main component is the Indonesian Armed Forces, which are ready to be used to carry out defence tasks. The reserve component consists of national resources that have been prepared to be mobilized through mobilization to enlarge and strengthen the strength and capability of the main components. Whereas the supporting component is a national resource that can be used to increase reserve strength and capability. Supporting components and reserves need to be fostered using State defence education.

To detain Indonesia from ideological threats, community resilience must be built through the Pancasila, then the state defence program was launched by Minister of Defence, Ryamizard Ryacudu. State defence is a concept that reflects the translation of Pancasila values. Framework for penetration of values: the theory of planned behaviour, where there is a belief system that is influenced and the importance of defending the country needs to be done early from the character side. This can affect the belief system of the family, environment and school. From intrapsychic values and attitude systems are very influential to do something. Psychological engineering for mind penetration, value systems and positive preparedness requires one individual in a family full of love. Groups to build trust and cooperation. Service and society in general are related to loyalty. Then there needs to be social sanctions and law enforcement against violations.

The state defence values that should be used to prevent the mindset war are as follows.

1. Loving the country. The love of the nation for the homeland in its real form is knowing the history of Indonesia, preserving Indonesian culture, protecting the environment and the good name of the State of Indonesia.
2. Willing to sacrifice for the nation and the State. This is indicated by raising the good name of the nation and the State through achievements both academic and non-academic.
3. Awareness of the nation and state. The attitude of the Indonesian people should be in accordance with the national personality that is associated with the ideals and goals of the nation.
4. Pancasila as the state ideology. Pancasila must be practiced by safeguarding it from foreign threats that want to replace Pancasila.
5. Possessing the ability of initial defence to the country. The initial ability to defend the State was

aimed at maintaining discipline, tenacity, and hard work of its citizens in facing military and non-military threats.

Another advantage of the concept of state defence is the nature of nationalism and patriotism in it. Nationalism is a notion that argues that the highest individual loyalty must be left to the nation state. [22] while Patriotism is the spirit and spirit of love for the country which complements the existence of nationalism. A group of humans who inhabit the earth of Indonesia must unite, truly love, and are willing to sacrifice to defend the Indonesian homeland as an independent nation. [23] Without a sense of nationalism and patriotism, the Indonesian people were unable to gain independence in the past and maintain independence in the present and future.

But in its implementation, the state defence program has not summarized all aspects of life. So that an innovation is needed so that all ages, professions and regions can feel the importance of state defence programs in overcoming the threat of mindset war. The government should also disseminate to the entire community the magnitude of the negative danger from this threat through media and propaganda.

5. Conclusion

In the face of a mindset war, it is necessary to have concrete and comprehensive efforts from all stakeholders and all Indonesian people to work together in carrying out deterrence and resistance to all forms of negative and destructive mindset war threats which will threaten national ideology and identity and this country of Indonesia. If you cannot anticipate this, the impact and consequences of this mindset war will be enormous and powerful for the continuity of the existence of the Republic of Indonesia in the future. Strengthening the implementation of Pancasila values and the state defence program is the right strategy to overcome the threat of mindset war in Indonesia. mindset war that relies on changing mindset with the help of technological advances and mass media.

In strengthening the implementation of the Pancasila three things are needed, namely to be well-socialized through propaganda, Pancasila Education included in the curriculum at all levels of education as a form of psychological operation, and good synergy between the ministry of institutions in making policies regarding strengthening the implementation of Pancasila values. While the concept of Martial Arts should be applied on an innovation so that all ages, professions and regions can take part in a state defence program that contains nationalism and patriotism in order to overcome the threat of mindset warfare.

References

[1] Kementerian Pertahanan Republik Indonesia. (2015). Strategi Pertahanan Negara. Jakarta:Kemhan

[2] Pranoto, A 2016 Perang Asimetris dan Skema Penjajahan Gaya Baru (Jakarta:Global Future Institute)

[3] Wahyuni, S 2012 Qualitative Research Method (Jakarta: Salemba Empat)

[4] Bungin, B 2003 Analisis Data Penelitian Kualitatif (Jakarta: PT Raja Grafindo)

[5] Sugiyono 2014 Metode Penelitian Pendidikan Pendekatan Kuantitatif, Kualitatif dan R&D (Bandung: Alfabet)

[6] Hatta, M 2015 Politik, Kebangsaan, Ekonomi (1926-1977) Jakarta: Kompas

[7] Prasetyo, T 2014 Membangun Hukum Berdasarkan Pancasila Bandung: Nusamedia

[8] Chairul, H 2018 Meneguhkan Pancasila sebagai Ideologi Bernegara: Implementasi Nilai-nilai Keseimbangan dalam Upaya Pembangunan Hukum di Indonesia Jurnal Resolusi Vol.1 No.1 Pp 78-99

[9] Ansar 2001 Perspektif Islam Tentang Bela Negara Jurnal Ketahanan Nasional Vol.VI No.1 Pp 32-41

[10] Lembaga Administrasi Negara - Modul Wawasan Kebangsaan dan Nilai – nilai dasar Bela Negara. Accessed on https://kepri.kemenkumham.go.id/attachments/article/2595/Modul%201.pdf at 01/06/2019

[11] Golda Eksa 2019 Perang Minset Ancam Ideologi Negara. Accessed on https://mediaindonesia.com/read/detail/234381-perang-mindset-ancam-ideologi-negara at 14/05/2019

[12] Clausewitz 1989 On War (United Kingdom: Princeton University Press)

[13] Gollwitzer, P & Keller, L 2016 Mindset Theory. Accessed on https://www.researchgate.net/publication/312340264 at 14/05/2019

[14] Rod Thornton, 2007, Asymmetric Warfare, (Cambridge : Polity Press, 2007), Hlm. 19.

[15] Joint Warfare of the Army Forces of the United States, (Washington DC: Government Printing Office),1995,hal.7

[16] Agus, SB 2016 Deradikalisasi Dunia Maya (Jakarta:Daulat Press)

[17] Kementerian Pertahanan Republik Indonesia. (2015). Buku Putih Pertahanan Negara. Jakarta:Kemhan

[18] Kotler,P 1999 Marketing: How to Create, Win, and Dominate Market Accessed on https://www.researchgate.net/publication/265069529_Kotler_on_Marketing_How_to_Create_Win_and_Dominate_Markets at 01/06/2019

[19] Ujfalusi, T 2013 Psychological Warfare and War Propaganda Proses Ilmiah NKE HHK Seni Perang (Budapest:Hadmuveszet) Pp.27-31

[20] Hariyono 2019 Sambutan Plt. Kepala BPIP. Accessed on http://www.bpip.go.id/ at 01/06/2019

[21] Pemerintah Republik Indonesia 2011 Ketetapan MPR RI Nomor I/MPR/2003. Accessed on http://jdih.bpk.go.id/wp-content/uploads/2012/08/ketetapan-mpr-ri-nomor-i-mpr-2003-1325650924.pdf at 01/06/2019

[22] Kohn, H 1982 Nationalism Its Meaning and History (Florida: Robert E. Krieger Publishing Co)

[23] Bakry, N 2010 Pendidikan Pancasila (Yogyakarta: Pustaka Pelajar)

Indonesian Cyber Security: A domestic Policy and International Cooperation to Promote Security and Protect Indonesian Society in Cyber Space – IIDSS2019

Wahyu Wardhana[1]

[1]Defense Economic Cohort 4, Universitas Pertahanan, Sentul, Bogor 16810, Indonesia

E-mail: wahyu12013@gmail.com

Abstract. Cyber space has been facilitating social interaction among people and ethnic group around the globe. The states also more rely on cyber space to manage their civilian and military function. It has created new security threat to human security and national security. This paper will explore Indonesian cyber security, its domestic policy, and its international cooperation in addressing cyber threat based on English school and Copenhagen school of security studies. Indonesia has faced cyber-crime, cyber terrorism, cyber espionage, hacktivism, digital misinformation, and cyber war. In addressing those threats, Indonesia need strengthen domestic policy in cyber security, cooperation with Private Sector, increase cyber resilience, and international cooperation. Indonesia can use current mechanism to propose the confidence building measure in cyber space to minimize cyber security dilemma, prevent malicious action in cyber space, limit the potential tension among states in cyber space, and promoting a secure cyber space for national and international prosperity.

1. Introduction

We live in digital era in which cyber space has been facilitating social interaction among people and ethnic group around the globe with different culture, idea, and language. In addition, our society is connected through internet, which made possible to order food, buy a book, or buy concert ticket without leaving our house. The states also more rely on cyber space to manage their civilian and military function. Such dependency has created new security threat to human security and national security. The cyber threat, such as misinformation, violent content, and malicious cyber activities, from individual, violent group, criminals, and even nations-states [1] carry potential devastating effect. Indonesia is one of the top five countries in the number of users of social media, such as, Facebook, Twitter, Instagram and WhatsApp. Almost half of the users in Indonesia are exposed to fake news in social media [2]. In addition to fake news, in 2018, Indonesia was faced 12.9 million cyber-attacks, and it grows by an average of 15 percent every year [3].

With this background, this paper will explore Indonesian cyber security, its domestic policy, and its international cooperation in addressing cyber threat in which based on English school and Copenhagen school of security studies. Copenhagen School is important to explain the conception of cyber security, cyber threat, the impact of cyber threat, and how to address cyber threat. All of those are a relatively new development and lacks sufficient historical context to define acceptable and adequate responses to cyber threat. In this context, English school perspective can be used to describe international rules, norms, and institutions to address cyber threat. It can be used to formulate policy, government-private sector cooperation, and international cooperation to encounter cyber threat. Several case studies of recent cyber-related incidents in this paper would help Indonesia to describe, to categorize cyber threat, to identify possible impact, and the best practice to respond potential threats and recover from cyber-attack.

2. The Conception of Cyber Security: A security Dilemma in Cyber Space

Cyber security can be defined as "the threat opportunities from digital and computational technologies" [4]. It also can be understood as "a means to protect and defend society and its essential information infrastructures, and carry out national and international policies through information-technological means" [5,6]. Cyber security is securitized in addressing cyber threats to specific "referent objects" [7]. The referent object of cyber threat could be the state, the nation, society, private actors, and information networks [7,8]. This situation encourages state to enhance their cyber security which leads to occurrence of cyber security dilemma. It happens due to difficulties in gathering information and measuring other state cyber capability. In addition, from economic point of view, offensive action in cyber domain is cheaper and easier than defensive measure [9]. While from strategic perspective, "offense will always trump defense," [10] due to offensive action in cyber space will success, even though the attack only create minor damage to digital infrastructure [9]. However, under the cyber security dilemma cooperation is still promising to prevent cyber incident [4]. Indonesia with its partner could act as architect of cyber security governance through complementary program, norms, and confidence building measures in cyber space.

3. The Cyber Threat Addressed by Cyber Security Policies

Cyber threat means the probability of action or an incident in the cyber space which can damage or disturb information system and some operation connected to the cyber domain [11]. The threat could threaten computer, internet-connected device, information network, data processed, stored, or transmitted on those systems [11]. In this paper, there are six cyber threats which can jeopardize cyber-related activity in Indonesia and need to be addressed by cyber security policies.

Cyber-Crime

Cyber-crime can be defined as acts of utilizing telecommunications network or information system to commit crime which violating national law or/and international treaties or convention [11, 12]. The purpose of the crime is mainly for financial profit [9]. From 2012 to April 2015, the economic loss due to cybercrime reached Rp33.29 billion [13]. One of the case was the act of hacking and stealing over Rp8 billion from multi-level marketing websites in 2012. This money was used to fund terrorist training camps in Indonesia. In May 2018, 103 Chinese nationals were arrested in Bali, and in 2019, 28 Chinese nationals were arrested in Semarang for alleged cyber fraud and extortion [14, 15]. Beside cyber fraud, cyber sextortion case has caused a hundred people lost tens of millions of rupiah [16].

Cyber Terrorism

Cyber terrorism is conjunction of terrorism in cyber space. It can be defined as the utilization of cyber space to attack against information system, critical infrastructures, and network to create fear in society [17]. However, there has not been a single case of real cyber terrorism, on Indonesian national critical infrastructure dependent on cyber space. On the other hand, all of terrorist activity which uses cyber space can be also categorized as cyber terrorism [12]. With this understanding, propaganda, radicalization, recruitment, and fund raising through cyber domain, such as social media, is cyber terrorism. For example, in 2018, Indonesian pro-ISIS group, Jamaah Ansharut Daulah (JAD), posted terror threat from hacktivist 1435 Anshar Caliphate Army on Indonesian government [18]. In regard of recruitment, the YouTube was used by ISIS to recruit foreign fighters from Indonesia through the publication of video titled "joining the rank" in July 2014 [19]. The Telegram Messenger was also used to conduct terrorist attack in Jakarta in January 2016 [20]. Five months later, in June 2016, ISIS published propaganda video which encouraged ISIS supporters to attack police in Central Java [21].

Cyber Espionage

This is a modern day spying that conducted by other country intelligence services to gather classified information for political and/or military purposes [11]. Sometimes, it is also conducted by private sector or company. The private sectors spy others company or university regarding research and development and steal information to minimize their research and development cost [9].

Hacktivism

Hacktivism refers to an action to disrupt information flow or steal information [9] and then spread to public. This action is hybrid cyber activity with include cyber espionage. This hybrid cyber activity can be described with the theft of F-35 plans in 2009. In this case, someone hacked US defense contractor's computer and stole the new plans of US' F-35 [22]. Another example is occurred in

July 2009, when New York Exchange and the Pentagon websites were attacked by denial of service [23]. In these both case, the hacker probably from China due to the Internet Protocol address (IP address) was traced back to China [9,24,25]. In Indonesian case, the cybercriminal group named Black Hat has hacked hundreds of websites, including companies based in Jakarta and even database of city of Los Angeles. The group detained by the Indonesian Police after the Internet Complaint Center from US' FBI informed Indonesian police concerning suspicious online activity in Indonesia during 2017 [26].

Digital Misinformation and Manipulation

Digital misinformation and manipulation is described as the use of algorithms, automation/computerization, big data, and human involvement to purposefully produce and distribute misleading information over social media networks to manipulate public opinion [27]. Over this several years, state and non-state actors were identified using digital misinformation during political events and security crises [27]. The utilization of digital misinformation in political events can be traced back to the 2014 presidential elections in Brazil and municipal elections in Rio de Janeiro in 2016 [27]. The involvement of Russia's information wars (InfoOps) in Ukrainian conflict is example of digital misinformation employment in international security crises. In this cyber conflict, disinformation operation was waged against Ukrainian citizens on VKontakte, Facebook, and Twitter [27]. In Indonesian case, digital misinformation can be found at presidential election in 2019. In this events, cyber trolls, or buzzers in Indonesia, has been distributed misinformation and hoax stories, using many fake accounts on Twitter and Facebook [2]. However, political parties in Indonesia have denied employing trolls or buzzers to spread fake news. They confirmed that they usually used Twitter to create trending topics [28]. Indonesian Ministry of Communication and Informatics published that there was 1,224 hoaxes related to political issues since August 2018 to March 2019 [29].

Cyber War

The most often cited definition of cyber war is "actions by a country to infiltrate or breach other countries' computers or cyber networks for causing damage or disruption" or disable other countries' information system [30]. This threat looks like science fiction, when the cyber-attack can paralyze national infrastructure dependent on cyber space. However, in Eastern Europe this science fiction had happened [31, 32]. In 2007, the botnets was utilized to spread the denial of service (DoS) attack which has brought down Estonian banking system [33]. Estonia was able to take fast and effective respond to minimize the effects and prevent permanent damages [34]. This fast and effective respond was come from the employment of Computer Emergency Response Team (CERT) and collaboration between government and civilian experts [33, 34]. In 2008, similar attack occurred in Georgia [9], it was happened together with the Russian invasion of South Ossetia [34]. This cyber-attack crippled internet in entire Georgia and cut off Georgia from the world [30]. Both cases reveal the significant role of cyber space in international conflict [33, 35].

When both cases did not produced physical damage, the Stuxnet malware case in June 2010 was known causing physical damage to computers and other equipment [17]. Stuxnet was a worm designed to infiltrate and establish control, it had penetrated specific control systems of Iranian nuclear facility at Natanz [17, 36]. In 2012, a computer virus to be related with Stuxnet known as "Flame" infected individual computer, government computer, and educational institution in Iran and several

Middle East nations [37]. Furthermore, in December 2015, Ukraine's electrical grid was attacked by Advanced Persistent Threat (APT) and left 230,000 populations in blackout [38]. The same malware has been also detected in US' electrical infrastructure [31, 32]. While those cyber-attacks can be contained easily, in June 2017 the virus named as "NotPetya" attacked Ukraine's. This ransomware designed to destroy Ukraine's information systems. However, this attack spread to 64 countries and affect not only government bodies, but also financial institutions, international enterprises, logistical operators, and telecommunication providers [32, 39]. In Indonesian case, in May 2017, the WannaCry malware attacked several hospitals in Jakarta and thousands of computers in almost 100 countries [3, 40]. Indonesia Defense minister argued that cyber war is real threat to national security, remembering that in 2017 there were 205,502,159 cyber-attacks in Indonesia [41].

4. The Impact of Cyber Threat: From Individual Security to National Security

Today social-economic activity is more and more reliant on cyber space. Therefore, cyber threat is a new threat for our daily activity, such as blackmail, extortion, sextortion, etc. In September 2018, a headman from Tembaleng sub-district, district of Jombang, was urged to resign by his society because a photo of his genital was spread on social media [42]. Another example, in February 2018, fake news in social media was distributed concerning an attack to ulema (Muslim scholars) by people with mental illness. This misinformation was distributed by Saracen and Muslim Cyber Army and creates persecution to people with mental illness in several regions in Indonesia [43]. This situation happens do to society favors sensational content, and they rarely crosscheck the news from reliable sources [27]. In economic aspect, the financial loss from cyber-attack includes intellectual property losses, financial fraud, and damage to reputation, and also possibility opportunity cost losses such as lower productivity and loss of sales [44]. It may not directly endanger national economy. However, during the WannaCry attack in May 2017, it has caused direct and indirect losses of up to US$6.7 million for large companies and $33,500 for mid-sized companies in Indonesia [3].

5. The Policy to Address Cyber Threat

When discussing policy to secure cyberspace, state is important actor in maintaining human security and national security in cyber space. Even though, national government has limited capability to protect cyber related activity, other entities, such as individual group and private sector, has similar problem. Furthermore, those limited capability faces certain degree of confusions concerning on what to secure, due to so many private and public's networks and computers need to be secured. If government needs to secure all cyber infrastructure, network, and computer, it will very difficult and need huge amount of resources. If partial cyber security is employed, which ones will be secured, society, private sector, or government network? If only government network, both military and civilian, network is secured, the society and private sector will vulnerable to cyber-related attack, and the state is arguably not secure. When, society and private network is secured, they will suspicious that their activity is inspected by government agency regularly [45]. With this dilemma, Indonesian government needs to build cooperation with private sector, domestically and internationally, to strengthen national cyber security. The cyber resilience is also important to secure public network and entire national cyber infrastructure. All this efforts also need to be strengthened with international cooperation to formulate cyber security strategy, exchange information, sharing best practice, and formulate norms or international legal framework to address cyber threat.

Indonesia Domestic Policy

Indonesia is democratic country, where equality, free speech, and media freedom is assured by the constitution. It will be difficult for Indonesia to maintain high levels of control over the internet, likes China does. China fortified its internet network by internet censorship regime known as "the Great Firewall." This regime blocks foreign platform and replaces with domestic alternative. However, China is not alone, several others countries also implement such regime with different level of control and censorship [46] to assure national cyber security from malicious activity.

Indonesia has similarity with the Western democracy to maintain free cyber space as integral component of all aspects of Indonesian life. With this consideration, Indonesian government secures cyber space through the establishment of National Cyber and Crypto Agency in 2017 under president regulation no.53 of 2017. This agency is mandated to formulate policy, monitoring and evaluation, coordinate, and perform international cooperation in cyber security. This agency was merged from National Crypto Agency and two directorates under ministry of communications and informatics, namely directorate information security and directorate general of information application. National Cyber and Crypto Agency coordinates with others ministries and national critical infrastructure industry, such as telecommunications industry, energy, and transportation [47]. This consolidation has been also carried out by Israel in 2015. Israel consolidated several cyber security authorities under National Cyber Directorate to formulate cyber security guidance and ensures its implementation [48].

In legal aspect, Indonesia has published two regulations, namely the law no.11 of 2008 on Information and electronic transaction and Government regulation no.82 of 2012 on management system and electronic transaction to assure cyber security in Indonesia [49]. However, current available regulation is not yet regulate specifically on cyber warfare or cyber security. In that association, the Defense Minister promptly issued Ministerial Regulation No. 82/ 2014 on defense guidelines regarding cyber war, cyber terrorism, cyber espionage, etc. [41].

Cooperation with Private Sector in Securing Cyber Space

A government is important actor in cyber security, but government alone would face difficulties to secure cyber space. Furthermore, private sector own and operate information network; provide internet service; provide information technology products and its related-services. It means, the state/public-private sector cooperation to secure cyberspace is needed, both domestically and internationally.

This kind of cooperation involves several government stakeholder, international institutions, and private actors [50]. The public and private sectors need to enhance information sharing and developing standards in addressing cyber threat, based on confidence and trust and innovation [51]. The European Union has enforced strict and unprecedented requirements on online search engines and cloud service providers [48]. In the US, the US government does not regulate entire private-sector, but they apply intervention and share intelligent information on particular private sector, such as health and financial sector [48]. The US' Automated Indicator Sharing (AIS) is another example of government cooperation with private sector to enable the reciprocal sharing indicators of cyber threat [52]. Similar to US, German and France work together with selective private sector, in the case of critical infrastructures [48]. In this cooperation, each state offers a several incentives to private sector. The selected private sector in Germany is granted an access to government information on cyber threats [48]. The US government provides liability waivers to private sector who exchange information with government concerning cyber threat. While in UK, the government contractors are accommodated to apply certain security control, and in France, the government offers a voluntary labelling arrangement for cyber security products [48]. In additions, the close and trustful cooperation between public and private sector in cyber security can be found in Israeli case. Under the recently established National Cyber Directorate, Israel classified firms and determines their cyber security necessities and took steps to address the vulnerability [48].

Indonesian government need to conduct information sharing on cyber related threat with private sector in critical infrastructure industry. Even though, greater information sharing on classified information with private sector could endanger technical sources and national security. Indonesian government can provide incentive and share indicators of malevolent action with private sector. For example, Facebook, Twitter, and Google have taken actions to prevent the distribution of fake news, automation, and online harassment [53]. In German, Facebook has been employed fake news detection tools to detect misinformation and launched media literacy campaign in April 2017 [54].

In addition, since 2015, Indonesia Security Incident Response Team on Internet Infrastructure Coordination Center (Id-SIRTII/CC), an agency under Indonesian ministry of communications and informatics cooperated with NEC Corporation, a Japanese based company which provides information technology services and products. This cooperation was conducted in the area of cyber security, designing Security Operation Center (SOC), and securing Internet-based communications in Indonesia [55]. Indonesian ministry of communications and informatics has been also established Critical Information Infrastructure Protection (CIIP-ID) Summit in 2015. This summit is a cooperation framework among stakeholder, private sector, and academic expert in cyber security. In 2018, the summit was held in cooperation with PT Xynexis International, a cyber-security company and expert from Japan and Singapore [47]. This summit discussed and exchange of information concerning cyber threat, the challenge in cyber security, and an efforts to address the threat [56].

After the establishment of National Cyber and Crypto Agency, the collaborative approach to address cyber security issues in Indonesia is conducted by this agency. In 2018, National Cyber and Crypto Agency cooperated with HoneyNet Project and Swiss German University to build research and database center on malicious software. This cooperation would identify malware attack, Indicator of Compromise (IOC), and malware signature [57]. As coordinating agency in cyber security, it will be better when National Cyber and Crypto Agency also cooperate with others university which has international cyber security cooperation, such as Universitas Indonesia cooperation with Keio University in Cyber Security Center of Excellence (INCS-CoE), ITB cooperation with South Korea in cyber security R&D centre, and Universitas Narotama Surabaya cooperation with University of Zagreb and IN2 company from Croatia.

Increase Cyber Resilience

In dissuading cyber threat, national security policy could focus on increasing cyber resilience [17]. Cyber resilience is the whole capability of cyber systems, government institution, private sector, and societal community to resist cyber-attack and recover immediately when damage occurs from cyber-attack. Cyber system or network resilience is important to quickly detect, prevent the spreading of the attack, and recover in slightest of time [58]. Resilience efforts will improve situational awareness, mitigate, and manage the consequences following potentially devastating cyber-attack [17]. Cyber system resilience also needs to be complemented with offline procedure, if the cyber-attack will occur [58]. Indonesian cyber resilience also needs cyber forensic to analyse the source of a cyber-attack for law enforcement or defense counterintelligence purposes [17].

Even though, a new communications technologies could improves survivability during cyber-attack, state also need increase the robustness of the information system through introduction of different modes of communications [44]. In conducting such effort, Indonesia can learn from Active cyber defense in UK, in which the government implements security measure to strengthen a network or system to make it durable target for cyber-attack [11, 59]. Government institutions, such as, National Cyber and Crypto Agency, need to cooperate with internet provider and social media platform and also civil society. This cooperation is essential to establish an early warning system and information sharing system when disinformation activities, terrorist propaganda, and other cyber threat are detected in their platform [32, 54]. In Indonesia, to increase resiliency of society to terrorist propaganda, government institution has been cooperated with civil society, Nahdatul Ulama, to distribute contra narrative and prevent online radicalization. However, in strengthening cyber resilience, Indonesia faces another vulnerability concerning public competition with private ownership of cyber systems. Indonesia relies heavily on private companies to provide the cyber technologies and it makes Indonesia vulnerable to unauthorized access from others parties who acquire similar technology [45]. In this regard cyber resilience also needs to address self-sufficient research and development of cyber technologies by government institutions.

International Cooperation in Addressing Cyber Threat

Indonesia bilateral cooperation in cyber security has been conducted with several countries in broad range of cyber related issues. In March and July 2017, Indonesia and Russia has begun to cooperate in cyber security, prevent cybercrime, and exchange of knowledge of cyber security [60, 61]. Then, in the late January 2018, Indonesia-Australia has strengthened cyber security cooperation to build further cooperative relationship which includes developing commercial partnerships and modelling government-industry ties in the cyber security field [62].

Indonesia also signed a letter of intent on cyber security cooperation with Netherlands in July 2018. This cooperation includes bilateral cyber-dialogue, enhancing capabilities, and share experience on cyber-legislation [63]. A month later, Indonesia signed a memorandum of understanding with UK which covers technological cooperation, capacity building and exchange of expertise on cyber security [64]. After with Netherlands, Indonesia and the United States signed a Letter of Intent on Promoting Strong Cyber Space Cooperation in September 2018 [65]. The cooperation between Indonesia and US also expanded to strengthen bilateral cooperation against transnational cyber and financial crime [66].

In addition to the US, Indonesian National Police also agreed with Ukrainian counterpart to enhance the Indonesian National Police's readiness in dealing with various potential of cyber-attacks [67]. Alongside cyber security cooperation with western countries, Indonesia has been actualized cyber defence cooperation with China since January 2016. This cooperation was focused on government responses to cyber war on civil infrastructure, cyber-war simulations, cyber-war responses and mitigations, cyber monitoring, cyber-crisis management, and data centre restoration planning [68]. However, having in mind that cyber threat is evolving threat, it is difficult to find on open sources concerning systematic process to detect and measure, on regular basis, potential cyber threat and damage to Indonesia national security. In that cooperation, consecutive coordinated communication in cyber space between parties also limited, if any.

In regional level, Indonesia takes active role to identify and implement cyber norms and confidence building measures (CBMs) through ASEAN and ASEAN Regional Forum (ARF) framework [69]. Even though, ASEAN Cyber Security Cooperation Strategy was formulated to coordinate cyber policies in 2017 [69], ASEAN member states have diverse perspective on cyberspace governance which affects ASEAN-cantered cooperation [69]. In this situation, Indonesia need to foster practical information sharing mechanism in ASEAN and ARF, to initiate cyber crisis mechanism, and regular cyber meeting or dialog to increase trust and expand cyber security collaboration. Indonesia can propose the establishment of cyber defence centre to enhance ASEAN's cyber defence and security capability such as NATO Cooperative Cyber Defence Centre of Excellence (NATO CCD COE).

In multilateral level, Indonesia takes active role in UN Group of Governmental Experts on Information Security (UN GGE) to create international norms on cyber security [70]. During the General Assembly in early November 2018 which adopted two separate resolutions on the actions of states in cyberspace, Indonesia alongside with Malaysia and the Philippines commented that they would have preferred a single resolution, however a small group of experts (a new GGE proposal from US) and a much larger group of generalists (open-ended working group/OEWGs proposal from Russia) could complement each other, and raise awareness of cyberspace challenges within the entire UN membership [71].

In sum, current cooperation in cyber security and cyber defence will provide Indonesia with experience, technical know-how, regulation, mitigation effort, and response to cyber related threat. Through this cooperation and Indonesian free and active foreign policy, Indonesia can play substantial role in international cyber security governance, bridging the western democracies and authoritarian regime in securing cyber space. Indonesia should organize an effort to complement the cyber security discourse with international norms, regulation, or value, due to the formulation of customary international law on cyber security may take time. It means that Indonesia need to design, not to create a new platform in cyber security. The creation of new framework such as "Paris Call For Trust and Security in Cyberspace" a week before General Assembly resolutions on the actions of states in cyberspace would made cyber norms formulation even more unfocussed [71].

6. Conclusion and Recommendation

Almost all aspects of Indonesian life are currently connected to cyber space. It has been created new security threat such as, cybercrime, cyber terrorism, cyber espionage, hacktivism, digital misinformation, and cyber war. Those threats have been created financial lose, social conflict, and national insecurity. In addressing those threats, Indonesia has established National Cyber and

Crypto Agency in 2017, strengthen government/public-private sector cooperation, strengthen cyber resilience, and expand international cooperation. With those policies, Indonesia can use current mechanism to propose the confidence building measure, minimize cyber security dilemma, and prevent malicious action in cyber space and promoting a secure cyber space for national security and human prosperity.

At the end, we recommend that Indonesian governments need to increase cyber awareness through digital literacy and development of proactive community. This effort also requires community resilience and tenacity from cyber-attack. A strong community will enhance Indonesian security in cyber space. Therefore, in national level, Indonesia should adopt international best practice and develop national cyber security mechanism. This mechanism can consist of standard guidelines of sharing information, detect and measure of potential cyber threat on regular basis, and disaster recovery plans. It will require a lot of coordinated efforts from all stakeholders, private sector, academia, expert, cyber related R&D, and international community to obtain the best possible result.

References

[1] Weimann, G. March 2004. How Modern Terrorism Uses the Internet. United States Institute of Peace-Special Report 116.

[2] Barker, A. 2019, March 30. Indonesia's election sees internet trolls try to bring down President Joko Widodo. Retrieved May 6, 2019, from abc.net.au

[3] Harsono, N. 2019, February 22. Businesses as risk: Experts sound alarm on cyberthreat. Retrieved May 6, 2019, from The Jakarta Post.

[4] Valeriano, B., & Maness, R. C. 2018. International Relations Theory and Cyber Security: Threat, Conflict, and Ethics in an Emergent Domain. In C. Brown, & R. Eckersley, The Oxford Handbook of International Political Theory. (Oxford : Oxford University Press.)

[5] Stevens, T. 2016. Cyber Security and The Politics of Time. (Cambridge : Cambridge University Press.)

[6] Stevens, T. 2018. Global cybersecurity: New directions in theory and methods. Politics and Governance 6(2). https://doi.org/10.17645/pag.v6i2.1569.

[7] Hansen, L., & Nissenbaum, H. 2009. Digital Disaster, Cyber Security, and the Copenhagen School. International Studies Quarterly 53(4).

[8] Reardon, R., & Choucri, N. April 2012. The Role of Cyberspace in International Relations: A View of the Literature. Paper Prepared for the 2012 ISA Annual Convention.

[9] Isnarti, R. November 2016. A Comparison of Neorealism, Liberalism, and Constructivism in Analysing Cyber War. Andalas Journal of International Studies 5(2).

[10] Crosston, M. D. 2011. World Gone Cyber MAD: How 'Mutually Assured Debilitation' is the Best Hope for Cyber Deterrence. Strategic Studies Quarterly 5(1).

[11] Dewar, R. S. September 2018. National Cybersecurity And Cyberdefense Policy Snapshots. ETH Zürich-Center for Security Studies (CSS)

[12] Oleksiewicz, I. 2016. Dilemmas and Challenges For EU Anti-Cyberterrorism Policy: The Example Of The United Kingdom. Teka Kom. Politol. Stos. Miedzynar 11(3).

[13] Tempo.co. 2018, October 19. Cyber Crime Costs Indonesia More than Rp33 M. Retrieved May 19, 2019, from Tempo.co

[14] Ervìani, N. K. 2018, May 1. 103 Chinese nationals arrested for alleged cyber fraud. Retrieved May 1, 2019, from The Jakarta Post

[15] Suherdjoko. 2019, April 22. 40 Chinese, Taiwanese nationals arrested for cybercrimes in Semarang. Retrieved May 22, 2019, from The Jakarta Post

[16] The Jakarta Post. 2019, February 16. Meeting dates on Facebook? Beware of 'sextortion'. Retrieved May 16, 2019, from The Jakarta Post

[17] Klein, J. J. Winter 2015. Deterring and Dissuading Cyberterrorism. Journal of Strategic Security 8(4). http://dx.doi.org/10.5038/1944-0472.8.4.1460.

[18] Chew, A. 2018, August 23. Pro-Islamic State Hacker threaten terror attack against Indonesian government. Retrieved May 23, 2019, from channelnewsasia.com.

[19] Nugraha, R. 2015, March 13. "One Way Jihad" demi Kekhalifahan Islam. Retrieved May 13, 2019, from www.dw.com.

[20] Institute for Policy Analysis of Conflict (IPAC). 13 May 2016. ISIS in Ambon: The Fallout from Communal Conflict. (Jakarta: IPAC).

[21] Reuters. 2016, August 12. Malaysia arrests Islamic State suspects for grenade attack on bar in June. Retrieved May 12, 2019, from Reuters.

[22] Barlow, J. 2010. Cyber War and U.S. Policy: Part I, Neo-neorealism. The journal of education, community and values 310(5).

[23] Weaver, M. 2009, July 8. Cyber attackers target South Korea and US. Retrieved May 8, 2019, from theguardian.com.

[24] Gorman, S., Cole, A., & Dreazen, Y. 2009, April 21. Computer Spies Breach Fighter-Jet Project. Wall Street Journal.

[25] CNN. 2009, July 8. U.S. government sites among those hit by cyberattack. Retrieved May 8, 2019, from CNN.

[26] The Jakarta Post. 2018, March 14. Surabaya Black Hat reportedly hacks national companies, US govt websites. Retrieved May 14, 2019, from The Jakarta Post.

[27] Woolley, S. C., & Howard, P. N. 2019. Introduction: Computational Propaganda Worldwide. In S. C. Woolley, & P. N. Howard, Computational Propaganda: Political Parties, Politicians, and Political Manipulation On Social Media. (Oxford : Oxford University Press.)

[28] Potkin, F. 2019, April 29. Backstory: Hunting for fake news and trolls in Indonesia's elections. Retrieved May 29 , 2019, from Reuters Backstory.

[29] Center for Digital Society. 2019, April 18. The Threats of Cyber Attack in Indonesian Election 2019. Retrieved May 18, 2019, from Center for Digital Society.

[30] Clarke, R. A., & Knake, R. K. 2010. Cyber War: The Next Threat to National Security and What to Do About It. (New York: Harper Collins.)

[31] Greenberg, A. 2017, June 20. How an entire nation became Russia's test lab for cyberwar. Retrieved May 20, 2019, from Wired.

[32] Polyakova, A., & Boyer, S. P. March 2018. The Future Of Political Warfare: Russia, The West, And The Coming Age Of Global Digital Competition. The Brookings Institution

[33] Sinopoli, A. F. January 2012. Cyberwar and International Law: An English School Perspective. (University of South Florida-Graduate School).

[34] Ashmore, W. C. 2009. Impact of Alleged Russian Cyber Attacks. Baltic Security & Defense Review 11(1).

[35] Shackelford, S. J. 2009. From Nuclear War to Net War: Analogizing Cyber Attacks in International Law. Berkeley Journal Of International Law 27(1).

[36] Farwell, J. P., & Rohozinski, R. 2011. Stuxnet and the Future of Cyber War. Survival 53(1).

[37] Nakashima, E. 2012, May 28. Newly identified computer virus, used for spying, is 20 times size of Stuxnet. Retrieved May 28, 2019, from The Washington Post.

[38] Zetter, K. 2017, March 3. Inside the cunning, unprecedented hack of Ukraine's power grid. Retrieved May 3, 2019, from Wired.

[39] Bajak, F., & Satter, R. 2017, June 30. Companies still hobbled from fearsome cyberattack. Retrieved May 30, 2019, from Associated Press: https://www.apnews.com/ce7a8aca506742ab8e8873e7f9f229c2/Companies-still-hobbled-from-fearsomecyberattack

[40] reuters.com. 2017, May 14. Indonesia warns of more cyber attack havoc as business week starts. Retrieved May 14, 2019, from reuters.com.

[41] Supriyadi, D., & Dethan, K. E. 2018, May 14. On the lookout for cyberwar. Retrieved May 14, 2019, from The Jakarta Post.

[42] Budianto, E. E. 2018, September 17. Foto alat vital tersebar, Perangkat desa ngaku jadi korban pemerasan. Retrieved May 17, 2019, from m.detik.com.

[43] Bhayangkara, C. S. 2018, March 28. 6 Informasi Hoax yang fenomenal hingga telan korban. Retrieved May 28, 2019, from News.Okezone.com.

[44] Lewis, J. A. December 2002. Assessing the Risks of Cyber Terrorism, Cyber War and Other Cyber Threats. Center for Strategic and International Studies.

[45] Strinde, G. Spring 2011. Cyber warfare: Connecting classical security theory to a new security domain. (Lund University.)

[46] Bolsover, G. 2019. China:An Alternative Model of a Widespread Practice. In S. C. Woolley, & P. N. Howard, Computational Propaganda: Political Parties, Politicians, And Political Manipulation On Social Media. (Oxford : Oxford University Press).

[47] kominfo.go.id. 2018, september 25. CIIP-ID Summit 2018 Tingkatkan Koordinasi Proteksi Keamanan Siber Indonesia. Retrieved May 25, 2019, from kominfo.go.id.

[48] Siboni, G., & Sivan-Sevilla, I. May 2018. The Role of the State in the Private-Sector Cybersecurity Challenge. George Town Journal Of International Affairs.

[49] aptika.kominfo.go.id. 2016, March 10. Kebijakan Keamanan dan Pertahanan Siber. Retrieved May 10, 2019, from aptika.kominfo.go.id.

[50] Metodieva, A. 2018. Disinformation as a Cyber Threat in the V4: Capabilities and Reactions to Russian Campaigns. Strategic Policy Institute.

[51] Raduege, H. D. 18 June 2013. The Public/Private Cooperation We Need on Cyber Security. Harvard Business Review.

[52] Knake, R. K. 2018, May 15. Sharing Classified Cyber Threat Information With the Private Sector. Council on Foreign Relations.

[53] Solon, O., & Wong, J. C. 2016, December 16. Facebook's Plan to Tackle Fake News Raises Questions over Limitations. Retrieved May 16, 2019, from The Guardian.

[54] Neudert, L.-M. N. 2019. Germany: A Cautionary Tale. In S. C. Woolley, & P. N. Howard, Computational Propaganda: Political Parties, Politicians, And Political Manipulation On Social Media. (Oxford : Oxford University Press.)

[55] republika.co.id. 2015, September 22. NEC and ID-SIRTII/CC to collaborate on cyber security in Indonesia. Retrieved May 22 , 2019, from republika.co.id.

[56] Tribunnews.com. 2019, March 26. Jaga Infrastruktur Nasional, BSSN Bakal Gelar Pertemuan Keamanan Siber. Retrieved May 26 , 2019, from Tribunnews.com.

[57] beritasatu.com. 2018, November 23. Tangkal Serangan Siber, BSSN Gandeng SGU. Retrieved May 23 , 2019, from beritasatu.com.

[58] Kello, L., Martinovic, I., Strohmeier, M., & Egloff, F. 2017. A Cybersecurity Threat Model for a Combined Cyberattack against Hospitals and Terrorist Attack in Spain. (Oxford University - Universidad Autónoma de Madrid Project Report).

[59] UK Government. 2016. National Cyber Security Strategy 2016-2021. UK Government.

[60] antaranews.com. 2017, March 23. Indonesia, Russia explore cooperation in cyber security. Retrieved May 23, 2019, from antaranews.com.

[61] Sheany. 2017, July 24. Russian Companies to Seek Cooperation With Indonesia on IT, Cybersecurity. Retrieved May 24, 2019, from jakartaglobe.id.

[62] austrade.gov.au. 2018, January 31. Indonesia-Australia Digital Forum, Cyber Security.

The Policy Strategy for Defense Industry to Cross the Death Valley of Technology – IIDSS2019

Dorothea S Jasi, Romie O Bura

Defense Industry Program, Faculty of Defense Industry, Indonesia Defense University
Lecturer of Defense Industry Program, Faculty of Defense Industry, Indonesia Defense University

E-mail: dorothea.jasi@gmail.com, romiebura@idu.ac.id

Abstract. Developing methods and instruments that can bridge the process stage in policy programmes as an urgent agenda. This connecting bridge is in Technology Readiness Level stage 4 to 7 which an area known as the death valley of technology, that describes the discontinuity in the innovation process. This condition occurs when there is a transition process from research entering the trial phase which will be commercially produced in the industry. This study presents a comparison of methods from various literature to design a bridge model that can be applied in the defence industry. The defence industry in Indonesia requires the synergy from research institutions, industry and the government known by triple helix to be able being the self-defence industry. The right methods and instruments in the technology transfer process will accelerate the development of the national defence industry, also be the guidance to develop more invention.

1. Introduction

The defense industry and the economy of a nation are closely intertwined. With relatively consistent, economic growth, Indonesia has a golden opportunity and momentum to grow as a major player of the worldwide defense industry. Currently, research in the Indonesian defense industry has not able to quickly develop as expected because of research problems. Nowadays the defense products must have good technological capabilities, while the research problem becomes very important. Through good research, the Indonesian defense industry will have the quality of competing for domestic products, the availability of advanced technology is great support for the formation of manpower forces in national defense. But in reality, that condition cannot be fulfilled so it assumes will weakening national defense forces [1].

The strong defense must remain pursued so Indonesia ready to face all threats to existing the country based on the existence of advanced defense industry. The effort to prepare a strong and established defense industry is one of the best ways to deal with war, therefore, it must be ready as early as possible. The rise and growth of the defense industry mirror the success of technological development, the empowerment of people while increasing the strength of national defense as a nation [2].

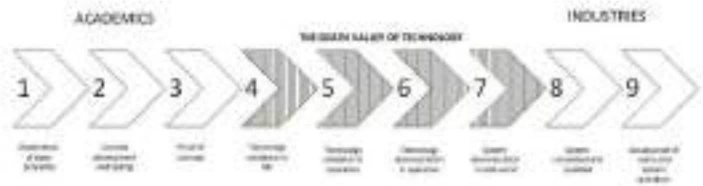


Figure 1. TRL and The Death Valley

2. Research Methodology

This paper uses the literature review as a basis of preparing a conceptualization for crossing the valley of death, specifically to assess the mastery of technology with TRL. Starting with studying the gaps in research which often kills many discoveries that beneficial to the development of the defense industry. To cross the death valley, it is not enough by only cooperate academics with industry, but also by the strong support of the government as the regulator. Therefore, triple helix synergy is a basic foundation for forming a final solution model which can be applied to the defense industry in general.

3. The Death Valley Of Technology

The death valley of technology is a metaphor that describes a critical area of the innovation process in technology transfer, where there is a gap between academic-based innovation and the application process of these products in commercial markets [5]. The first use of the Death Valley metaphor was conducted by Vern Ehlers to show the gaps that must be bridged in technology transition efforts. Ehler stated that valley of death is a market failure which impedes the long-term applied research needed to turn scientific discoveries into marketable products [6].

There are various reasons why technology transitions do not happen easily. It is not caused by researchers who do not support the transition, because most of them assuming the result must have an impact [7]. Valley of death was known as a symbolic barrier to government-sponsored innovation, where technology with the potential to increase military capabilities is lost due to lack of funds from public or private sources. There is a huge negative consequence associated with the death valley: without funding the final stages of TRL Level 7, 8 and 9, the government support for first research and development (R&D) will fail to have a positive impact on economic growth and military innovation [8].

The process of innovation with linear models through technological impetus starts from basic sciences to design and techniques for the manufacturing process until marketing and sales are carried out. In this model, the role of the academics is often fundamental. It shows that innovation must be seen as an evolutionary, non-linear and interactive process, which requires intensive communication and collaboration between industry and organizations such as academics and government institutions. Seeing this condition, the policy made does not only focus on basic research and technological aspects of innovation but also comes with organizational, skills, financial and commercialization aspects of the innovation [9].

The conceptualization of technology transfer is often described as a form of obstacles and bridges to success [10]. It is known by many academics hard to identify the innovations that arise from their researches, patent the results then look for businesses to take licenses for commercialization. Only a few innovations has arrived at the licensed stage in the industry, while the rest died in the valley of death [11].

In a newly established industry, there are two crossings from the valley of death. First, the process of physical conversion of value-oriented science and technology which transforming technological innovation to real products on the market; This first crossing coincides with industrializing profit-oriented technology, to realize technology into a commodity and able to socially produce goods in bears. Second, transform products to commodities related to the scale of production and quality [12].

The death valley in the Indonesian defense industry has experienced by many transitional challenges from the results of research conducted in government research institutions and academics to enter the commercialization stage in the industry. Not only the process in different areas but also half-quick the results from research come with new market demand does not simultaneously, where the industry often requires fast and precise results while the academics are constrained by conditions of changes in governance and the researchers which ultimately caused a delay. In this condition a synergy of the three parts of the triple helix is urgently needed, together government, industry and academics cross the death valley of technology.

4. Triple Helix Synergy As A Bridge Base

The importance of research in the industry is a step to harvest the results of basic research that benefit society. The gaps which have been resulted in creating a valley of death occur when academic research becomes more fundamental, while applied research increasingly shifts towards product development. In this condition, the discovery might be beneficial for the lost community into the abyss of death or forgotten because unable to cross the valley of death. Bridges available between the two do not follow a straight track but have complex and interactive relationships. As a result, truly innovative research in industry is necessary and must be encouraged [13].

In market analysis, the defense sector can be divided into two sides, namely the supply whose role is played by the defense industry, and demand from the government as the defense provider. It is known as the characteristics of market defense is monopsony while the most important aspect of the relationship between customers and suppliers is the size and predictability of demand [14]. The government have multi-role as a user, sponsor and regulator of the defense industry with the responsibility to encourage research to be able to cross the valley of death. The government can help develop innovation through several efforts including transparency of defense needs, basic research funding, tax policy, assisting in applied research, and rewarding innovation.

The first policy which the government needs to do as a customer is transparency in planning procurement of defense equipment, it will help the process of consolidating the defense industry. The government determines the demand for the defense industry in the country through how much defense spending. If customers are able to provide information about future needs, they will help the supplier to develop their plans and investments for the best outcome for them. The problem is transparency of government about the certainty planning expenditures and future needs can vary greatly because the amount of the budget is sometimes uncertain. With transparency, the defense industry can propose the right products, calculate future demand also focus on funding for specific research and product development activities [15].

The mindset of determining first needs is determined by the Government as a user unilaterally. In the process of the synergy of Triple Helix, the view from the industry as a supplier can be used as one of the considerations to plan the budget for the ministry of defense. If there is a new mindset where all planning involves coordinating the three parts of Triple Helix, Indonesia is one step forward towards independence of the domestic defense industry.

The second policy is about tax incentive such as R&D tax credits must be made permanent. Uncertainty about the existence of tax credits from year to year inhibits innovative, long-term multi-year research in the industrial sector. The regulations made must be shortened to not be burdensome for the industry. In addition, partnerships between government, academic and industrial laboratories must also be promoted [16].

South Korea's success in high-tech industries makes its economy based on high-tech exports also supported by Korea's government by providing fiscal incentives in the form of tax credits as well as decreasing import tariffs on R&D-related goods [17]. As a regulator, the government can synergise a strong Triple Helix foundation, Higher Education / Science and Technology Institutions play a role in producing innovation and Industry whose role is to create and the urgency for the innovation of Defense and Security Equipment Tools, realize the tools innovation ecosystem to fulfil reliable and ready defense postures, these collaboration shown in figure 2.

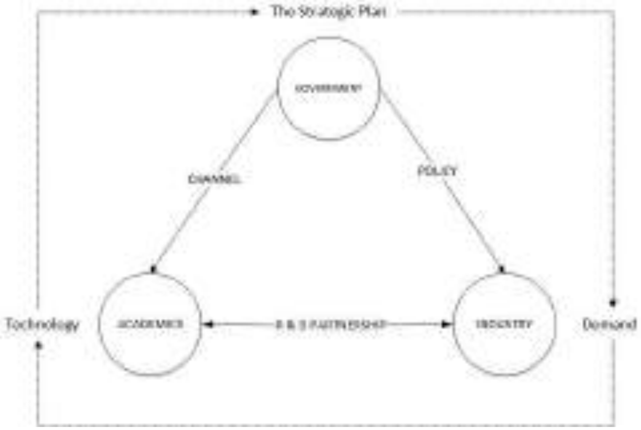


Figure 1. Triple Helix Model

5. Bridging The Death Valley Of Technology

Furthermore, new technological innovations will make changes if they can be used to the fullest. It does not matter how visionary a technology is if the technology was able to meet the needs and requirements from the user, and available as an acceptable product. In a congressional report on change technology, citing evidence of the gap between Science and Technology (S&T) and the acquisition community, namely the valley of death can be bridged only through collaborative and investment efforts by the two communities [18]. In this model, the company obtained the leading of R&D collaboration, with some being supported by the government, while the academics and its staff were satisfied knowing the innovations had been carried out were quickly and efficiently transferred to the industry. This certainly can help narrow the Valley of Death, in some cases it can ease the connection between academics research and industry applications [19].

Former CEO of Lockheed Martin, the biggest defense industry in the US stated the importance of a long-term investment plan on R&D. Spin-off companies which doing R&D partnerships with large companies able to create cash returns for universities through royalties. R&D partnerships are the ideal environment to applied R&D, bridging the gap between academia and industry [20].

In accordance with Law Number 16 of 2012, the defense industry is requested to give at least 5% of net income for research and development purposes, where the government does not give funding for research activities. Funding innovation is one of the efforts that can be made by the government to accelerate the growth of technological innovation in Indonesia. By providing the right funding, a strategy can be decided to accelerate the downstream process of the discovery and breakdown of the obstacles that caused the failure of the innovation process.

The technology transition is a requirement to spreading new innovations and a major consideration for all R&D investments. It requires the federal government to move past work models where most R&D programs support the most limited operational evaluations or experiments, most R&D program managers consider their work to be done with the final report, and most research participants consider their work to be carried out by publication. Future R&D activities need to focus on real goals, technology transition. Current Main Investigators (R&D) and Program Managers are not rewarded for technology transitions. Academic are valued for publication, not transitions. Future government-funded R&D programs need to reward program managers and government for transition progress.

To change the innovation landscape is the R&D process needs to ensure that organization spend program's funds for technology transitions and have sufficient program funding to fund less research, but together valuable needed to bridge the transition gap [21].

6. Conclusion

Technology Readiness Level is needed to help the defense industry in Indonesia to be able to operate effectively and efficiently, so it can cross the valley of death by maximizing the role of the triple helix. First, to ensure transparency in planning procurement of defense equipment. Second, with the certainty policy of tax incentives. When both of these has been fulfilled, the R & D partnership will be easier to do because it already has legal guarantees and ease in taxes. Thus, Indonesia is one step forward towards the independence of the defense industry.

References

[1] Karim S 2014 Membangun Kemandirian Industri Pertahanan Indonesia (Jakarta: PT Gramedia – Kepustakaan Populer Gramedia)

[2] Karim S 2014 Membangun Kemandirian Industri Pertahanan Indonesia (Jakarta: PT Gramedia – Kepustakaan Populer Gramedia)

[3] Karim S 2014 Membangun Kemandirian Industri Pertahanan Indonesia (Jakarta: PT Gramedia – Kepustakaan Populer Gramedia)

[4] Venkata K K U, Venkataramana G, Shanmugam K, Souihi N, and Mats T 2017 Advancing game changing academic research concepts to commercialization: A Life Cycle Assessment based sustainability framework for making informed decisions in Technology Valley of Death (USA: Elsavier)

[5] Gulbrandsen K E 2009 Bridging the valley of death : The rhetoric of technology transfer (Iowa State University)

[6] Lubell M S 2015 Bridging the Innovation Valley of Death

[7] Maughan D and Balenson D 2013 Crossing the Valley of Death : Transitioning Cybersecurity Research into Practice. IEEE Security & Privacy Magazine, Vol. 11, No. 2, pp. 14-23.

[8] Avrett J T, Cordes A M, Ewart R M 2014 Rapid Innovation in the Air Force: Pushing Innovative Space Technologies Across the Valley of Death. CA AIAA SPACE 2014 Conference and Exposition

[9] Hudson J and Khazragui H F 2013 Into the valley of death: Research to innovation Drug Discovery Today, vol. 18, no. 13-14, pp. 610-613.

[10] Coppola N 2007 Communicating green innovation technology: Transfer in a university-business-government consortium. Comparative Technology Transfer and Society, 5, pp 233-252.

[11] Williams E 2004 Crossing the valley of death. Research and Development (University of Warwick)

[12] Gou J, Li J, and Ruan P 2014 Study on the Formation of Emerging Industries Based on Industry Philosophy. International Conference on Management and Engineering (CME 2014), ISBN: 978-1-60595-174-4.

[13] Rodriguez L 1999 Materials in a New Era Proceedings of the 1999 Solid State Sciences Committee Forum.

[14] Karim S 2014 Membangun Kemandirian Industri Pertahanan Indonesia (Jakarta: PT Gramedia – Kepustakaan Populer Gramedia)

[15] Karim S 2014 Membangun Kemandirian Industri Pertahanan Indonesia (Jakarta: PT Gramedia – Kepustakaan Populer Gramedia)

[16] Rodriguez L 1999 Materials in a New Era Proceedings of the 1999 Solid State Sciences Committee Forum.

[17] Amir H, Hastiadi F 2015 Dinamika Kebijakan Fiskal Merespon Ketidakpastian Global (Jakarta : PT. Gramedia Pustaka Utama)

[18] Maughan D and Balenson D 2013 Crossing the Valley of Death : Transitioning Cybersecurity Research into Practice. IEEE Security & Privacy Magazine, Vol. 11, No. 2, pp. 14-23.
[19] Williams E 2004 Crossing the valley of death. Research and Development (University of Warwick)
[20] Williams E 2004 Crossing the valley of death. Research and Development (University of Warwick)
[21] Maughan W D 2010 Crossing the "Valley of Death": Transitioning Research into Commercial Products - A Personal Perspective. IEEE Symposium on Security and Privacy.

Towards a New Concept of Counterterrorism in Indonesia: a Gender-Sensitive Approach – IIDSS2019

R. Widya Setiabudi Sumadinata[1], Dina Yulianti[1] and Otong Sulaeman[2]

[1]International Relations Department, Padjadjaran University, Jalan Raya Bandung-Sumedang KM 21, Sumedang, 45363, Indonesia
[2]Sadra Islamic College, Jalan Lebak Bulus 02/02, Jakarta, 12440, Indonesia

E-mail: dina14@unpad.ac.id

Abstract. Over the past few years, more and more women have been related to terrorism as both victims and perpetrators. In the symposium organized by the Counter-Terrorism Committee Executive Directorate (CTED) and the UN Women (2018), it was stated that further research was needed in accordance with the local context to better understand the gender dimension of terrorism and counterterrorism. This article offers a close examination of the BNPT Blueprint 2014, Indonesia's counterterrorism design plan. BNPT (National Agency for Combating Terrorism) is a ministry-level institution serving as the center force to handle terrorism in Indonesia. The authors found that this blueprint has not applied any gender-sensitive approach. Therefore, the authors offer several recommendations for improvements.

1. Introduction

In 2018, 43 year-old Puji Kuswati and her two daughters, Fadhila Sari and Famela Risqita who were respectively 12 and 9 years old, came to a church called Gereja Kristen Indonesia on Diponegoro Street in Surabaya on Sunday (5/13) around 7.30 AM. Unfortunately, that visit resulted in a devastating shock when it was revealed that the three of them had bombs tied around their bodies, thus causing an explosion just outside of the church building. The explosion killed all of the three preparators with seven other people hurt. The next day (5/14), another woman named Tri Ernawati (43) with her husband named Tri Murtiono showed up at the gate of Surabaya City Police Headquarter (Polrestabes) as suicide-bombers.

They were two among a number of women who had committed acts of terrorism in Indonesia in the past few years. Other names such as Dian Yulia Novi, Ika Purnama Sari, Siska Nur Aziah, Dita Siska Millenia, Solimah, Roslina, and Yuliati had also been either apprehended or died in suicide-bombings. According to Sidney Jones, Director of the Institute for Policy Analysis of Conflict, 45-50% of Indonesian citizens who were sent home from Turkey borders on their way to Syria to join the terrorist organization ISIS were women and children. [1] In addition, a survey published by the Center of Islam and Society Study (PPIM) UIN Syarif Hidayatullah Jakarta (2018) on Islamic Education teachers for various levels in Indonesia showed a highly concerning result of intolerance and radicalism in teachers with 50% and 46.09% of the total respondents respectively. Among those numbers, it was also found that female teachers had even more prejudiced and radical mindset. [2]

On the other side of the coin, women have also undoubtedly been victims of terrorism. Women have been victims of numerous kidnappings and rapes. They have lost their families in terrorist acts. An indirect way for women to be victims of terrorism also happens as the result of counterterrorism efforts such as social exclusions of women who have family ties with terrorism suspects or even detention of innocent women for receiving information about their suspected male relatives.[3]

It can be concluded that there are at least four dimensions of women involvement in terrorism: women as direct victims of terrorism acts, women as perpetrators, women as indirect victims of counterterrorism efforts, and women as counterterrorism activists. In response of these complex dimensions of women in terrorism cases, many have recommended a more thorough approach in counterterrorism policies to include more specific perspectives of gender and local contexts.

In this article, the authors examine the BNPT Blueprint 2014, a design plan of the Indonesian Government's effort in countering terrorism and radicalism, from a gender perspective and recommend several improvements. This article is divided into three parts: conceptual framework of gender-sensitive approach, the review and analysis of BNPT Blueprint 2014, and conclusion.

2. Conceptual Framework of Gender-Sensitive Approach

The concept of gender refers to the social constructions of women and men who are dynamic in nature, varying over time, place, and culture in which they live. 'Gender' is different from 'sex' which refers to human biological and physiological characteristics. The concept of gender rejects the social construction that places women as second class creatures and calls for gender equality. Meanwhile, gender equality means that "different behaviour, aspirations and needs of women and men are considered, valued and favoured equally" [4] In other words, gender equality does not mean equating women and men, but it views that both sexes must be treated fairly and sex should not be used as a basis for their assessment.

When we use 'gender-sensitive approach', it means that we consider gender in our approach towards a phenomenon. In other words, citing Frohlich (2014), we avoid "incorrect differentiation between men and women by placing one gender in a hierarchical position relative to the other in a certain context, as a result of stereotypical images of masculinity and femininity" [5]. UN Counter-Terrorism Committee in 2018 stated that women's equality was a powerful factor preventing violent extremism. [6]

According to Cristina Goni, a gender expert, there are 3 reasons why a gender-sensitive approach towards radicalism and counter-radicalism is important: first, because much evidence shows that gender-sensitive security policies are more effective and lead to civilian accountability. Second, this policy complies with international human rights law and standards, such as Resolution 2242 concerning the role of women in counterterrorism. Third, this approach is important because it can counter the narratives of the terrorist organizations that manipulate gender by using the jargon of 'women's rights' or 'respect for women' and 'women's role in the Caliphate'. Goni emphasized that involving women's human right groups at the grassroots level would have a positive impact on security. [7]

In 2017, the Canadian Government, after conducting consultations involving more than 15,000 people in 65 countries, launched a program called the Feminist International Assistance Policy, which was based on the idea that "gender equality and the empowerment of women and girls is the best way to build a more peaceful, more inclusive and more prosperous world". To achieve this goal, what needs to be done is "to protect and promote the human rights of all vulnerable and marginalized groups and increase their participation in equal decision making. This will help women and girls achieve more equitable access to and control over the resources they need to secure ongoing economic and social equality." [8]

UN Resolution A/RES/60/288 paragraphs 13 pushes member states to engage women leaders and women's organizations in establishing a design or blueprint to counter terrorism and "violent extremism which can be conducive to terrorism, including through countering incitement to commit terrorist acts, creating counter narratives and other appropriate interventions, and building their capacity to do so effectively." [9]

Furthermore, United Nations Secretary General's Plan of Action and the Working Group on Radicalization and Extremism recommended the importance of empowering women to play an active role in preventing terrorism and keeping marginal communities from creating terrorists. Unfortunately, as reported by the UN Special Rapporteur, the involvement of women in the planning, priorities and implementation of national security is still very uneven at the national and international levels. [10]

3. Review and Analysis of BNPT Blueprint 2014

In 2014, BNPT (Indonesia's National Agency for Combating Terrorism) published a blueprint which contains universal prevention policies and strategies for hindering terrorism. The terrorism prevention program covers the areas of prevention, protection, and deradicalization. This blueprint involves all parties nationally so that the implementation of this designed policy can be carried out comprehensively in a targeted, structured, and sustainable manner. [11]

It is stated in the blueprint that in 2002, the Government of Indonesia issued Peraturan Pemerintah Pengganti Undang-Undang (Government's Regulation) No.1 on the elimination of terrorism acts. The blueprint mentioned that this regulation is "a strategic and responsive policy in combating terrorism to strengthen public order and safety. The regulations uphold the law, human rights, and are not discriminatory based on ethnicity, religion, race, or between groups." [12] It does not mention about gender discriminatory.

The Blueprint also identified 5 steps for preventing terrorism: intensifying the role of the Terrorism Prevention Coordination Forum and the involvement of related ministries/agencies; increasing supervision and counter-propaganda in cooperation with the Intelligence Agency; increasing the role of the educational, religious and community institutions; raising public awareness of the dangers of terrorism; and developing the deradicalization program in detention centers, prisons, and the community environment. [13] Again, women are not mentioned in these 5 steps.

BNPT Blueprint categorizes groups that carried out acts of violence in Indonesia into 3 types: (1) militia groups, those who commit acts of violence due to social conflicts, (2) separatist groups, those who do violence because they wanted to separate themselves from the Republic of Indonesia, and (3) radical terrorist groups, those who execute terror attack based on religious doctrines.[14] Chapter 4 of the blueprint discusses the 3rd group further and explains that most terrorism acts in Indonesia are based on a narrow interpretation of Islamic teachings.

It is written on the blueprint:

...acts of terror in the name of religion usually arise as a result of a literal religious understanding, which is based on text alone without relating it to the surrounding context. Such understanding will eventually give birth to fanatical and militant traits that lead to a view that assumes that only he owns the truth. Such attitude will lead to the birth of terrorism if it is supported by a socio-political environment that is believed incorrect and oppressive. Such conditions will result in acts of terrorism. [15]

The blueprint divides the community into 5 clusters: (1) intellectual actors, (2) executors, (3) individuals or groups that provide supporting facilities for acts of terrorism (4) sympathizers who have the potential to support the terrorism movement but are not involved terrorist acts and (5) the general public who are vulnerable to being subjected to the spread of radical ideologies of terrorism. [16]

In general, it can be concluded that women have been broadly invisible in this blueprint. Women are only mentioned twice: (1) women's organizations must be involved in counterterrorism efforts and (2) the Ministry of Women's Empowerment and Child Protection must be involved in the design of a system protecting the children of terrorism victims and the children of the terrorists. [17] However, this is inadequate in fulfilling the UN Resolution A/RES/60/288 that has been mentioned earlier.

Moreover, the number of terrorism acts involving women is increasing. According to the Indonesia's Directorate General of Penitentiary as of October 2016, since the enactment of Law of Terrorism No. 15 of 2003, 9 women have been charged with being perpetrators of terrorism and most of them are/were wives of terrorists. The involvement of woman in terrorism crimes is dominated by kinship system relations; they were recruited into the terrorist network by their husbands, fathers, brothers, uncles, or even their sisters. [18]

Thus, the authors recommend that the blueprint must consider the four dimensions of women involvement in terrorism: women as direct victims of terrorism acts, women as perpetrators, women as indirect victims of counterterrorism efforts, and women as counterterrorism activists.

In this article, the authors explore the complex dimensions of women as perpetrators and as victims. By using a gender-sensitive approach, we will be able to provide careful judgments, not merely using traditional security approaches.

At least, there are two dimensions that must be considered in countering terrorism involving women:

(1) Women as the Collateral Victim of Counterterrorism Measures

As stated in UN Doc A/64/211, counterterrorism measures sometimes cause women to become collateral victims, such as unlawful detention and mistreatment of women and children in order to obtain information about male family members suspected of committing terrorism. For this reason, the United Nations recommends that women and families of terrorist perpetrators must be protected by privacy laws and guaranteed justice; they should get compensation for human rights violations that occurred, including economic, social and cultural rights. [19]

The interview conducted by Taskarina to Umi Yazid proved the existence of a collateral victim, where a woman who initially did not know that her husband was committing an act of terror and only intended to accompany her husband was finally sentenced to prison as a terrorist. [20]

Human rights violations and discrimination experienced by women when their husbands were arrested or killed in terrorism crimes will create an ecosystem for the continuation of a cycle of violence, revenge against the state, and vulnerability of children being drawn into terrorist networks. Therefore, counterterrorism must be prudent in distinguishing between victims and perpetrators.

(2) Women as Victims of Deviant Religious Doctrine

In the cases of women as perpetrators of terrorism in Indonesia, most of them are wives receiving religious doctrines that place women in an inferior position. In their culture and beliefs, women are required to follow whatever is conveyed by their husbands. In some cases, the wives believe that they were doing 'holy war' (jihad); so, they feel obliged to follow their husband. [21] At the same time, in areas controlled by terror groups (ISIS and its affiliates) in the Middle East and Africa, women are being raped, traded as slaves, or killed. In both conditions, women are victims of deviant religious doctrine rooted in the teachings of Wahhabism, one of misguided sects in Islam. This sect views women as follows.

a. Women are evil beings

The Wahhabi advocates the use of hadith texts which portray women as evil and dirty. Women cause men to commit sinful acts, to forget the doomsday (qiyamah), to fall into the muddy world. On this basis, men should stay away from women; otherwise, they will suffer the destruction of the world and the hereafter.

b. Women are inhabitants of hell.

The Wahhabi campaigners use various historical texts and hadith mentioning that the majority of women are prospective inhabitants of hell. They also called women the fuel of hellfire.

c. Woman are part of Satan

The Wahhabists view women and Satan as two inseparable entities. They state that women are the tail of the devil. In other narrations, it is said that when women were created, Satan rejoiced.

With those beliefs, the Wahhabists obstruct women's political activity. Women are prohibited from being involved in political affairs at all levels. Women have no right to be leaders, from regional to state leaders, or to become candidates for the legislative body. Basically, women have no right to vote, because this right can become an entry point for women to surpass the position of men. [22]

In summary, Wahhabi teachings characterize women as fitnah (temptation, sedition) for men. With this assumption, the Wahhabi jurists often produce fatwas (Islamic law) that restrict women's appearance in public sphere, such as the obligation of using niqab (face cover), ban on driving, traveling alone, or working in public areas. They are also required to obey their husbands' wishes. These fatwas use hadith (the statement of the Prophet) interpretations that have vague or disputed base. [23]

Obviously, these kinds of teachings are contradictory to the counterterrorism strategies recommended by some international organizations. The teachings will hinder 'gender equality', 'empowerment of women and girls', 'increasing women's participation in decision making', or 'enhancing women's control over resources'. This school of thought makes the UN Resolution which emphasize the importance of engaging women leaders and women's organizations in establishing the counterterrorism blueprint inconceivable.

By implementing a gender-sensitive approach, women who live and were raised in culture and thoughts based on the doctrine of Wahhabism are victims. They become the object of highly patriarchal indoctrination in the name of religion. These teachings are then internalized within themselves and shape their perspective on themselves and the world. They fully believe that they must obey all orders of their husbands, including their husbands' ask for help in the acts of terrorism. Therefore, the most important thing to do in countering terrorism is emancipating women and disengaging them from the milieu of Wahhabi thought and doctrines.

Finally, these are some recommendations for improving the BNPT Blueprint.

(1) The BNPT should use gender-sensitive approach in the blueprint since it is very important and useful for countering and preventing terrorism.

(2) New categorizations of perpetrators and victims of terrorism need to be added carefully and comprehensively in the blueprint. Further studies on treatments that are appropriate for each category must be done.

(3) Since the root of women involvement in terrorism (as perpetrators and as victim) is Wahhabism, it is very urgent to involve prominent scholars in the field of religion to produce counter-doctrine appropriately and logically.

(4) It is important to evaluate the past counterterrorism measures involving women with a gender-sensitive approach.

(5) The blueprint must include the recommendation of the United Nations Resolution A/RES/60/288 regarding the active involvement of women in answering provocation to perform violence operations, developing counter narratives for the terrorists' propaganda, and improving their ability to carry out those efforts sufficiently.

4. Conclusion

A number of suicide bombings carried out by women in recent years have attracted the attention of many scholars and peace organizations. At least there are 4 categories of women in relation to terrorism: as perpetrators, as direct victims, as indirect victims, and as peacemakers. The authors conducted a review and analysis of the BNPT blueprint (2014) and found that this blueprint has not implemented a gender-sensitive approach. This article further discusses the distinguishment of women as victims and as perpetrators. It is concluded that many women considered perpetrators of terrorism were actually victims of indoctrination and culture in their communities based on the teaching of Wahhabism. The author recommends 5 points that BNPT needs to consider for upgrading its blueprint, namely: the importance of using a gender-sensitive approach, adding new categorizations of perpetrators and victims of gender-based terrorism, doing research on appropriate treatment in each category, involving prominent scholars to counter Wahhabists' doctrine about women, evaluating counterterrorism actions in the past with a gender-sensitive approach, and accommodating recommendations from the United Nations on the involvement of women in counterterrorism efforts. Further research is still needed, especially related to the second and fourth points.

References

[1]Pusat Studi Agama dan Demokrasi Paramadina 2015 Indonesia Perlu Buat Program Deradikalisasi Khusus Perempuan dan Anak in http://www.paramadina-pusad.or.id/indonesia-perlu-buat-program-deradikalisasi-khusus-perempuan-dan-anak/

[2] Convey Indonesia 2018 Survei PPIM 2018: Menyibak Intoleransi dan Radikalisme Guru
in https://conveyindonesia.com/survei-ppim-2018-menyibak-intoleransi-dan-radikalisme-guru/

[3] UN Doc A/64/211 2009 Promotion and protection of human rights: human rights situations and reports of special rapporteurs and representatives in https://www2.ohchr.org/english/issues/terrorism/rapporteur/docs/A-64-211.pdf

[4] Frohlich R 2014 Theoretical/Conceptual Framework for the gender-sensitive perspective in http://www.infocore.eu/wp-content/uploads/2016/02/INFOCORE-conceptual-paper_INFOCOREs-gender-sensitive-Perspective.pdf

[5] ibid

[6] Counter-Terrorism Committee Executive Directorate and UN Women 2018 Summary Report in https://www.un.org/sc/ctc/wp-content/uploads/2018/08/Summary-report_final.pdf

[7] Goni C Gender approach in European counter-radicalization strategies: why, what and how to make it? in https://mindb4act.eu/news/gender-approach-in-european-counter-radicalization-strategies-why-what-and-how-to-make-it/

[8]Global Affairs Canada 2017 Canada's Feminist International Assistance Policy in https://international.gc.ca/world-monde/assets/pdfs/iap2-eng.pdf

[9] UN Resolution A/RES/60/288

[10] UN Doc A/72/43280 2017 Promotion and protection of human rights: human rights questions, including alternative approaches for improving the effective enjoyment of human rights and fundamental freedoms in https://www.ohchr.org/Documents/Issues/Terrorism/A_72_43280_EN.pdf

[11] Deputi Bidang Pencegahan, Perlindungan Dan Deradikalisasi Badan Nasional Penanggulangan Terorisme 2014 Blueprint Pencegahan Terorisme p.6
[12] ibid p.53
[13] ibid p. 55
[14] ibid p.22
[15] ibid p.41
[16] ibid p.58-59
[17] ibid p. 128 and 130
[18] Taskarina L 2018 Perempuan dan Terorisme - Kisah Perempuan dalam Kejahatan Terorisme (Jakarta: Elex Media Komputindo) p. 13, 16
[19] UN Doc A/64/211
[20] Taskarina L 2018 Perempuan dan Terorisme - Kisah Perempuan dalam Kejahatan Terorisme (Jakarta: Elex Media Komputindo) p. 59-73
[21] ibid p. 9
[22] Ali M A M and Rezaei A 2016 Hudud-e Azadi-e Faaliyyat-e Zan az Didgah-e Wahhabiyat in

http://www.jwss.ir/article_49910_0404821d53a38e4d7eb6dbc9fd8011d9.pdf

[23] Gorman B C 2009 The Green Glass Ceiling: Gender Inequality And Wahhabi Political Influence (University of Georgia Department of Religion) p.26

Sea Defense Strategy Implementation Against Asymmetric Warfare Threats for Securing International Shipping Lanes in The Sunda Strait – IIDSS2019

Suhirwan[1], Lukman Yudho Prakoso[2], Dohar Sianturi[3], Agus Adriyanto[4] and Ratna Damayanti[5]

[1]Lecturer of Asymmetric Warfare of IDU, IPSC, Sentul-Bogor, Indonesia
[2,3,4]Lecturers of Sea Defense Strategy of IDU, IPSC, Sentul-Bogor, Indonesia
[5] Student of Doctoral Programme of IDU, IPSC Sentul-Bogor, Indonesia.

E-mail: suhirwan@idu.ac.id; lukman.prakoso@idu.ac.id; dohar.sianturi@idu.ac.id; agus.adriyanto@idu.ac.id; ratna.damayanti@idu.ac.id

Abstract. The Sunda Strait is one of the areas in the Indonesian Archipelago Sea Channel (ALKI) I. The flow of this voyage is used for international interests. Facing the factual and potential threats that occur today, the Sunda Strait waters has an important role for international interest, particularly in Indonesia, since the position of its capital city is relatively close. This study is using a qualitative descriptive method of phenomenology and using the theory of George Edward III. The results of the study indicate that the variable communication between related entities shows that it still needs to be optimized since it is still not integrated. In the variable resources of each entity related to the security of the Sunda Strait are still have many limitations, particularly in budgetary resources that are related to the availability of other resources. The disposition variable is still found by persons related to the attitude of the executor who makes the obstacle an opportunity to do negative things, and in the variable structure of the bureaucracy, opportunities are still found to optimize the security of the international shipping channel in the Sunda Strait.

1. Introduction

Indonesia as an archipelagic country that has a vast sea area has the advantage of having extraordinary natural resources, as well as a large potential threat, the potential threat in the Indonesian sea is one of Indonesia's five biggest threats at this time, as stated by Marshal TNI Hadi when carry out feasibility tests as TNI Commander. The consequence of having a vast sea area, the state must be able to protect the region from factual threats and potential ones, Marshal TNI Hadi said that "Vulnerability in the sea as an archipelagic country, Indonesia is responsible for safety and security in the sea area which is the jurisdiction the free sea which borders the region [1].

The Indonesian Sea Area not only has an important meaning for Indonesia, it also has a very important meaning for the international world, because the Indonesian sea area is located in a cross position of the world which is often passed by sea transportation of other countries. One of the consequences of world recognition for Indonesia as an archipelagic country, Indonesia must create and establish several international lanes that pass through Indonesia's national jurisdiction to be used by various countries to cross the Indonesian sea.

In 1996, the Indonesian Government proposed to the International Maritime Organization (IMO) regarding the establishment of the Indonesian Archipelago Sea Flow (ALKI) and its branches in Indonesian waters. In accordance with Article 1 paragraph 8 of Law No. 6/1996 concerning Indonesian Waters, Islands Sea Flow is a sea channel that is passed by foreign ships or aircraft above the channel, to carry out shipping and flights in a normal way solely for continuous transit, directly, and as quickly as possible and not hindered through or above the archipelagic waters and adjacent territorial seas between one part of the Indonesian high seas or EEZ and in the other part of the high seas or the Indonesian Exclusive Economic Zone [2]

Each ALKI has a potential threat that is considered relevant and requires more serious coordination. Based on the author's interview with the speakers from the Sea Security Coordination Agency (Bakorkamla), each ALKI has different potential threats. The potential threat in ALKI I is related to the impact of conflict over territorial claims over the Spratly and Paracel Islands in the South China Sea, such as the use of the ALKI I region for the activities of the state army involved in maneuvering. In addition, the impact of traffic congestion in the Malacca Strait, such as the use of ALKI I areas by pirates to avoid the pursuit of Indonesian security forces and joint security forces (Indonesia, Malaysia and Singapore) or smuggling. The impact of the centers of growth and economy of Asia and Southeast Asia in the People's Republic of China (PRC) and Singapore, such as the smuggling of illegal goods and also human trafficking, is also a potential threat in ALKI I, including the effects of the danger of natural disasters and tsunamis in the Sunda Strait , such as the threat of volcanic earthquakes / volcanic eruptions (Anak Krakatau) and the impact of Malaysia's expansionary politics, such as the possibility of claiming new territorial territories.

The factual threat that occurred in July 2017 shocked the Sunda Strait region, namely the arrest of smuggling of shabu-shabu 1 (one) ton in Banten waters [3]. This shows that the existence of access to the waters of the Indonesian sea area is still very vulnerable and has the potential for warfare asymmetric threats, if only the methamphetamine is not caught can kill five million according to the Head of National Narcotics Agency Budi Waseso [4]. After the incident, successively captured again smuggling by sea in the amount of Ton.

In this study, the place of research taken was in the Sunda Strait. One of the strongest reasons for taking place in the Sunda Strait is the position that is very close to the State Capital so that it has a very high escalation of potential threats, if the potential threat of defense that might occur in the Sunda Strait is not anticipated. The policy on national defense has been made by the Indonesian Ministry of Defense to protect all nations, but it is considered important to always be vigilant by incessantly conducting research on how the implementation of this defense policy is carried out especially in locations that have the highest potential level.

2. Problem Formulation

Based on the background above, the formulation of the problem in this study is how is the Defense Policy Implementation in the face of the threat of asymmetric warefare especially in the dimensions of sea defense in the Sunda Strait, to secure international shipping lanes?

3. Method and Theory

The method used in this study is descriptive qualitative, phenomenology. The informants involved were all stake holders related to law enforcement in the Sunda Strait region. The theory used to answer the research problem formulation according to George Edward III, Edward proposed four factors that play an important role in achieving successful implementation or failure of policy implementation, namely communication, resources, disposition, and bureucratic structure factors [5].

4. Analysis and Discussion

The Sunda Strait is part of the Indonesian Archipelago Sea Channel (ALKI) I, which connects the waters of the Indian Ocean through the Karimata Strait to the South China Sea or vice versa. ALKI is a consequence of Indonesia as an archipelagic country after the Indonesian government ratified the UNCLOS 1982 International Sea Law through Republic of Indonesia Law Number 17 of 1985 [6,7}. Indonesia has designated three ALKIs as crossing lines of foreign ships in shipping from an open sea (ZEE) to other free seas. covers the air path above it. The Sunda Strait is a route commonly used for international shipping. In these waters there are also crossing lines from Java Island (Merak port) to Sumatra Island (Bakauheni port), operated by the Transportation Ministry of Lake and Crossing Transportation (ASDP).

Asymmetric warfare is a war that has a pattern that is different from the pattern of warfare that we generally know. Asymmetric warfare is carried out not militarily; mobilize troops; use defense equipment or invade a country. Asymmetric warfare is carried out non-military (without military force), even the range of war areas is wider than military warfare, and can be carried out without declaring war or deploying troops. Aspects that can be reached are not just military or political. More broadly Asymmetric War has the power to influence all aspects of life. The principle used in Asymmetric War is to use the minimum resources to get maximum results.

The implementation of Defense Policy in dealing with potential asymmetric warefare threats especially in the dimensions of sea defense in the Sunda Strait is as follows:

4.1 Communication

Communication in policy implementation includes several important dimensions, namely information transformation (transmission), information clarity (clarity) and information consistency (consistency). Submission of information regarding the contents of the policy to the implementor is very important, so that the policy can be implemented properly and the main tasks can be carried out.

Transmission of communication / delivery regarding national defense in the face of the potential threat of asymmetric warefare especially in the dimensions of sea defense in the Sunda Strait. Based on the research data from the interview to the resource person regarding the field of transmission / communication transmission, that: the national defense policy has been understood and has been implemented and described in the programs, informed and constraints and differences in perceptions can be resolved properly, and delivered by utilizing activities formal or through official announcements.

Clarity of communication regarding national defense in the face of the potential threat of asymmetric warefare especially in the dimensions of sea defense in the Sunda Strait.

Implementation in the Sunda Strait of the Banten Province. Based on the research data from the interview to the informants in the field of policy content, that: the contents of the national defense policy can be understood and described in programs and actions in accordance with the fields of duties and responsibilities of each maritime implementor, implemented in sea patrol activities.

Consistency regarding national defense in the face of potential asymmetric warfare threats especially in the dimensions of sea defense in the Sunda Strait. Based on the research data from the interview to the resource person regarding the consistency factor of communication, that: there is consistency from each implementor in the implementation of their duties and functions that are carried out continuously in the form of programs and evaluated according to the rules and work programs of each implementor.

4.2 Resources

Staff / executive staff resources from the parties involved in the implementation of national defense in the face of the potential threat of asymmetric warefare especially in the dimensions of sea defense in the Sunda Strait. Based on research data from interviews to resource persons on the factors of staff / personnel implementing resources, that: there is a limited number of personnel in carrying out their main tasks and responsibilities compared to the broad scope of supervision, however the implementation of the main tasks and responsibilities can still be implemented. Use of personnel in the implementation of duties and functions so that they are able to always carry out improvement in the quality of human resources through education and training.

Budget support in the implementation of the goals, objectives and contents of policies regarding national defense in the face of potential asymmetric warfare threats especially in the dimensions of sea defense in the Sunda Strait. Based on the research data from the interview to the resource person on the budget support factor, that: there is budget support but the budget support is insufficient and the amount is minimal, its use is optimal in carrying out the main tasks and responsibilities according to the task fields of each implementor. If there is a development of a strategic environment in accordance with the dynamics in the field, the use of the budget is adjusted to the scale of priorities.

Information on port governance in the implementation of the goals, objectives and contents of policies regarding national defense in the face of potential asymmetric warfare threats especially in the dimensions of sea defense in the Sunda Strait. Based on the research data from the interview to the resource person on the information resource factor regarding port governance, that: at present there is clarity of information and port governance. However, there are private ports that have not been included in the supervision of government port authorities, this will create vulnerability in terms of supervision, so that it can allow crime in the asymmetric field of warfare to occur there.

The executive authority of the parties involved in implementing the goals, objectives and contents of the policy regarding national defense in the face of warfare asymmetric potential especially in the dimensions of sea defense in the Sunda Strait. Based on the research data from the interview to the informant on the resource authority's executor, that: there is already the authority of the main duties and responsibilities of each implementor in the maritime field and carried out in accordance with the laws and functions of each, however, there is a need for socialization and education to parties outside of each agency. The implementation of the implementation is carried out in a mutually assisting and supportive manner in preventing crime.

Physical facilities or infrastructure and facilities in implementing the objectives, objectives and contents of policies regarding national defense in the face of potential asymmetric warfare threats especially in the dimensions of sea defense in the Sunda Strait. Based on the research data from the interview to the resource persons on the field of physical facilities / infrastructure and facilities, that there are sufficient facilities and infrastructure to carry out support in the sea defense but still need additions according to the ideal needs. In the case of the Navy and lack of facilities and infrastructure, the Indonesian Navy coordinated with the implementor related to their use, so that the implementation of their respective duties and functions could be carried out properly.

Support of Defense and Security Equipment in implementing the goals, objectives and contents of policies regarding national defense in the face of potential asymmetric warfare threats especially in the dimensions of sea defense in the Sunda Strait. Based on research data from interviews with resource persons (Defense and Security Equipment Tools), that: there are limitations (Defense and Security Equipment Tools) and if there are inadequate, both in the number and ability to carry out supervision in their respective working areas. In the case of the Indonesian Navy's limitations (Defense and Security Equipment), it will coordinate with the maritime implementer with involvement (Under Operation Control) of ships from other maritime agencies and coordinate with the unit regarding support (Defense and Security Equipment Tools) for marine security operations.

4.3 Disposition

Disposition or attitude of the parties involved in implementing the implementation of national defense in the face of potential asymmetric warfare threats, especially in the dimensions of sea defense in the Sunda Strait. Based on the data from the interview research on the resource persons in the field of implementing attitudes, that: there is / the attitude of the maritime sector implementor strongly supports the implementation of the maritime defense sector and is described in the main tasks and responsibilities of each maritime implementor.

Implementation in the field is carried out by coordinating with each other.

Commitment from the parties involved in implementing the implementation of national defense in the face of potential asymmetric warfare threats, especially in the dimensions of the sea defense in the Sunda Strait. Based on data from interviews with informants on the attitude factor of the implementers related to commitment, that: there is / there is a high commitment of maritime implementors to carry out tasks in the face of the threat of asymmetry warfare, which is manifested in written regulations and verbal instructions, so that implementation the main tasks and responsibilities can be carried out properly.

4.4 Bureaucratic Structure

The organizational structure in charge of implementing the policy has a significant influence on policy implementation. The aspect of organizational structure is Standard Operating Procedure (SOP) and fragmentation. Organizational structures that are too long will tend to weaken supervision and lead to complex and complex bureaucratic procedures.

Standard Operational Procedure (SOP) on the implementation of the implementation of national defense in the face of potential asymmetric warfare threats, especially in the dimensions of sea defense in the Sunda Strait. Based on data from research interviews to SOP resource persons in carrying out the task of facing asymmetric warfare, that: there are SOPs for each maritime sector stakeholder in accordance with their respective areas of main duties and responsibilities, but still need shared perception so that implementation can be carried out well. The implementation of existing SOPs has been carried out as part of the standard in carrying out tasks, so that members in the field can know what their main tasks are and what they do.

Fragmentation (division of roles) of organizational structures implementing implementation of national defense in the face of potential asymmetric warfare threats especially in the dimensions of sea defense in the Sunda Strait. From the interview data to the resource person regarding the fragmentation factor (division of roles) of the organizational structure, that there are already roles for each maritime field implementor in accordance with their respective duties and functions outlined in the implementation instructions and supervision, the division of roles for tasks internal and external tasks carried out in stages.

Synergy or relationship between one work unit and various other work units in the implementation of the objectives, objectives and contents of the policy on the implementation of national defense in the face of potential asymmetric warfare threats especially in the dimensions of sea defense in the Sunda Strait. From the interview data to the resource person regarding the synergy factor, that there has been a synergy in the implementation of the main tasks and responsibilities of each of the implementers in the maritime field, although it is still running separately, this can be proven in the absence of information exchange. Others seek information on their own. Combined official forums are needed that can bring together the implementers to exchange information that can be used for the benefit of tackling asymmetric warfare in the Sunda Strait in accordance with the potential of their respective task fields and functions.

5. Conclusions

Conclusion of Defense Policy Implementation in the face of potential asymmetric warfare threats especially in the dimensions of sea defense in the Sunda Strait to secure international shipping lanes.

5.1 Communications

Information transformation (transmission), has been conveyed to the implementer and has provided understanding. The implementation of the acceptance of this policy has been translated into programs and informed to the implementer through formal activities and official announcements. Clarity of information (clarity), has been clearly understood, this can be seen by the elaboration into programs and actions in accordance with the tasks and responsibilities of each maritime field houlder stake. The implementation of the clarity of the acceptance of defense policy is implemented in the activities of security patrols at sea. Information consistency (consistency), the consistency of the implementation of defense policies that have been carried out continuously in the form of programs and evaluated in accordance with the fields of duties and responsibilities of each maritime sector stakeholder. The implementation of duties and functions is carried out in accordance with the regulations in each implementer and carried out continuously and continuously, if it changes according to the dynamics in the field, it will seek approval from the head office.

5.2 Resources

Staff or implementers, have not run effectively because there are limitations in the number of personnel in carrying out their main duties and responsibilities when compared to the extent of the coverage area that must be implemented, however the implementation of the main tasks and responsibilities can still be implemented. In order to improve the ability of personnel to be able to carry out their duties and functions, quality improvement is carried out through education and training. By having trained personnel, the tasks given will be completed according to the duties and functions of each implementor.

Budget support, does not work effectively because there is budget support, but the budget support is insufficient, its use is optimal in carrying out the main tasks and responsibilities according to the respective task fields of stakeholders with a scale of priorities, thus defense policy in the sea in the Sunda Strait will not work effectively in achieving goals and objectives.

Information on port governance is not effective because there is information about domestic port data that has not been integrated in the port governance information system. This condition will make the implementation of the policy ineffective because the government port authority cannot carry out supervision, so that it can enable the occurrence of crime in the asymmetric warfare field in the sea of the Sunda Strait region.

Authority, has been effective. The implementation of the implementation is outlined in the regulations. Implementation of these regulations is carried out by means of socialization and education to the implementor and to parties outside of each agency. The implementation of the duties and functions of each implementor is carried out based on the rules of each implementor, in the event of problems in the implementation, then each implementor will coordinate and help each other so that the crime does not occur.

Facilities or Infrastructure facilities, not yet effective, because there are still a lack of facilities and infrastructure, for additions it becomes a problem itself with limited budget support. In the case of one implementor does not have the facilities and infrastructure so that coordination between implementors is carried out by carrying out loans, so that the duties and functions of the implementor can be carried out properly.

Alpalhankam support, there is a shortage of defense and security and if there is inadequate both the number and ability to carry out supervision in their respective working areas. In the case if Indonesia Navy lacking Alpalhankam, it will coordinate with maritime implementers by involving BKO ships from other maritime agencies as well as coordinating with the top unit regarding al-Khalam support for Sea Security operations.

5.3 Disposition

The attitude, the attitude of the implementers of the policy has been effective, because the implementor strongly supports defense policies in the Sunda Strait sea, this is a good attitude for the implementor. For the success of the implementation, the implementation is carried out by copying the coordination in accordance with the respective task areas and functions.

Commitment, there is a high commitment from the implementor in carrying out their respective duties and functions. The implementation of this commitment is in the form of written regulations and verbal instructions, so that the implementation of the main tasks and responsibilities can be carried out properly.

5.4 Organizational Structure

SOP, that there is already an SOP for each implementor as a guide for all members in carrying out their duties and functions in the field. The implementation of this SOP is to achieve the implementation of defense policy so that its implementation can be carried out properly.

Organizational structure, that the organizational structure of each implementor is flexible in carrying out their duties and functions. The implementation of this activity is that it can be implemented to adjust the SOP in accordance with the development of the dynamics in the field, the SOP conformers are requested to approve the head office.

The synergy between one work unit and various other work units, is that there is no optimal synergy, because the implementation of defense policy is still running on its own, so that there is no information sharing implemented, the acquisition of information is obtained individually. Given the importance of information in the implementation of the duties and functions of defense policy, a joint forum is needed which is used as a meeting place for implementors in terms of exchanging information to carry out tasks on each implementor.

References

[1] Hadi Djahjanto, http://nasional.republika.co.id/berita/nasional/politik/17/12/06/p0j2kq409-ini-5-potensi-ancaman-bagi-indonesia-menurut-marsekal-hadi, Accesed on April 2019.

[2] Law of The Republic of Indonesia Number: 6 of 1996 Consernring of Indonesian's waters

[3] Yandi Deslatama, 2017, https://www.liputan6.com/news/read/3021300/sabu-1-ton-diselundupkan-ke-banten-via-jalur-laut. Accesed on April 2019.

[4] Budi Waseso, (2018), https://regional.kompas.com/read/2018/02/12/13344321/temuan-1-ton-sabu-selamatkan-5-juta-jiwa-panglima-tni-beri-apresiasi. Accesed on April 2019.

[5] Edwards III, George C. 1980. Implementing Public Policy. Washington, D.C: Congressional Quarterly Press.

[6] The United Nations Convention on the Law of the Sea (UNCLOS) of 1982

[7] Law of The Republic Of Indonesia Number 17 Of 1985 Consernring Of Restriction Of United Nations Convention On The Law Of The Sea (Convention Of The Nation Of The Nations On Law Of Law)

Ecological Sustainability Strategy the Source of Bioterrorism from Slaughterhouse in Indonesia

Maya Dewi Dyah Maharani

The University of Sahid Jakarta, Department of Environmental Engineering, Jl. Prof. Dr. Supomo, SH No. 84 Tebet, South Jakarta 12870

E-mail: mayasudarsono@gmail

Abstract. The chance, probability, and rationality of terrorists in the use of biological weapons is worth considering in the preparation of the Terrorist handling strategy in Indonesia. This is because the methods of obtaining biological pathogens are easy to learn by anyone in recent decades. In fact, to get the biological material is also easily obtained in the slaughterhouse. This study aims to formulate the ecologycal sustainability directive strategy of management Bioterrorism in Indonesia. The methods used are Multidimensional Scaling (MDS) and Analytical Hierarchy Process (AHP). MDS method to calculate the index of sustainability and generate leverage attributes. As leverage attribute is the recruitment of slaughterhouse workers with Root Mean. Square is 6.10. Furthermore, the leverage attribute is included in the main criteria in AHP analysis to get an alternative priority strategy. The resulting directive strategy is the control of the Ante and Post Mortem Animal health strictly by involving the police with score 0.1980

1. Introduction

Throughout 2019, the Special Detachment Team (Densus) 88 Antiterror Polri has arrested 68 suspected terrorism actors of the congregation Ansharut Daulah (JAD). Four unexpected terrorists were arrested in January, 1 suspect arrested in February, while 20 suspects were arrested in March, 14 unexpected terrorists were arrested during April 2019. In May 2019 was arrested 29 unexpected terrorists, this number became the highest number for POLRI in capturing terrorist network members.

The threat of bioterrorism in the world has risen over the last few years, given the history of asymmetric war. This is a threat posed by highly challenging biological weapons, given that the unique characteristics of this agent are coupled with the lack of community knowledge in terms of first health care. As the history of Biowarfare has shown that, exposure to the number of minutes of biological agents can be fatal (Madad, 2014). The threat of future terrorism seems increasingly complex because they do not only commit terror attacks in conventional ways, but the recent developments of the opportunities, potential, and threats of terrorism are already able to do Attacks using chemical, biological and other materials known as bioterrorism (Mahendra Pal, 2017). Bioterrorism has received a lot of attention in the first decade of this century. Biological agents are considered attractive weapons for bioterrorism as these are easy to obtain, comparatively inexpensive to produce and exhibit widespread fear and panic than the actual potential of physical damage.

2. Methods

This paper is conducted by the method of desk study and direct observation in Slaughterhouse of Bogor, Malang, Semarang, Surabaya, Yogyakarta, Kudus and Bekasi. This study took place in the year 2017-2018.

The data collection process, both primary and secondary data, is conducted for 23 months, i.e. from February year 2017 to December year 2018. The data types that are collected include primary data and secondary data. Primary data is data obtained directly in the field, in the form of interviews from Manager of Slaughterhouse and related agencies. Secondary data is data obtained from reading sources or documents related to the management of Slaughterhouse. The data analysis method is tailored to research objectives. These methods include Multidimensional Scaling (MDS), Montecarlo, leverage analysis with the use of the Rap-Terrorism and Analytical Hierarchy Process (AHP) analysis.

2.1. Analisis Multidimensional Scalling (MDS)

Multidimensional Scalling (MDS) analysis is one of the doble-variable techniques that can be used to determine the position of a different object based on its resemblance, as well as to know interdependent relationships or mutual dependence Between variables or data. This relationship is not known through the reduction or grouping of variables, but rather by comparing the variables in each object in question using the perceptual map. MDS is also a technique that can help researchers to identify key dimensions and leverage attributes (Maya Dewi Dyah Maharani, 2017). MDS relates to the creation of maps to illustrate the position of an object with other objects based on the similarities of the objects. The MDS method helps identify double dimension scaling known as a perceptual map, which is a method that is to describe or map a perceived relative impression of a number of objects related to perception.

In MDS the attribute/factor/component or size to be measured can be mapped within the distance of Euclidian where the perceived object has the same characteristics as the closest Euclidian distance. Conversely, objects with different characteristics are called dissimilarities so that the difference between them can be measured within the perceived perception distance in the perception index such as the Sustainability Index. Distance determination techniques are based on Euclidian Distance with the following formula:

$$d_{1,2} = \sqrt{(X_1 - X_2)^2 + (Y_1 - Y_2)^2 + (Z_1 - Z_2)^2 + \ldots} \qquad (1)$$

Description:

$d_{1,2}$ = euclidian distance
X, Y, Z = Attribute
$_{1,2}$ = Observation

The distance Euclidian between these two points (D1, 2) then inside the MDS is projected into the two-dimensional Euclidian distance (Ḋ1, 2) based on the regression formula in the following equation:

$$D_{1,2} = \alpha + b\,D_{1,2} + c \qquad (2)$$

Description:

α = intercept
b = slope
c = error

In MDS, two points or similar objects are mapped in one point adjacent to each other. The technique used is the ALSCAL algorithm and is easily available on almost every statistical software (SPSS and SAS) (Sofia Papazoglou, 2017). Rap-Bioterrorism in principle makes iterations of the regression process so that the value of the smallest e is obtained and attempts to force the intercept on the equation equal to 0 (α = 0). Iteration stops if the stress is < 0.25 (Patrick Mair, 2016). For the attribute as much as M then stress can be formulated in the equation as follows:

$$stress = \sqrt{\frac{1}{m}\sum_{k=1}^{m}\left(\frac{\sum_i \sum_j \left(D_{ijk}^2 - d_{ijk}^2\right)^2}{\sum_i \sum_j d_{ijk}^2}\right)} \qquad (3)$$

Through the rotation method, the position of the sustainability point can be visualized through the horizontal and vertical axes with the value of sustainability indexes rated 0 percent (bad) and 100 percent (good).The Output of the Rap-Bioterrorism analysis is a sustainability index of 0-100 displayed in the ordination and leveraging indicators. Sustainability indices are grouped in 4 categories, namely: 0-25 (bad or unsustainable); 25,01-50 (less sustainable); 50,01-75 (fairly sustainable); 75,01-100 (good or very sustainable) (Kholil, 2015).

2.1.1. A Leverage analysis. Leverage analysis is performed to determine the effect of stability if one of the attributes/factor/components is omitted during ordination. The results of the Influence analysis (Leverage) shows the attributes that have the highest Root Mean Square are the most sensitive to sustainability attributes (Ryke Nandini, 2015).

2.1.2. Montecarlo Analysis. To evaluate the effect of errors on the estimation of ordination values used Montecarlo analysis, namely statistical simulation method to evaluate the effect of random error on the estimation process, as well as to evaluate the actual value (Lili Dahliani, 2018)

2.2. Analytical Hierarchy Process (AHP)

Analytical Hierarchy Process (AHP) is one of the data analysis methods for the process of choosing an alternative strategy which in this case is an alternative of directive strategy Bioterrorism in Slaughterhouse Industrial management. AHP was developed by Dr. Thomas L. Saaty of the Wharton School of Business in the year 1970 to organizer information and expert opinion (judgment) in choosing the most liked alternative (Basar, 2018). By using AHP an issue will be resolved in an organized thinking framework, so it can be expressed to make effective decisions on the matter. Complex issues can be simplified and expedited the decision-making process.

.

3. Result

The Rap-Terrorism analysis shows that the ecology sustainability status value is 53.1090 % that is categorized as a fairly sustainable value. The condition showed that the directive strategy of management bioterrorism is important. The results were validated with a 52.7440 % Monte Carlo value indicating a very small difference of distinction of 0.3650 or less than 1%. These values indicate that the effect of an error, or the impact of a relatively small scoring error. While the stress value of 0.2130 % and coefficient of determination (R2) has a high enough value of 95 % which means that the included attributes have a considerable role in explaining the diversity of the directive strategy bioterrorism from slaughterhouse

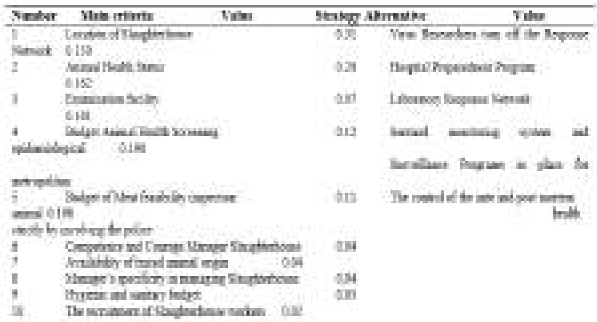
Based on the MDS analysis and leverage analysis showed that the attribute/factor/component that has the highest Root Mean Square (RMS) value is the use of the recruitment of slaughterhouse workers (6.10), it indicates that the attribute/factor/component the use of the type and amount of energy effectively and efficiently is a key factor that needs to be leveraged (Table 1)

Table 1. Attributes of leverage produced by Rap-Bioterrorism (MDS)

No	Attributes	Root Mean Square
1	Location of Slaughterhouse	4.65
2	Animal Health Status	5.08
3	Examination facility	4.85
4	Budget Animal Health Screening	4.29
5	Budget of Meat feasibility inspection	3.87
6	Competence and Courage Manager Slaughterhouse	3.61
7	Availability of traced animal origin	3.74
8	Manager's specificity in managing Slaughterhouse	4.16
9	Hygienic and sanitary budget	4.78
10	The recruitment of Slaughterhouse Workers	6.10

The ten attributes of leverage are then carried out by assessment of influence levels between attributes, either directly or indirectly. It is done considering there is a relationship between each attribute in the directive strategy of management bioterrorism. Results of AHP analysis obtained as in Table 2.

Table 2. Main criteria and alternative strategy of processed expert choice based on combined three expert using the average aggregation



Number	Main criteria	Value	Strategy Alternative	Value
1	Location of Slaughterhouse	0.35	Virus Researchers turn off the Response Network	0.130
2	Animal Health Status	0.28	Hospital Preparedness Program	0.162
3	Examination facility	0.17	Laboratory Response Network	0.161
4	Budget Animal Health Screening	0.12	Sentinel monitoring system and epidemiological Surveillance Programs in place for [illegible]	0.190
5	Budget of Meat feasibility inspection	0.11	The control of the ante and post mortem animal health strictly by involving the police	0.198
6	Competence and Courage Manager Slaughterhouse	0.04		
7	Availability of trusted animal origin	0.04		
8	Manager's specificity in managing Slaughterhouse	0.04		
9	Hygiene and sanitary budget	0.03		
10	The recruitment of Slaughterhouse workers	0.02		

Based on the results of this study obtained data that alternative strategy is the right priority is **the control of the Ante and Post Mortem Animal health strictly by involving the police** with the highest value (0.198). Spores bacillus Anthrax can still be found at Slaughterhouse when the Ante and Post Mortem tests on animals to be cut are not optimal. Bacillus anthracis is the etiologic agent of anthrax, and this is supposed to be one of the most potent Bioterrorism Weapons agents because its spores are extremely resistant to natural conditions and can survive for several decades in the environment (Goel, 2015). Bacillus anthracis spores enter the body through skin lesion (cutaneous anthrax), lungs (pulmonary anthrax), or gastrointestinal route (gastrointestinal anthrax) and germinate, giving rise to the vegetative form. Anthrax is a concern of public health also in many countries where agriculture is the main source of income including India. Anthrax has been associated with human history for a very long time and regained its popularity after Sept 2001 incidence in the United States.

The second alternative strategy is Sentinel monitoring system and epidemiological **(0.190).** Bioterrorism Information System has been widely used as a control and evaluation of bioterrorism attacks in various countries. Appling such system, based on the various characters that lead to eduction of epidemiological effects and reduction of its etiologic factors in the community. The effects of such a system depend on its features that aims to investigate the features of Bioterrorism Information System (Moghaddasi H, 2018)

The third alternative strategy is the Hospital Preparedness Program (0.162) ineffective action plans to counter bioweapon attacks and improve nursing care for victims of bioweapon according to international standards (Bamrasnaradura Infectious Disease Institute, 2019). Biological weapons are subject to a specific and comprehensive prohibition under international law that based of the Biological and Toxin Weapons Convention (BWC) year 1972 and bans the development, possession, and transfer of biological weapons. The Protocol for the Prohibition of the Use of Asphyxiating, Poisonous or Other Gases, and of Bacteriological Methods of Warfare of 1925 (the Geneva Protocol, or the Gas protocol), explicitly prohibits the use of bacteriological (biological) weapons (James Revill, 2018).

The fourth alternative strategy is Laboratory Response Network (LRN) (0.161). Cooperation among all network stakeholders helps ensure that laboratory response is an integrated part of the national response. The added laboratory testing capacity provided by the US Centers for Disease Control and Prevention LRN assets helps protect persons who reside in South Korea, US military personnel and civilians in South Korea, and those who reside in the continental United States (J. Todd Parker, 2017).

The last alternative strategy is Virus Researchers turn off the Response Network (0.130). Regular review of the management of bioterrorism is essential for maintaining readiness for these sporadically occurring events. Specific guidelines and recommendations for laboratory safety and risk assessment in the clinical microbiology are explored so that virus researchers turn off the response network can better prepare for the next biological disaster (Wagar, 2015).

4. Conclusions

The result of the ecological sustainability directive strategy of management Bioterrorism in Indonesia is the control of the Ante and Post Mortem Animal health strictly by involving the police with a score of 0.1980. In order for the directive strategy to be sustainable then components the recruitment of slaughterhouse workers deserve to be included in the Agricultural and Police Affairs

Acknowledgements

The Author thanked Prof. June Mellawati visiting, as a Senior Nuclear Environmental Chemist in BATAN for his discussion, correction, and advice on the manuscript.

References

[1] Madad, S. S. 2014 Bioterrorism: An Emerging Global Health Threat 5 Journal of Bioterrorism and Biodefence

[2] Mahendra Pal, M. T. 2017 An Overview on Biological Weapons and Bioterrorism American Journal of Biomedical Research 5 pp 24-34

[3] Maya Dewi Dyah Maharani, S.S. 2017 Manajemen Strategy for Sustainable Ruminant-Cattle Slaughterhouse Journal Veteriner 18 pp 94-106

[4] Sofia Papazoglou, K. M. 2017 An Examination of Alternative Multidimensional Scaling Techniques Journal Psychol Meas 77 pp 429-448

[5] Patrick Mair, I. B. 2016 Goodness –of-Fit Assessment in Multidimensional Scaling and Unfolding MultivariateBehavioral Research 51 pp 772-789

[6] Kholil, T. A. 2015 Multidimensional Scaling Approach to Evaluate Sustainability of Cirata Reservoir-West Java Province J. Manusia Dan Lingkungan 22 pp 22-31

[7] Ryke Nandini, A. K. 2017 Multidimensional Scaling Approach to Evaluatev Sustainability the Level of Community Forestry Sustainability in Babak Watershed, Lombok Island, West Nusa Tenggara, Indonesia Indonesian Journal of Spatial and Regional Analysis

[8] Lili Dahliani, M. D. 2018 Palm Oil Sustainability Management Using MDS Model from Social Dimension 5th International Conference on Community Development (amca 2018) 231 Atlantis Press

[9] Basar, P. 2018 The Analytic Hierarchy Process Method To Design Strategic Decision Making For The Effective Assessment Of Supplier Selection in Construction Industry 6 Research Journal of Business and management pp 142-149

[10] Bamrasnaradura Infectious Dieses Institute 2019 Anti-bioterrorism strategies of nursing services Journal of Health Science Research 13

[11] James Revill, B. H. 2018 Strengthening the Bioweapons Convention Oxford Research Group

[12] Goel, A. K. 2015 Anthrax: A disease of biowarfare and public health importance World Journal of Clinical Cases 3 pp 20-33

[13] J. Todd Parker, A.-C.J.-e 2017 Enhancing Laboratory Response Network Capacity in South Korea Emerging Infectious Disease 23

[14] Moghaddasi H, S. A. 2018 Features of Bioterrorism Information System Journal of Bioterrorism and Defence 9

[15] Wagar, E. 2015 Bioterrorism and Role of the Clinical Microbiology Laboratory Journal of Clin Microbiol Rev 29 pp 175-189

Defense Strategy

Defense Management

National Security

Defense Technology

Index Measurement of National Energy Security Based on Fuzzy Analytical Hierarchy Process

Yanif Dwi Kuntjoro, Anggun Andreyani, Asih Tri Marini, Khusnul Khotimah

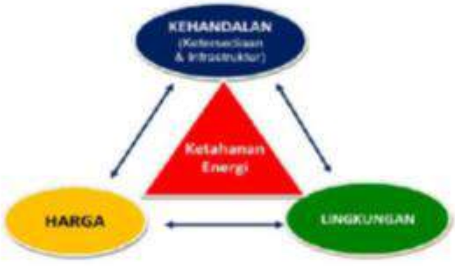
Fakultas Manajemen Pertahanan, Prodi Ketahanan Energi, Sentul Indonesia
yanif_dk@yahoo.com, asihtrimarini@gmail.com, khusnul486@gmail.com

Abstract. There is no method that has been used in the assessment of the national energy security index using Fuzzy Analytic Hierarchy Process (FAHP). Fuzzy Analytic Hierarchy Process is an Analytic Hierarchy Process (AHP) method, was developed with fuzzy logic theory, specifically triangular fuzzy. Steps to analyse data with the Fuzzy AHP method is almost the same as the AHP method. While AHP has only been a method that supports decisions that developed to solve problems by ranking of problem solutions, grouping, and the arranging it into a hierarchical structure. The AHP method also takes into account the validity of the data with the inconsistency limit. However, considerable uncertainty and doubt in giving an assessment will have an impact on the accuracy of the data and the results obtained. Based on this, further theory was developed as an alternative measurement indicator, namely the Fuzzy Analytic Hierarchy Process method. The results of the energy security index assessment using the Fuzzy Analytic Hierarchy Process method are one alternative choice for considering the categorized national energy security index assessment on the assessment of energy security levels in 5 scales, namely very strong, strong, sufficient, vulnerable, very vulnerable. The results obtained indicate that the national energy security index value is 7.357 based on the range issued by DEN, the current national energy security index category in Indonesia is GOOD.

1. Introduction

Indonesia's current energy security conditions are at a level that is quite vulnerable. Based on data from the World Energy Council (WEC) in 2015, Indonesia was in the position of 17 countries with low energy security (WEC, 2015). To overcome this, the Government of Indonesia is committed to increasing the primary energy mix of 25% petroleum, 22% natural gas, 30% coal and 23% EBT in 2025 in realizing the Sustainable Development Goal (SDG) for national energy independence and security (BPPT, 2016).

The energy mix target is the target of the provision and utilization of primary energy as the direction of national energy management documented in official documents on national energy security conditions from the national energy security index assessment. The direction of national energy management to realize national energy security is compiled in the National Energy Policy (KEN) through Government Regulation Number 79 of 2014, where energy management is based on the principles of justice, sustainability and environmental insight in order to create national energy independence and security. The National Energy Council (DEN) in the National Energy Policy (KEN) defines energy security (figure 1.1) as a condition of ensuring the availability of energy, people's access to energy at affordable prices in the long term while paying attention to environmental protection.



Source : DEN, 2015

Figure 1.1 Energy Security Concept

The assessment of energy security has been carried out by BPPT and the National Energy Council (DEN) using the AHP (Analytical Hierarchy Process) method, each of which has a different g rating of the national energy security index. This difference is due to the dynamics of indicators that refer to aspects of dimensions that are used as assessments in measuring the national energy security index. BPPT has an assessment of the rating with a cumulative value for all elements of 10 so that the cumulative value of components per element is 100 (Boedoyo, 2012). Whereas DEN has a rating for all elements is one so that the cumulative value of components per element is 10 (DEN, 2015).

The dimensions used in measuring energy security refer to the dynamic 4A + 1S concept, adjusting to national conditions or capabilities to build national energy security. The availability dimension includes the availability of energy sources, such as fossil fuels, alternative energy and renewable energy originating from domestic and non-domestic, accessibility namely the ability to access energy sources, energy network infrastructure including geographic and geopolitical challenges to energy, affordability including affordability of prices and costs energy from the stage of exploration, production and distribution to consumers, acceptability, namely acceptance of energy and sustainability includes the use of sustainable and environmentally friendly energy sources.

The method that has been used through the Analytic Hierarchy Process (AHP) is a decision support method developed to solve the problem by breaking the problem solution, grouping and then arranging it into a hierarchical structure. To obtain priority criteria, this method uses a comparison of criteria paired with a predetermined measurement scale. The main input of the AHP method is the perception of experts or experts, so that it has a factor of subjectivity in decision making. This method also takes into account the validity of the data with the inconsistency limit (Saaty & Kearns). However, considerable uncertainty and doubt in giving an assessment will have an impact on the accuracy of the data and the results obtained. Based on this, further theory was developed as an alternative measurement indicator, namely the Fuzzy Analytic Hierarchy Process method.
Fuzzy Analytic Hierarchy Process (figure 1.2) is an Analytic Hierarchy Process (AHP) method developed with fuzzy logic theory, specifically triangular fuzzy. The problem solving step with the Fuzzy AHP method is almost the same as the AHP method. It's just that the Fuzzy AHP method converts the AHP scale into a triangular fuzzy scale to get priority, where the changed data is processed further with extent analysis.

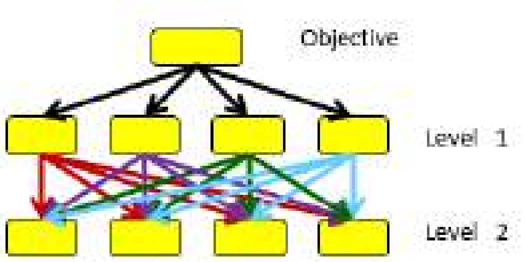


Figure 1.2 Energy Security Assesment with FAHP Method

Therefore, energy security (part of the tri gatra) is often described as the foundation of national resilience so it is necessary to measure the national energy security index using the Fuzzy Hierarchy Process method, covering the dimensions of 4A + 1S (Availability, Accessability, Affordability, Acceptability and Sustainability) so that increasing Indonesia's national resilience which includes aspects of five gatra (ideology, politics, economy, socio-culture, defense and security) and tri gatra (region, population (demography) and natural resources (including energy).

1.2. Formulation of the problem

National energy security and independence index is a variable that can measure the level of energy security. Assessment of the level of energy security is divided into 5 scales, namely very strong, strong, sufficient, vulnerable, very vulnerable, which will be measured by the Fuzzy Hierarchy Process method, so the research problem formulation is how the results of national energy security index results are measured using the Fuzzy Analytical Hierarchy Process (FAHP) can be used as input to the government as material for consideration in an alternative measurement of the national energy security index.

1.3. The aims of Paper.

The aims of this research is to analyze the measurement results of the national energy security index using the Fuzzy Analytical Hierarchy Process (FAHP) method for input to the government as a material for consideration in the alternative measurement of the national energy security index.

1.4. Benefits of Writing This Paper

The preparation of this journal is expected to provide information about the measurement of the national energy security index that has been carried out by BPPT and DEN. However, the problem is that almost all the results of the national energy security index measurement are still carried out through the Analytical Hierarchy Process (AHP) method which does not include indicator variables which are still unclear so that they have not been targeted in the General Energy National Draft (RUEN). This research is important to do considering that the assessment of the national energy security index must be included in the National Energy General Plan so that an alternative to measuring other methods besides AHP, namely FAHP, is important to do.

2. Literature Review

2.1. Theoretical basis.

2.1.1 Analytical Hierarchy Process (AHP) Method

AHP analysis is one method for choosing one or more among the many alternative decisions proposed. Basically AHP is a model of comprehensive decision making by combining quantitative and qualitative concepts. AHP allows interaction between a system and the environment then unites them by measuring and regulating the effects of components of system errors (Saaty, 2001). According to Burgeois (2005) AHP techniques are generally used with the aim of arranging the priorities of various alternatives / choices that exist and those choices are complex or multi criteria. Using the priority AHP produced will be consistent with the theory, logical, transparent and participatory. AHP is considered very suitable to be used to prioritize public policies that demand transparency and participation.

AHP techniques have been used extensively in the decision making process for example OPEC uses AHP to choose strategies in an effort to realize organizational goals (Brodjonegoro, 1992). Bayazit and Karpak (2005) also use AHP in supplier selection for the modern market. The working principle of AHP is by simplifying complex problems, having no structure, requiring strategies and changing or unstable into structured parts and forming a level or herarchy. Determination of the level is done using numerical data that is formulated subjectively using considerations, namely the priority level of other variables. From these various considerations, an analysis is then carried out to determine the variables that have high priority and have a role that influences the results of the system being studied. (Marimin, 2004). According to Saaty (1991) the use of the AHP method in the decision making process has three (3) work principles, inter alia:

a. Compilation of hierarchies

Compilation of hierarchies defines or simplifies complex problems into clear and detailed problems, then compiled based on the views of those who have competencies in related fields.

b. Priority determination

Priority determination is based on the opinions of experts and married parties concerned through discussions and through questionnaires. Priorities of the elements in the hierarchy can be viewed as the weight / contribution of these elements to the goals to be achieved in decision making.

c. Logic consistency

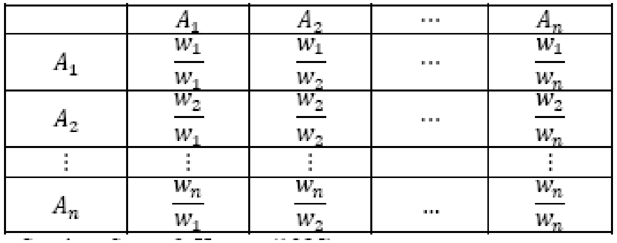
This principle determines the suitability between conceptual and operational data and the consistency of the answers of the respondents. It can be seen the assessment of elements and comparing them in pairs.

2.1.2 Fuzzy Analytical Hierarchy Process Method (FAHP)

Fuzzy AHP is an analytical method developed from traditional AHP. Although AHP is commonly used in handling qualitative and quantitative criteria in MCDM, fuzzy AHP is considered better in describing decisions that are vague than traditional AHP.

The basic principles of FAHP are decomposition, comparison of judgments, and priority synthesis. Decomposition is a step to break down or divide a problem into a hierarchical structure. The structure consists of three levels, namely the first level (goal), the second level (criteria) and the third level (alternative). Furthermore, the comparison of assessments is done by comparing criteria in pairs and measured by a comparison scale from 1 to 9. The weight of the assessment obtained is then arranged into a paired comparison matrix and a synthesis process is carried out to obtain the value of each criterion. The value of each criterion is obtained by calculating the priority vector (eigenvector) from the pairwise comparison matrix. Suppose there are as many as n criteria (A1, A2, A3, ... An) with wi / wj (i = 1,2, ... n and j = 1,2, ... n) is the weight of paired comparisons, then a paired comparison matrix can be arranged as Table 2.1.

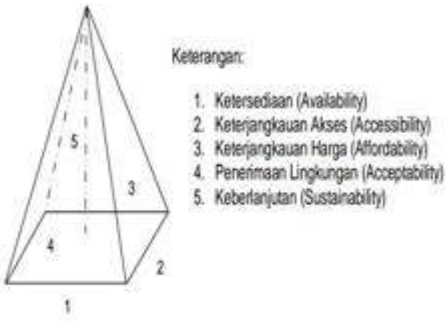
Tabel 2.1 Pairing Comparison Matrix



	A_1	A_2	$\cdots$	A_n
A_1	$\frac{w_1}{w_1}$	$\frac{w_1}{w_2}$	$\cdots$	$\frac{w_1}{w_n}$
A_2	$\frac{w_2}{w_1}$	$\frac{w_2}{w_2}$	$\cdots$	$\frac{w_2}{w_n}$
$\vdots$	$\vdots$	$\vdots$		$\vdots$
A_n	$\frac{w_n}{w_1}$	$\frac{w_n}{w_2}$	$\cdots$	$\frac{w_n}{w_n}$

Source: Saaty & Kearns (1985)

2.1.3 Energy Security


Keterangan:
1. Ketersediaan (Availability)
2. Keterjangkauan Akses (Accessibility)
3. Keterjangkauan Harga (Affordability)
4. Penerimaan Lingkungan (Acceptability)
5. Keberlanjutan (Sustainability)
1
2
3
4
5

Source : DEN, 2015

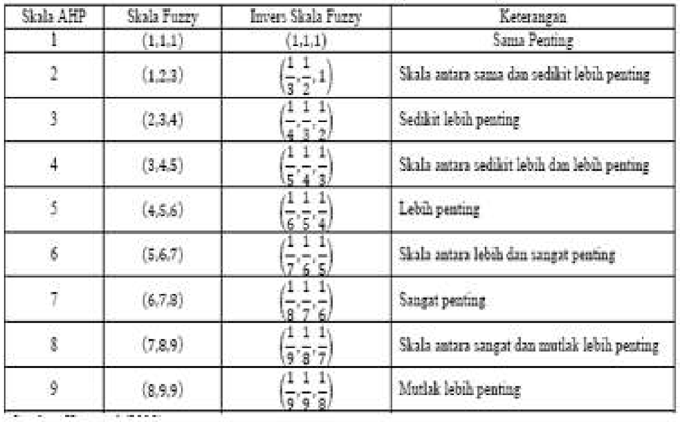
Figure 2.1 Concept of the Dimension of National Energy Security

One of the definitions of energy security is one where conditions are guaranteed for energy availability and people's access to energy at affordable prices and the quality received through a healthy and sustainable energy mix. There is no definite definition of the concept of energy security, in the concept of energy security there are 4 energy security indicators consisting of how physical availability (availability), accessibility, how affordability, and how / the quality of the product so that acceptable to society (acceptability). Of the four indicators also must meet the requirements of sustainability (sustainability) in order to say that energy security has been achieved (Nugroho, 2014).

3. Research Methods

The method used in this study is a literature study method with the application of Fuzzy AHP to the measurement of the national energy security index, to find out sectors that contribute dominantly to national energy security. Energy grouping is based on the 4A + 1S concept that is adapted to national conditions or capabilities to build energy security through indicators of energy availability (accessibility), access to energy (accessibility), affordability, acceptability, and energy sources sustainability. FAHP measurement scale with triangular fuzzy number (table 3.1)

Table 3.1 AHP Scale and Triangular Fuzzy Number



Skala AHP	Skala Fuzzy	Invers Skala Fuzzy	Keterangan
1	(1,1,1)	(1,1,1)	Sama Penting
2	(1,2,3)	$\left(\frac{1}{3},\frac{1}{2},1\right)$	Skala antara sama dan sedikit lebih penting
3	(2,3,4)	$\left(\frac{1}{4},\frac{1}{3},\frac{1}{2}\right)$	Sedikit lebih penting
4	(3,4,5)	$\left(\frac{1}{5},\frac{1}{4},\frac{1}{3}\right)$	Skala antara sedikit lebih dan lebih penting
5	(4,5,6)	$\left(\frac{1}{6},\frac{1}{5},\frac{1}{4}\right)$	Lebih penting
6	(5,6,7)	$\left(\frac{1}{7},\frac{1}{6},\frac{1}{5}\right)$	Skala antara lebih dan sangat penting
7	(6,7,8)	$\left(\frac{1}{8},\frac{1}{7},\frac{1}{6}\right)$	Sangat penting
8	(7,8,9)	$\left(\frac{1}{9},\frac{1}{8},\frac{1}{7}\right)$	Skala antara sangat dan mutlak lebih penting
9	(8,9,9)	$\left(\frac{1}{9},\frac{1}{9},\frac{1}{8}\right)$	Mutlak lebih penting

4. Analysis and Discussion

4.1 Identification of IKEN factors and indicators

Research on measuring the national energy security index has been carried out by BPPT and the National Energy Council. In determining the energy security index identification of criteria and sub criteria that affect the energy security index. In the research BPPT and DEN have measured energy security index by considering the aspects of Availability, Acceptability, Affordability and Accessability where the four aspects are indicators of energy security currently in use. Then use the derivative indicators of each aspect to measure the index of each indicator. In this study the aspects of resilience indicators that are used not only include Availability, Acceptability, Affordability and Accessability but also Sustainability aspects considering the concept of energy security that is relevant to current conditions must consider sustainability. Then the sub criteria used are from the social side where the big goal of achieving energy security is National Resilience. So that sub-criteria from energy security indicators are ideology, politics, economics, social and culture, and defense and security.

Based on the five sub-criteria including Ideology, Politics, Economics, Social and Culture, and Defense and Security, each sub-criterion was analyzed to determine the value of current energy security conditions in terms of the relevance of sub-criteria to aspects of Energy Security. Then an assessment is carried out to obtain an energy security index. The valuation method is done by comparing ideal conditions with current conditions with a range of valuations between 0-10. Where the value of 10 is a perfect condition and is the goal of energy security for all countries in the world. Based on the results of the measurement of the energy security index carried out by DEN, the Indonesian energy security index in 2015 was 7.518 and it was categorized as a good index. This value is obtained based on the derived aspects of the aspect of energy security. The criteria and sub criteria used in this study are as follows:

Criteria:

1. *Availability*
2. *Acceptability*
3. *Affordability*
4. *Accessability*
5. *Sustainability*

Sub Kriteria Panca Gatra

1. Ideology
2. Politics
3. Economics
4. Social and Culture
5. Defense and Security

Referring to the value of the energy security index that has been studied by the DEN the category of energy security conditions is divided into 4 categories including:

Table 4.1 Range of IKEN Values

Condition	*Range* Value of IKEN
Very Good	8 s/d 10
Good	7 s/d <8
Moderate	6 s/d <7
Low	<6

In this study, testing was carried out if using the five gatra aspects, so that the Indonesia energy security index value can be known if it is judged based on the correlation of energy security aspects to Panca Gatra using the Fuzzy Analytical Hierarchy Process (R-FAHP) Engineering method. The concept of the method used to determine the condition of the energy security index is shown in Figure 4.1 below:

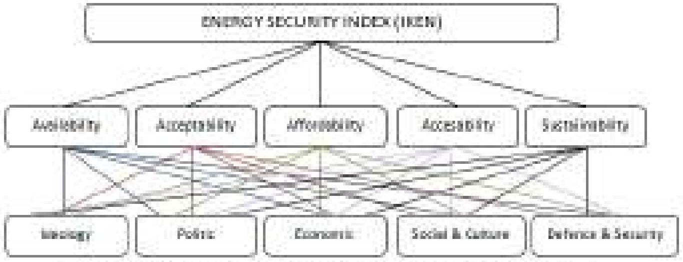


Figure 4.1 Determining the Conditions of the Energy Security Index

4.2 Modeling the energy security index measurement with FAHP

In this study the measurement of the energy security index using the FAHP method was carried out to determine the current condition of Indonesia's energy security whether 1) Very Good; 2) Good; 3) Moderate; or 4) Low in terms of every aspect of energy security parameters. The steps taken in this study are as follows:

A. Determine the scale of pairwise comparisons

The comparison scale is a method used to determine the importance of each criterion in the AHP method. The comparison matrix is based on the instructions in the following table:

Table 4.2 Pair Comparison Scale

Interest Intensity	DEFINISI DEFINITION	EXPLANATION
1	Both elements are equally important.	The two elements make up the same level.
3	One element is slightly more important than the other.	Experience and consideration a little support for one element over the other.
5	One element that is essential or very important than the other elements	Strong experience and consideration of one element over the other.
7	One element is clearly more important than the other elements.	One element strongly supported and dominant has been seen.
9	One absolute element is more important than the other elements.	Evidence that supports one element over another has the highest degree of affirmation.
2,4,6,8	Middle values between two contiguous considerations.	If a compromise is needed .
Reverse	If for activity i get one number when compared to an activity j, then j has the opposite value when compared to activity i	

The energy security index value obtained is 7.35. Based on these results Indonesia's energy security conditions fall into the category of "GOOD" according to the energy security index range made by the National Energy Council. These results can be seen from the results of the following scheme:

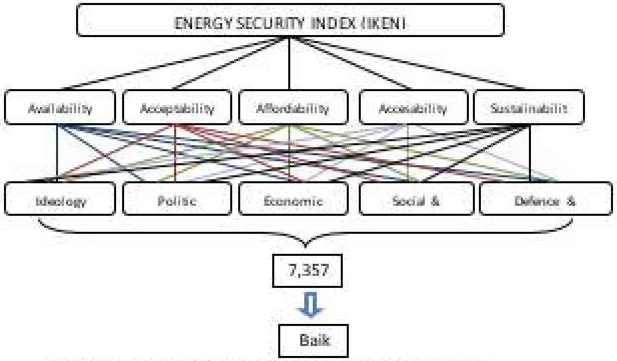


Figure 4.2 Condition of the Energy Security Index

5. Conclusionsuand Suggestions

5.1 Conclusions

The conclusions from the results of this study are as follows that the results of the measurement of the National Energy Resilience Index (IKEN) using the Fuzzy Analytical Hierarchy Process (FAHP) method produce an energy resistance index value of 7.35 which belongs to the category "GOOD."

5.2 Suggestions

For suggestions from the results of this study can be used as input to the government as material for consideration in the alternative measurement of the national energy security index. Going forward, it is hoped that it can be used as a reference for research on measuring energy security indexes associated with derivative indices from the aspects of energy security and the conditions of IPOLEKSOSBUDHANKAM.

Reference

1. Boedoyo, M. Sidik. 2011. Analisis Ketahanan Energi Nasional. Jakarta: BPPT DEN. 2015. Ketahanan Energi Nasional 2015. Jakarta: Sekjen DEN
2. Brodjonegoro, B. P. (1992). AHP: Analitical Hierarchy Pocess. Jakarta: Pusat Antar Universitas-Studi Ekonomi, Universitas Indonesia.
3. Jumina dan Wijaya, j. d. (2012). KETAHANAN ENERGI DAN KEBIJAKAN BBM DI INDONESIA. Yogyakarta: Pusat Studi Energi Universtas Gadjah Mada.
4. Marimin. (2004). Teknik dan Aplikasi Pengambilan Keputusan Kriteria Majemuk. Jakarta: Grasindo.
5. Nugroho, H. (2014). Ketahanan Energi Indonesia Gambaran Permasalahan dan Strategi edisi 2. Bappenas.
6. Saaty, T.L. 1991. Pengambilan Keputusan Bagi Para Pemimpin. Setiono L. Penerjemah. Jakarta: Institut Pendidikan dan Pembinaan Manajemen
7. (IPPM). Terjemah dari: Decision Making for leaders The Analytical Hierarchy Process for Decision in Complex World.

Flare Gas Management in The National Energy Security Perspective

Syaiful Hidayat [1], Suyono Thamrin [2]
[1]Energy Security Graduated Program, Indonesia Defense University (UNHAN),
Indonesia Peace and Security Center (IPSC), Bogor 16810, Indonesia
Email: bukanbangipul@gmail.com

[2]Energy Security Lecture, Indonesia Defense University (UNHAN), Indonesia
Peace and Security Center (IPSC), Bogor 16810, Indonesia
Email: suyono.thamrin@gmail.com

Abstract. Gas flaring is a gas produced by the oil and gas exploration and production or processing of oil or natural gas is burned as it cannot be handled by the production or processing facilities provided so untapped. This gas comes from upstream and downstream of the business. The data from Ministry of Energy and Mineral Resources in 2014 indicated that, the gas was burned through flaring amounted to approximately 131.15 Million Square Cubic Feet per Day (MMSCFD) or equivalent with the potential electricity production for 655.75 Megawatt (MW), this number was bigger than the utilized associated gas by 75.45 MMSCFD. The Minister Regulation No. 31 of 2012 regulated the procedures of flaring gas in the oil and gas production field. However, this regulation only a few mentions of the utilization. This paper conducted with indicators assessment of energy security, which are availability that indicates the availability of associated gas reserves, affordability of the flare gas selling price, accessibility of infrastructure provision, and acceptability of the environment and economy acceptance. The results of this research are expected to provide recommendations to the government to create a policy that specifically regulates the utilization of flared gas based on priority of the problem.

1. Introduction

The history of the use of energy sources in the industry is very simple. First, humans use wood, then move to coal which is considered more practical. Over time, petroleum was discovered which was considered more practical, even though getting fuel oil had to go through quite complicated processing. Technological advances in the petroleum sector, especially the petrochemical industry, have created downstream industries with various by-products that provide high economic value. This is one of the causes of the rapid growth of the petroleum industry. The discovery of natural gas lately has given a new color in the procurement of energy sources. Unlike petroleum which requires long processing before use, gas is more practical and cheaper. Indonesia has considerable natural gas reserves, namely 102.9 Trillion Cubic Feed (TCF) or 1.5% of world gas reserves (BP Statistical Energy Review: 2018).

The efforts to use gas are part of the diversification of fossil energy, especially petroleum. With the phenomenon of energy scarcity in various parts of the world, energy security is the hottest issue in the context of the national interest of a nation in an effort to maintain its existence. The issue of energy security is the background of various political, economic, socio-cultural and defense security issues. Energy Security is a condition of ensuring the availability of energy and people's access to energy at affordable prices in the long term while paying attention to environmental protection (PP No. 79: 2014).

One of the highlights of the problems of the oil and gas industry is about flare gas and their use. Flare gas is gas produced by exploration and production or processing of oil or gas that is flared because it cannot be handled by production or processing facilities so that it has not been utilized (ESDM Minister Regulation No. 31 of 2012). Flare gas usually comes from upstream oil and gas business (upstream industry) and downstream business (downstream industry). Basically, the installation of flares is a safety system of gas produced from the processing and production by flaring the gas. Aside from being a safeguard, combustion of gas flares aims to minimize environmental pollution, because if the gas is discharged into the air without being burned first it certainly has a negative impact on the surrounding environment. The impact of gas combustion on the flare system turns out to be one of the causes of CO (carbon monoxide) emissions, Sox (sulfur oxide) and NOx (mono-nitrogen oxide) into the air which can cause global warming so it must be reduced.

2. The potential of Flare Gas

Based on Minister of Energy and Mineral Resources (ESDM) Regulation No.31 of 2012, the definition of flare gas is gas produced by exploration and production or processing of oil or gas that is flared because it cannot be handled by available production or processing facilities so that untapped. The amount of flare gas in Indonesia originating from the gas association from the oil production field is quite significant. Data from the Directorate General of Oil and Gas at the Ministry of Energy and Mineral Resources in 2014 showed that the gas burned through the flaring ranged around 131.15 Million Square Cubic Feet per Day (MMSCFD) or equivalent to the potential for electricity production of 655.75 Megawatts (MW), this amount is greater than the associated gas utilized at 75.45 MMSCFD. The flaring of this exhaust gas will not only cause environmental pollution, it also indirectly results in the waste of potential resources that are actually still very potential to be utilized. The amount of profits that can be achieved by utilizing this gas flaring. At present, the use of flare gas is still treated the same as conventional gas, namely by prioritizing supply for the electricity sector.

The management of oil and gas exploitation activities only focuses on oil and gas commodities as natural resources that have high economic value, whereas on the other hand the activities of oil exploitation also produce gas flaring. If it is not reused, the gas flares will re-enter the atmosphere to subsequently pollute the air. Flare gas production in Indonesia is ranked fourth among oil-producing countries members of the Global Gas Flaring Reduction (GGFR), which is a non-profit organization under the auspices of the World Bank which consists of oil-producing countries (OPEC) and state-owned oil companies and oil companies other multinational.

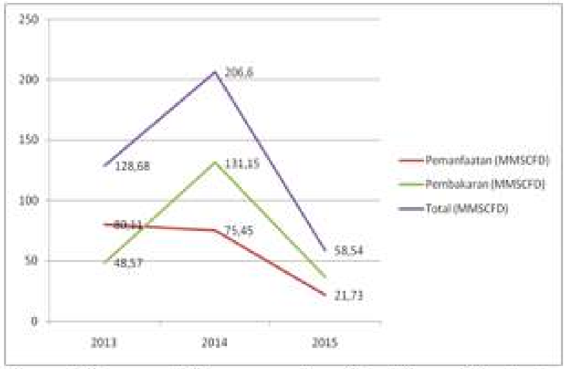


Figure 1. The amount of flare gas used and flared (sourse: Directorate General of Oil and Gas: 2015)

Flare gas usually comes from upstream oil and gas business (upstream industry) and downstream business (downstream industry). Basically, the installation of flares is a safety system of gas produced from the processing and production by burning the gas. Aside from being a safeguard, combustion of flare gas aims to minimize environmental pollution, because if the gas is discharged into the air without being burned first it certainly has a negative impact on the surrounding environment.

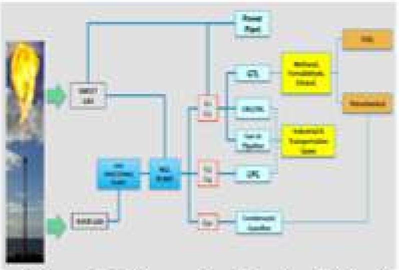


Figure 2. Schemes for Flare Gas Utilization

Through the processing of flaring gas into LPG, condensate and CNG, a positive economic, ecological and social impact will be obtained. Economically, the products produced are fuels that have high economic value, can increase the company's income. Gas flaring processing will also reduce the amount of flared gas, this will reduce the air pollution produced in the combustion process.

3. Regulation

Several rules have been made to regulate the governance of Gas Flaring, including:

Law No. 30 of 2007
In this law, utilization is included in energy management. The use of energy is an activity using energy both directly and indirectly, from energy sources. The efficiency of energy utilization is also included in energy conservation, which is a systematic, planned and integrated effort to preserve domestic energy resources and improve the efficiency of its utilization.

In the context of using gas flaring, this can be categorized as the utilization of new energy sources. And this matter is also regulated in this law, that energy utilization is carried out based on the principle:

1. optimizing all potential energy resources;
2. consider technological, social, economic, conservation and environmental aspects; and
3. prioritizing the fulfillment of community needs and increasing economic activities in energy-producing regions.

Law No. 22 of 2001
In this Oil and Gas Law it is stated that oil and gas are non-renewable strategic natural resources that are controlled by the state and are vital commodities that control the livelihoods of many people and have an important role in the national economy so that management must be able to optimally provide prosperity and welfare. This law regulates the role of oil and gas management, with arrangements including, among others, the power of mining, implementation and implementation of cooperation contracts.

Mastery by the state is held by the government as the holder of the mining authority. The government determines the terms and conditions of the cooperation contract, the working area of the cooperation contract, and the contractor that will carry out upstream business activities. Furthermore, the government as the holder of the mining authority formed the Executing Agency for Upstream Oil and Gas Business Activities (BP Migas) which has now changed to the Special Task Force for Implementing Oil and Gas (SKK Migas). Upstream business activities are carried out by a Business Entity or permanent establishment based on a Cooperation Contract with BP Migas.

Presidential Regulation No. 61 of 2011

Presidential Regulation No. 61 of 2011 concerning the National Action Plan for Reducing Greenhouse Gas Emissions (RAN-GRK) is a guideline for planning, implementing, monitoring and evaluating GHG emissions reductions. This regulation was made to fulfill the Indonesian government's commitment to reduce greenhouse gas emissions by 26% with its own business or reach 41% with international assistance in 2020.

Particularly for the energy sector, the programmed action plan is monitoring the implementation of policies for reducing flare gas combustion volumes. The program has a target for the availability of data on gas flare combustion volume per year as a result of monitoring the implementation of policies to reduce gas flare burning volumes throughout Indonesia. This task was given to the Ministry of Energy and Mineral Resources (ESDM) in the period 2010-2014.

Regulation of the Minister of Energy and Mineral Resources No. 31 of 2012

This regulation regulates the implementation of flaring of gas in oil and gas business activities. This regulation regulates technically the combustion of gas flaring by contractors or oil and gas business license holders. The contractor is allowed to burn gas flaring if the gas volume does not exceed the limit:

a. 3% (three percent) of feed gas (feed gas) for natural gas fields;
b. daily average in 6 (six) months of 5 (five) MMSCFD for petroleum fields;
c. 0.3% (zero point three percent) of natural gas for natural gas refineries;
d. 0.8% (zero point eight percent) of petroleum oil refinery intakes.

The contractor is obliged to calculate the volume provisions above based on the method of using the meter for gas flaring and calculating the estimation of the gas burned. Contractors who wish to conduct flaring must make an application for approval from the Directorate General of Oil and Gas of the Ministry of Energy and Mineral Resources. The application for approval contains a technical document consisting of:

a. the volume of Gas Flaring;
b. utilization of Gas Flaring that has been done;
c. technical aspects, safety, environment;
d. economic calculation of Gas Flaring; and
e. Gas Flaring (Flaring) volume reduction program

In essence, this regulation mandates that contractors or holders of processing business licenses must use gas flaring optimally.

4. Energy Security

In the concept of energy security, gas flaring governance will be seen through energy security indicators, namely, accessibility, affordability, acceptability, and sustainability.

The availability of flaring gas related to the availability of associated gas reserves will always determine the gas flaring gas itself. Its high uncertainty also influences the value of investment, so this availability side provides a description of the potential of gas flaring from the volume side.

On the other hand, the infrastructure provision factor has a very important role in the use of gas flaring. Gas flaring volume that reached 131.15 MMSCFD (Source: Directorate General of Oil and Gas, 2014) or equivalent to electricity production of 655.75 Megawatts does indeed promise as an alternative solution to the problem of electrification. However, this huge potential is spread across various parts of the country and most are in remote areas. This is certainly a problem for its utilization.

What can be done is by building processing and distribution infrastructure. Facilities Gas flaring processing infrastructure includes pipes, compressors, block stations, etc. However, this requires a very high cost. So far, the construction of infrastructure for processing gas flares is the contractor's obligation. This certainly becomes complicated, because from the contractor's point of view, the processing and utilization of gas flaring must generate income economically. Meanwhile, what happened was that contractors had to finance expensive processing facilities and had to sell gas flaring products amid a drop in world oil prices. If the government is committed to optimizing the use of gas flaring, one of the things that might be done is to find solutions to these infrastructure problems, such as sharing costs to finance processing facilities with contractors. In order to reduce the burden of contractors and improve the investment climate, especially for the use of gas flaring.

In 2017, the ESDM Minister Regulation Number 32 of 2017 was issued concerning Provisions and Procedures for Determining the Allocation and Utilization and Price of Natural Gas. One article with 6 (six) sub-articles in this regulation discusses gas flaring. But it is very unfortunate, by still including the same definition as Ministerial Regulation No. 31 of 2012 concerning gas flaring, as well as the pricing mechanism that is still B to B, experts consider that this candy is not "firm". Expectations that with the issuance of this regulation will increase efforts to use gas flaring to be responded to as usual by experts. The price mechanism that was submitted to SKK was then determined by the Directorate General of Oil and Gas to be considered too wordy and very bureaucratic. On the other hand, amid the high uncertainty the decision about the selling price of gas flares must be done as quickly as possible given the industrial dynamics and various technical constraints such as the possibility of reduced volume, pressure, etc. One possible solution is to form a special team for setting gas flaring prices. This team must consist of various elements such as the Directorate General of Oil and Gas, SKK Migas, DEN, and Lemigas who will take to the field directly to see the gas flaring specifications of each field to then collectively calculate the prices of contractors based on the economic provision of processing infrastructure. Then, the team will submit a price recommendation that is ratified by the Minister of Energy and Mineral Resources through the Directorate General of Oil and Gas. In short, in the gas flaring pricing policy the strategy must be top-down to avoid processes that are too bureaucratic and take a long time, because the dynamics of the oil and gas market requires quick and appropriate decision making.

In terms of acceptability, the intended environmental acceptance is from the natural and social side, while economic acceptance is when gas flares are accepted as a new commodity as something worth selling. In the previous chapter it was said that, daily energy use is often considered the biggest factor causing environmental pollution. Energy is the engine of economic growth that supports industrialization (Yusgiantoro, 2000). Increasing the industrialization process also encourages energy consumption. The relationship between energy and the environment was initially not considered an important issue. However, along with the increasing industrialization in developed and developing countries, environmental problems then received significant attention. This problem then developed into an issue about the sustainability of a country's development process. In further developments, environmental issues are increasingly global. At present it is well recognized that the cost of overcoming environmental damage is greater than the cost of prevention. In addition, the demands of the community are no longer limited to the quantity of commodities. The community has become increasingly aware of the quantity as well as the quality of the environment that is clean. Gas flaring containing carbon elements will damage nature when flaring is done. In several countries such as the United States, China, Germany and Russia, the processing and utilization of gas flaring is done on the basis of minimizing environmental damage. In Indonesia, the use of gas flaring is more likely to be carried out on the basis of commercialization and to develop the economy of the community in the vicinity of the mining site.

5. Conclusion

Flaring gas is the remaining oil and gas production that can still be utilized, both for own-use and monetization purposes. The application of gas flaring cannot be compared to conventional gas because of its different specifications. In terms of volume, gas flaring is very potential, but its existence is spread out and most of it is located in remote areas which is an obstacle in its utilization. Optimizing the use of gas flaring is very possible if the government together with contractors work together in providing processing infrastructure in the production field. And not less importantly, there must be a pricing policy team consisting of various elements of interest needed to accelerate the determination of gas flaring prices based on observations of their specifications in the field. When the management efforts of this flare gas have been carried out through the right way, the environmental damage will be reduced in the future.

Acknowledgements

This paper was made as a continuation of previous research that was made by the author as a final assignment to obtain a master's degree in defense science. The problem of gas flares has not yet found a solution in terms of its governance. The author considers it necessary to rewrite gas flares, with the hope that more academic studies that address these issues will contribute to the government in making appropriate policies.

References

[1] Dewan Energi Nasional (DEN). Ketahanan Energi Indonesia. (2014). Jakarta

[2] Dharmasaputra, Metta. (2014). Wajah Baru Industri Migas Indonesia. Jakarta. Katadata

[3] Handiko, Gunard. (2012). Pemanfaatan Gas Suar Bakar Untuk Industri Sekitar di Tiga Lokasi. Depok. Universitas Indonesia

[4] Juliadi, Teuku. (2013). Analisis Unjuk Kerja Kompresor Sentrifugal Pada Unit Flare Gas Recovery PT. Arun NGL. Banda Aceh. Universitas Syiah Kuala

[5] Kementerian Energi dan Sumber Daya Mineral (ESDM). (2015). Rencana Strategis Kementerian Energi dan Sumber Daya Mineral. Jakarta. http://www.esdm.go.id/

[6] Lubiantara, Benny. (2014). Dinamika Industri Migas. Jakarta. Petromindo.Com

[7] Nugroho, Hanan. (2004) Percepatan Infrastruktur untuk Mendongkrak Pemakaian Gas Bumi. IPB Press

[8] Rangkuti, Zulkifli. (2012). Model Ekonomi Pemanfaatan Gas Ikutan. Bogor. IPB Press

[9] Sitorus T. B. (2002). Tinjauan pengembangan bahan bakar gas sebagai bahan bakar alternatif. Fakultas Teknik, Jurusan Teknik Mesin: Univesitas Sumatera Utara. https://repository.usu.ac.id

[10] Tjandaranegara, Abdul Qoyum. (2012). Gas Bumi sebagai substitusi Bahan Bakar Minyak Optimalisasi Investasi Infrastruktur dan Analisis Dampaknya terhadap Perekonomian Nasional. Depok. Disertasi Fakultas Teknik Universitas Indonesia

[11] Yusgiantoro, Purnomo. (2000) Ekonomi Energi: Teori dan Praktek. Jakarta. Pustaka LP3ES

Study of Technology Readiness Level of Green Diesel in Indonesia

Khoirun Naimah[1], Andhika Rahman[1] and Nugroho Adi Sasongko[1,2]

[1]Energy Security Graduate Program, Indonesia Defense University (UNHAN), IPSC Area, Bogor, 16810, Indonesia

[2]Agency for The Assessment and Application of Technology (BPPT), M.H Thamrin Road No.8, Jakarta, 10340, Indonesia

E-mail: khoirun.naimah@mp.idu.ac.id, andhika.rahman@mp.idu.ac.id, nugroho.sasongko@idu.ac.id

Abstract. Biomass based green energy could be an alternative solution to a number of existing problem ranging from scarcity of petroleum resources, greenhouse gas emissions, to technical constraints in fuel field operation, especially biodiesel in non PSO sector. Technology used in green energy, varies according to the type its raw material. However, in general there are 2 types of technology namely standalone and co-processing. In some countries, the green refinery processing unit has become the main focus in providing environmentally friendly fuels. This study aims to provide a review of the various technology pathways than can be used in biodiesel conversion into green energy (green diesel) and find out technology readiness level of green diesel in Indonesia. Thus, it anticipated that green diesel is realised for not only PSO but also for non PSO sector. This research showed green diesel that obtained by co-processing technology from plant oil (in particular palm oil) with conventional diesel is more likely to accelerate commercialization of green diesel in Indonesia compared to standalone technology. Technology readiness level of green diesel has reached TRL 8, and that is potential to improve fuel availability and energy security in Indonesia.

1. INTRODUCTION

Fossil Fuel (BBM) is the final type of energy that most consumed compared to other fuel, namely 32%. In 2014 gasoline consumption was 45.5%, diesel 45.2%, avtur 6.3% and kerosene 1.5%. Of these compositions, 79.7% were consumed by the transportation sector (motorcycle, cars and aircraft) [1]. Diesel consumption is almost same as gasoline consumption, which means that diesel also plays an important role in fuel energy mix. The consumption of diesel is increasingly in time, it seen in fig.1.

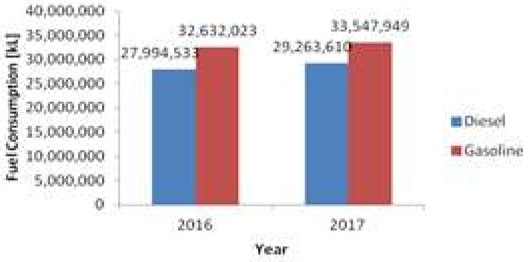


Fig.1 Fuel consumption [2]

From Figure 1. it can be seen that there is an increase in diesel consumption by 1.04%, which in 2016 Solar consumption is 27,994,533 KL and in 2017 it reached 29,263,610 KL. This means that fuel consumption will continue to increase from time to time. Fuel is the final energy produced from crude oil. Crude Oil is a type of fossil energy source that requires a very long time even million years to reform it. Thus, the increasing use of fuel will accelerate the depletion of fossil energy resources and its reserves. Currently, our domestic fuel production cannot meet domestic needs so we must import fuel to meet those needs. The high rate of fuel import makes Indonesia's trade balance undergo deficit which results in a weakening of the rupiah exchange rate and decreasing of Indonesia's competitiveness in the eyes of the world [3]. Therefore, government is currently making new efforts to reduce the volume of imports of fuel by substituting it to green diesel or green solar.

The huge potential of Indonesian crude palm oil (CPO) production up to 32 million tons/year can be fully utilized to produce Green Diesel [4]. Green Diesel itself is considered better than conventional fossil fuel because it can have RON 96 and a high cetane numbers reaching 60-70 [5]. The higher the octane value, the less fuel leaves dirt in the combustion chamber so that the engine lasts longer and the higher the value of cetane numbers shows the quality of combustion in the combustion chamber so that combustion is more perfect and more efficient. Green diesel also plays a role in reducing the volume of fuel imports and increasing renewable energy mix in transportation sector. Green diesel produces emissions up to 90% lower than fossil fuels [6]. Green diesel also has the same specifications as gasoline and meets the criteria for the Euro IV emission standard [7].

Currently the development of refineries for green diesel production has been carried out. There are two refineries being revitalized to become green refinery which can produce green diesel, the refinery is the Plaju Refinery in South Sumatra and the Dumai Refinery in Riau [7]. The selection of the two refineries was based on consideration of the proximity of the refinery location to the location of the green diesel raw material, namely oil palm. In its development, government collaborated with an oil and gas company from Italy, ENI, which experienced from 2016 in the context of technology transfer. Pertamina has sent experts to study directly from the ENI oil refinery in Italy so that they can fully understand the technology and can apply it at Indonesian oil refinery. Pertamina also collaborates with PTPN III for green diesel raw material, CPO. The government targets that by 2021 the two refineries will be able to produce green diesel [8].

Therefore, technology readiness level (TRL) conducted based on Permenristekdikti No. 42/2016 about the measurement and determination of TRL for determining readiness status of green diesel technology, evaluate the implementation of green diesel research and development programs, reducing the risk of failure in monitoring green diesel technology and increasing the utilization of the results of research and development of green diesel.

2. METHOD

The method used in this study is the measurement of technology readiness level (TRL) of green diesel in Indonesia based on Permenristekdikti No. 42 of 2016 which is then used to measure the level of manufacturing readiness level (MRL). TRL measurements are carried out using technometer, which is assessed based on self assessment by referring to existing references. However, basically the assessment was assessed by self assessment manually and online by the Research Coordinator (Assessment Team) and verified by the Verifier and the person in charge of measurement. The object of TRL measurement is research and development activities that has been be carried out using state budget funds, regional budgets and other government funds, such as LPDP, DIPI and also research and development activities carried out in government agencies with other funds.

3. RESULT AND DISCUSSION

The following is the result of the Green Diesel TRL assessment from CPO using a technometer that is assessed by self assessment can be seen in table 1.

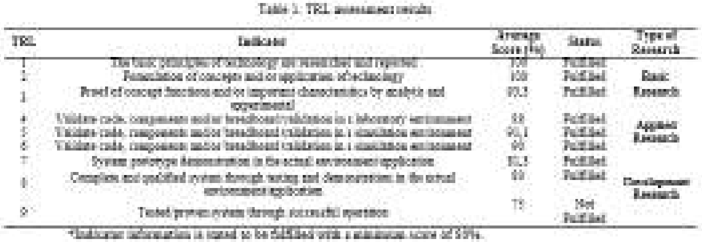


Table 1: TRL assessment results

TRL	Indicator	Average Score (%)	Status	Type of Research
1	The basic principles of technology are researched and reported	100	Fulfilled	Basic Research
2	Formulation of concepts and or applications of technology	100	Fulfilled	
3	Proof of concept function and/or important characteristics by analysis and experimental	93.3	Fulfilled	
4	Validate code, components and/or breadboard validation in a laboratory environment	88	Fulfilled	Applied Research
5	Validate code, components and/or breadboard validation in a simulation environment	93.1	Fulfilled	
6	Validate code, components and/or breadboard validation in a simulation environment	90	Fulfilled	
7	System prototype demonstration in the actual environment application	93.3	Fulfilled	Development Research
8	Complete and qualified system through testing and demonstration in the actual environment application	89	Fulfilled	
9	Tested proven system through successful operation	75	Not Fulfilled	

*Indicator information is stated to be fulfilled with a minimum score of 80%.

This assessment results in the form of a map of technological readiness level conditions in research and development institutions in Indonesia from upstream to downstream, a map of budget use for research and development, a map of the strength of research and development institutions in Indonesia. Besides that, with the knowledge that this manufacturing readiness level can make policies/programs towards a more directed down streaming, focus more on incentive programs and downstream certainty [9,10,11].

3.1 TRL 1-3 (Studies)

The TRL assessment at this stage consists of studies related to the production of green diesel, namely:

- Literature study of biomass conversion process into green diesel. The process of converting biomass to green diesel can be done by extraction, pyrolysis, and gasification [12].
- Literature study of selecting the type of raw material and the type of catalyst to be used.
- Literature Study of Green Diesel processing technology. The technology used can be either standalone or co-processing. Standalone is the process of processing green gasoline only from biomass. While co-processing is the cultivation process of green diesel with a mixture of biomass and diesel [22].

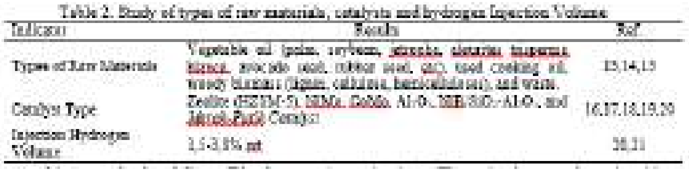


Table 2. Study of types of raw materials, catalysts and hydrogen Injection Volume

Indicator	Results	Ref
Types of Raw Materials	Vegetable oil (palm, soybean, jatropha, [illegible] [illegible] [illegible], avocado seed, rubber seed, etc), used cooking oil, woody biomass (lignin, cellulose, hemicellulose), and waste.	13,14,15
Catalyst Type	Zeolite (HZSM-5), NiMo, CoMo, Al_2O_3, NiB/SiO_2-Al_2O_3, and [illegible] Complex	16,17,18,19,20
Injection Hydrogen Volume	1,5-3,5% wt	20,21

Green diesel is a renewable fuel obtained by the mechanism of hydroprocessing (hydrotreater and/or hydrocracking) and/or decarboxylation and/or decarbonation of triglycerols or originating from different renewable resources such as vegetable oil [6,23,24]. Hydrodeoxygenation removes oxygen by reacting triglycerides and FFAs with hydrogen to form water and n-paraffin, decarboxylation or decarbonation removes oxygen to carbon dioxide or carbon monoxide and n-paraffin [18,25]. The following are the hydrodeoxygenation, decarbonylation, and decarboxylation reactions [22].

$$C_x\,COOH \xrightarrow{+H_2} nC_{x+1} + 2H_2O \qquad (1)$$

$$C_x\,COOH \xrightarrow{+H_2} nC_x + H_2O + CO \qquad (2)$$

$$C_x\,COOH \longrightarrow nC_x + CO_2 \qquad (3)$$

Green diesel is different from biodiesel. Biodiesel still has oxygen content, while green diesel does not contain oxygen [26]. The characteristic comparison between fossil diesel, biodiesel and green diesel can be seen in Table 3.

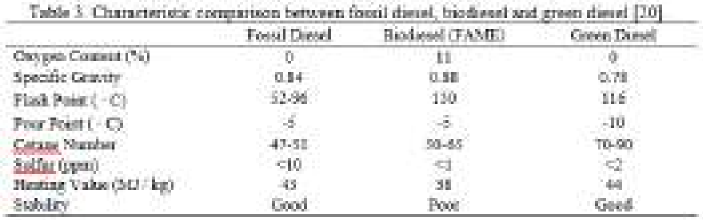


Table 3. Characteristic comparison between fossil diesel, biodiesel and green diesel [20]

	Fossil Diesel	Biodiesel (FAME)	Green Diesel
Oxygen Content (%)	0	11	0
Specific Gravity	0.84	0.88	0.78
Flash Point (°C)	52-96	130	116
Pour Point (°C)	-5	-5	-10
Cetane Number	47-52	50-65	70-90
Sulfur (ppm)	<10	<1	<2
Heating Value (MJ / kg)	43	38	44
Stability	Good	Poor	Good

Table 3 shows that green diesel has none oxygen content, has highest cetane number compared to fossil diesel and biodiesel which is 70-90, heating value 44 MJ/kg higher than others and good stability. The technology pathways of green diesel can be seen in figure 2.

Figure 2, illustrates that green diesel can be obtained from various types of raw materials and various types of processes. The type of raw material used in Indonesia to produce green diesel by PT. Pertamina is extracted from palm oil, then refining, bleaching and degumming are carried out. Degumming is the process of removing dissolved substances and suspended particles in CPO. Bleaching is the process of removing CPO pigments either dissolved or dispersed. Deodorizing is the process of removing unwanted odors in palm oil. The technology used is co-processing. The reason for using co-processing compared to standalone is because of low capital investment, only by minor modification in the existing plant unit can becomes a co-processing plant, high operation flexibility, dual feeds (fossil and vegetable) to anticipate uncertainty in the amount of supply and price of raw materials, require relatively faster time than conventional plant for engineering, procurement and construction (EPC) and are able to produce green diesel 96.5% wt.

The refine, bleached, and deodorized palm oil (RBDPO) is blended with fossil fuels (residual/gasoil) which then enter hydro treatment unit at temperatures of 310-340°C with help of hydrogen and catalyst [18,22]. Then catalytic cracking/hydrocracking process hold at temperature of 450°C for 1 hour with the help of catalyst injection PK 220 HBD or known as *merah-putih* catalyst and hydrogen injection 1.5-3.8% [20,22]. After that, the product is distilled to produce green diesel. While for the co-processing of RBDPO with untreated diesel the next process after hydro treatment is isomerization and distillation for producing green diesel. The product composition produced from the co-processing process consists of 96.5% green diesel as the main product, 1.2% by-products in the form of H2O and 2.3% off-gas [20]. Preliminary green diesel studies have been carried out by Pertamina RU II Dumai since 2007 and published in 2018. In 2018, Pertamina conducted a feasibility study about production of green diesel from CPO with an Italian oil company named ENI [27]. In 2-3 years from 2018, Pertamina is ready to realize green diesel production at the Pertamina refinery [8]. Production of palm oil in 2018 is 47.6 million tons, consists of 43.4 million tons CPO and 4.2 million tons palm kernel oil (PKO) produced from 14 million ha of palm farm [2]. Regarding the challenges of CPO supply, Pertamina cooperates with PTPN III and RNI [28].

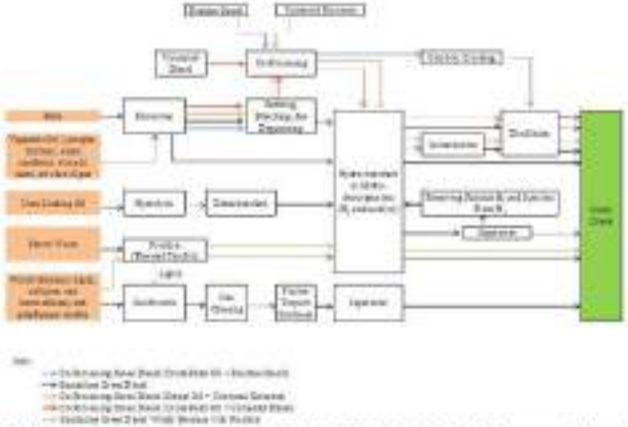


Fig. 2 Tech pathways of green diesel [5,12,13,14,15,20,21, 22,25,29,30,31,32] processed by author

3.2 4-6 TRL (Laboratory Validation and Prototype)

After studies and testing in laboratory and assessment of the 1-3 TRL stage fulfilled, the 4-6 TRL stage assessment continued with collaboration between Pertamina and ENI. This collaboration was carried out because Italy succeeded in producing a green diesel patent that was first conducted by ENI and Honeywell UOP Ecofining^{TM} in 2007. In collaboration with UOP America, ENI established the world's first co-processing unit in Venecia existing refineries that turn palm oil to green diesel known as Ecofining^{TM} in 2016. The technology can be seen in the following figure 3.

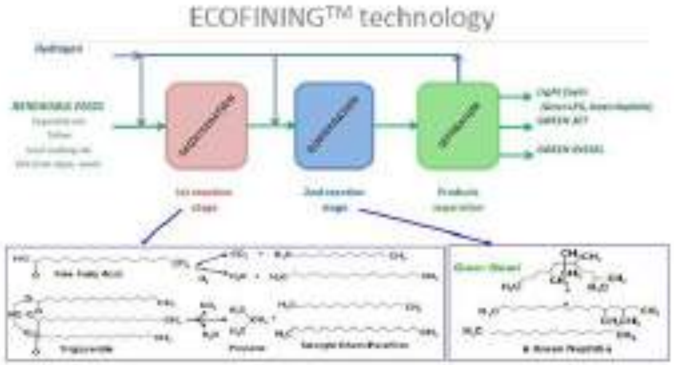


Fig. 3 Ecofining™ technology of green giesel [22].

From fig. 3 we understand that the process sequence for obtaining green diesel is divided into 3 steps, it begins with the deoxygenation process, which is the process of removing oxygen content contained in oil with help of hydrogen injection. After that, the oil produced by the deoxygenation process will be carried out by an isomerization process wherein the isomers are combined between C atoms and H atoms and other components. The last step is separation, where there is separation based on its specific mass, then green diesel are produced with atomic composition C_{15}-C_{18} about 94-98% and the rest are sulfur, ash, etc.

3.3 TRL 7-8 (Pilot Plant, Plant test and/or Demonstration)

In Indonesia, for a pilot plant scale, will be done [20]:

- Pilot Test Catalyst PK 220 HBD (Collaboration between RTC Pertamina and ITB).
- Consumption review of H_2
- Calculation of Yiled produced

Indonesia has successfully conducted a green diesel trial that has been carried out by Pertamina RU II Dumai on March 6, 2019. The green diesel trial at RU II Dumai was carried out with a ratio of petroleum to CPO of 87.5: 12.5, with the results of cetane number about 60-90 [2]. The challenge of implementing co-processing in green diesel is the consumption of hydrogen used is three times from conventional, identification of bottlenecks that occur during trial co-processing and modification of existing units for co-processing [20].

In 2025, we recommend that from total production of 52 million CPO, 9.6% for Biodiesel, 3.8% for PLTD, 25% for co-processing and standalone green fuel and 65% for food and exports. The concept was carried out as a step in dealing with supply uncertainty [2]. With condition the price of green diesel does not have to be pegged at 420 dollars/ton but depends on supply [20].

3.4 TRL 9 (Commercialization)

In Indonesia, it is planned that RU II Dumai produces green diesel 12.7 MBSD in DHDT units , RU IV Cilacap 13 MBSD in TDHT units , and RU VI Balongan 35 MBSD in GO HTU units is Refinery which is ready to commercialize green diesel made from CPO and PKO with DHDT Unit Coprocessing technology with RBDPO/Degum CPO 5 - 15% injection on feed existing tentative . Besides that, PK 220 HBD catalyst fabrication was also carried out in accordance with the proposal from ITB & RTC which had been tested through the Pilot Test [20] . The potential Co-Processing unit in Pertamina along with the amount of diesel predicted will be obtained can be seen in figure 4.

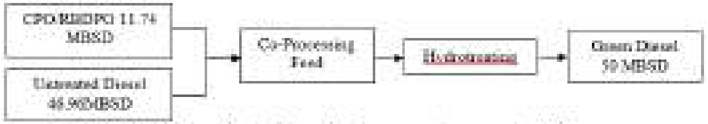
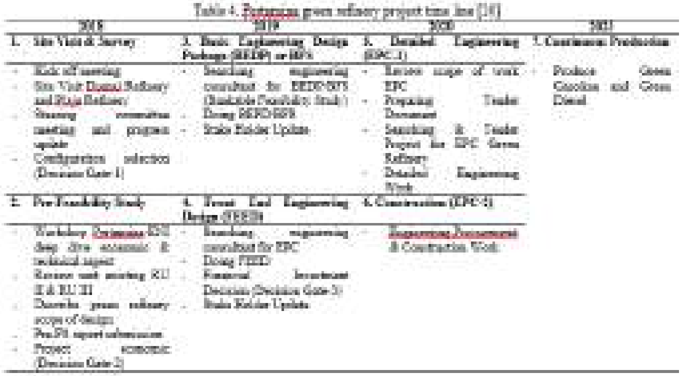


Fig. 4 Potential unit of green diesel co-processing pertamina [20]

From figure 4, it can be seen that the volume ratio between Untreated Diesel and CPO/RBDPO is 80:20 (46.96 MBSD: 11.74 MBSD) which is estimated to produce 50 MBSD of green diesel. The time line for the Green Diesel Co-Processing project in Indonesia by Pertamina can be seen in table 4.

Table 4. Pertamina green refinery project time line [18]



2018	2019	2020	2021
1. Site Visit & Survey	3. Basic Engineering Design Package (BEDP) or BPS	5. Detailed Engineering (EPC-1)	7. Continuous Production
- Kick off meeting - Site Visit Dumai Refinery and Plaju Refinery - Steering committee meeting and progress update - Configuration selection (Decision Gate 1)	- Searching engineering consultant for BEDP/BPS (Bankable Feasibility Study) - Doing BEDP/BPS - Stake Holder Update	- Review scope of work EPC - Preparing Tender Document - Searching & Tender Project for EPC Green Refinery - Detailed Engineering Work	- Produce Green Gasoline and Green Diesel
2. Pre-Feasibility Study	4. Front End Engineering Design (FEED)	6. Construction (EPC-2)	
- Workshop Pertamina-ENI deep dive economic & technical aspect - Review unit existing RU II & RU III - Describe green refinery scope of design - Pre-FS report submission - Project economic (Decision Gate 2)	- Searching engineering consultant for EPC - Doing FEED - Financial Investment Decision (Decision Gate 3) - Stake Holder Update	- Engineering Procurement & Construction Work	

From table 4, it can be seen that this year (2019) the project is in the stage of Front End Engineering Design (FEED) or just reach TRL 8 (Demonstration/Plant test), then in 2023 construction work will be completed and ready to start mass production of green diesel.

4. Conclusion

For Indonesia, green diesel has reached TRL 8 stage, which means that the product has gone through testing and demonstration stage in its actual application. TRL 8 assessment means that it has reached demonstration stage of maturing process of green diesel production. This is assessed from the success of Pertamina RU II Dumai demonstrating production of green diesel on March 6, 2019 in DHDT unit, with technology that enables accelerating the implementation of green diesel is co-processing palm oil with gasoil or residue (LCGO). We estimate that Indonesia will reach TRL 9 on 2022 or 2023 with the assumption that there are no significant obstacles. Greendiesel has the potentia l to help reduce co$_2$ emissions, alternative source of sustainable and high quality fuel and also able to support fuel availability in Indonesia which greatly helps to rise national energy security and reduce fossil fuel import.

Acknowledgements

This research is supported by Energy Security Program of Indonesia Defense University (UNHAN), data from the Green Fuel Implementation Plan of PT. Pertamina (Persero) and reports from study visits at PT. Pertamina (Persero) RU II Dumai.

Reference

[1] BPPT 2016 *Outlook Energi Indonesia* (Jakarta:Pusat Teknologi Sumber Daya Energi dan Industri Kimia (PTSEIK) BPPT)

[2] Priyanto, Unggul 2019 *Palm Oil untuk Green fuel*.(Jakarta:BPPT)

[3] Arvirianty, Anastasia 2018 *Impor Migas Naik, Defisit Neraca Perdagangan Membengkak Onlin.* (https://www.cnbcindonesia.com/news/20180711083534-4-22955/impor-migas-naik-defisit-neraca-perdagangan-membengkak , accessed on 25 April 2019)

[4] Nurmala, Novianti 2018 *Mengenal Potensi Limbah Kelapa Sawit Indonesia Online* https://kumparan.com/noviyanti-nurmala1519197736585/dari-limbah-menjadi-berkah-mengenal-potensi-limbah-kelapa-sawit-indonesia, accessed on 25 April 2019

[5] Piemonte, Vincenzo *Green Diesel Online* (http://www.oil-gasportal.com/green-diesel/?print=pdf.UCBM:Italy. Accessed on 2 April 2019)

[6] Simakova, I 2010 *Handbook of Catalytic Transformations of Fatty Acid Derivatives* (Turku:Abo Akademi)

[7] Tyas, Dini Arining 2018 *Oktober Diterapkan, Seperti apa Standar Emisi Euro 4 di Indonesia Online* (https://www.otosia.com/berita/oktober-diterapkan-seperti-apa-standar-emisi-euro-4-di-indonesia.html, accessed on 25 April 2019)

[8] Melanova, Denis Riantiza 2018 *Pemerintah dorong pertamina produksi green diesel mulai 2021 Online* (https://ekonomi.bisnis.com/read/20181116/44/860666/pemerintah-dorong-pertamina-produksi-green-diesel-mulai-2021, accessed on 25 April 2019)

[9] Direktorat Riset dan Pengabdian kepada Masyarakat. 2017 *Selayang Pandang Tingkat Kesiapterapan Teknologi (TKT) Online* . (https://www.google.com/search?q=Direktorat+Riset+dan+Pengabdian+kepada+Masyarakat.+(2017).+Selayang+Pandang+Tingkat+Kesiapterapan+Teknologi+(TKT)&oq=Direktorat+Riset+dan+Pengabdian+kepada+Masyarakat.+(2017).+Selayang+Pandang+Tingkat+Kesiapterapan+Teknologi+(TKT)&aqs=chrome..69i57j69i59.673j0j9&sourceid=chrome&ie=UTF-8#, accessed on 21 April 2019)

[10] Kemenristekdikti 2016 *Dasar Hukum TKT Hasil Litbang Online* (http://dinus.ac.id/repository/docs/lppm/TKT.pdf, accessed on 21 April 2019)

[11] Risbang Ristekdikti 2018 *Peraturan Menteri Riset, Teknologi, dan Pendidikan Tinggi Nomor 42 tahun 2016 Tentang Pengukuran dan Penetapan Tingkat Kesiapterapan Teknologi Online.* (http://risbang.ristekdikti.go.id/wp-content/uploads/2018/01/Permenristekdikti-42-2016.pdf, accessed on 14 April 2019)

[12] Kismanto Agus 2019 *Pengembangan Teknologi Konversi Biomassa menjadi Biofuel: Metoda Pyrolysa Cepat* (Jakarta:BPPT)

[13] Bezergianni, Stella 2017 Alternative Diesel from waste plastics *Journal of MDPI energies* 10,1750

[14] Boerrigter, H, dkk 2002 Green Diesel from Biomass by Fischer-Tropsch Synthesis: New Insight Gas Cleaning and Process Design *PGBW Expert Meeting* (*Strasbourg, France*) 1 October 2002.

[15] Herianto, Heri, dkk 2018 Synthesis of Green Diesel From Waste Cooking Oil Through Hydrodeoxygenation Technology With NiMo/γ-Al2O3 Catalysts *MATEC Web of Conferences* 156, 03032

[16] A. Srifa, K. Faungnawakij, V. Itthibenchapong, S. Assabumrungrat 2014 Roles of Monometallic Catalysts in hydrodeoxygenation of palm oil to green diesel *Journal of Chemical Engineering*, **278** pp 249-258

[17] Atthapon Srifa, Kajornsak Faungnawakij, Vorranutch Itthibenchapong, Nawin Viriya-empikul, Tawatchai Charinpanitkul dan Suttichai Assabumrungrat 2014 Production of bio-hydrogenated diesel by catalytic hydrotreating of palm oil over $NiMoS_2/YAl_2O_3$

catalyst.Bioresource Technology *Journal of Bioresourch Technology* **158** pp 81-90

[18]Jensen, Claus Uhrenholt 2015 Co-Processing potential of HTL bio-crude at petroleum refineries. Part 2: A Parametric hydrotreating Study *Journal of Fuel* **165** pp 536-543

[19]LIU lu-Juan, LIU Yong-gang, GAO Xiang, ZHANG Rui-qin, dan ZHAI Yun-pu 2017 Hydrodeoxygenation of bio-oil model compounds over amorphous Ni/Bi/SiO_2-Al_2O_3 catalyst in oil-water biphasic system *Journal of Fuel Chemistry and Technology MDPI* **45** pp 932-938

[20]Sugiana Dadi 2019 *Rencana Implementasi Green Refinery di Pertamina*. (Jakarta: PT Pertamina Indonesia)

[21]Natural Resources Canada 2012 *Final Report Study of Hydrogenation Derived Renewable Diesel as a Renewable Fuel Option in North America* (Canada:Ottawa Ontario)

[22]Perego Carlo 2015 *From Biomass to Advanced Biofuel: The Greendiesel Case*. (Bologna: Centre for Renewable Energy and Environmental Research Istito Eni Donegani: Novara)

[23]Kalnes et.al, 2009 dalam Koutinas et al 2016 *Handbook of Biofuels Production (Second Edition)* (Greece: Agricultural University of Athens)

[24]Hoekman, SK 2009 Biofuels in the US-Challenge and Opportunities. *Journal of Renewable Energy* **34** pp 14-22

[25]Jeffry, Skeer, et al 2016 Technology Innovation Outlook Advance Liquid Biofuels for Transport: Abu Dhabi. *Journal of IRENA* **1** pp 724–725

[26]Sari, Elvan 2013 *Green Diesel Production Via Catalytic Hydrogenation/Decarboxylation Of Triglycerides And Fatty Acids Of Vegetable Oil And Brown Grease* (Wayne State University, Major of Chemical Engineering)

[27]Gapki 2018 *Solar Hijau: Gagasan Super Optimalisasi CPO Online*. (https://gapki.id/news/6116/solar-hijau-green-diesel-gagasan-super-optimalisasi-cpo-crude-palm-oil, accessed on 25 April 2019)

[28]Indrawan, rio 2019 *Green Refinery Plaju dan Dumai akan serap 15 juta ton CPO per tahun Online* (https://www.dunia-energi.com/green-refinery-plaju-dan-dumai-akan-serap-15-juta-ton-cpo-per-tahun/, accessed on 25 April 2019)

[29]Alakangss, Eija, etal 2014 *Handbook of Biomass Technology Roadmap*. (Brussels:RCH)

[30]Basu, B 2017 Assessment of Technology and Manufacturing Readiness Levels *Journal of Biomaterials for Musculoskeletal Regeneration* pp 235-256

[31]Eni 2018 *Green Diesel and Eni Diesel Online* (https://www.eni.com/en_IT/innovation/technological-platforms/bio-refinery/green-diesel.page, accessed on 26 Maret 2019)

[32]Haldor, Topsoe 2019 *Hydro FlexTM. Technology Online*. https://www.topsoe.com/products/hydroflextmtechnology. Accessed on 30 Maret 2019)

An Explanation of Cybercrime in Financial Technology Industry: Supply-Demand Opportunity of Crime Theory and Economic Theories of Crime and Delinquency Approach

Nurina Munasyaroh, Muhammad Haikal Kautsar, Ikhsan Yoga Utama, Putri Alyani Fadhilah

Indonesia Defense University, IPSC Sentul, Bogor 18810, Indonesia

Email: nurinanrn@gmail.com

Abstract. Financial intermediaries services based on technology growth rapidly. Revolution in industry 4.0 contribute to catalize the increase of number. Intenet of Things, blockchain, and cryptocurrencies ared used by financial technology institutions. This study aims to determine the relationship between financial technology providers and cyber crime in Indonesia. This study uses a literature study approach, using two theories, there are supply-demand opportunity of crime theory and economic theories of crime and delinquency. The results of research 1 based on the theory of supply-demand opportunity of crime theory show that the existence of cybercrime crimes committed by criminals is due to the low prevention efforts of potential criminal targets, and the high level of vulnerability of criminal targets. Research results 2 based on the economic theories of crime and delinquency show that individuals who commit criminal acts consider costs and benefits and short-term benefits that will be obtained when committing a criminal act.

1. Introduction

Industrial Revolution fourth generation bring new changes in operational of industry. Financial Industry is one of may industries that is impacted by Industry 4.0. Financial Industry have to receive the present of *blockchain technology*, *internet of things*, *robotic*, etc. The emerging of Industrial Revolution drive new phenomenon of start up company in financial services based on technology that known as *financial technology* (fintech). Fintech company provide services such as *payment*, *peer to peer or business to business lending*, *crowd funding*, or just for literacy and *advisory*. The growth of *Fintech* in Indonesia increase rapidly. According to Wimboh (2019) as quoted in CNBC website the number of fintech institutions in Indonesia is approximately 99 company, but only one institutions of all that already has official permission from Financial Services Authority (OJK) (CNBC Indonesia, 2013).

The presence of fintech could bring positive and negative impact to the country. The positive impact of fintech is encourage public welfare by facilitate peoples needs, promote capability of Small Medium Enterprises Company to compete in national or international market, boost of national funding, and improve national financial literacy (Hadad, 2017). In other side the presence of fintech also carry negative impact, such as presence of industrial revolution in England in the 18 ages that also carry negative impact to the society, that is, illegal fintech institutions, money laundering, tax evation, contraband transaction (Pejkovska, 2018). Besides negative impact in finacial and economics crime, there also cybercrime risk in fintech industry. Technology risk of fintech must be calculated, cause fintech depend on technology in the operational. Several technology risk that faced by fintech institution is data breaching and stealing, hacking of payment system, and cyber spionage in corporate (Corbet and Gurdgiev, 2017). According to the phenomenon of fintech presence in Indonesia and also its impact. Researcher find it is very important to study why cybercrime happened in fintech industry. Researcher try to explain the phenomenon based on the supply-demand crime theory to suggest the preventive action and solution to minimize the number of cybercrime in fintech industry. This paper consist of five section that is first part introduction that explain phenomenon and goals of the study, second section literature review consist of the explanation of cyber, fintech, and several related research, third section explain of methodology of the research, fourt part section discussion of the study, and section part consist of summary and recommendation.

2. Methodology

Several institutions and expert try to define the phenomenon of Financial Technology (*fintech*), according to Micu and Micu (2016) financial technology is a new sector in the finance industry that incorporates the whole plethora of technology that is used in finance to facilitate trades (Micu and Micu, 2016). Next according to Shim dan Shin (2016) fintech is an emerging financial services sector that includes third-party payment, MMF, insurance product, risk assesment, authentication, and peer-to-peer (P2P) lending (Shim and Shin, 2016). Other definition from Arner, et al (2015) fintech refers to technology enabled financial solutions. Fintech is often seen today as new marriage of financial services and information technology (Arner *et al.*, 2015). Therefore fintech development could be segmented to four era. The first era of financial technology (*fintech 1.0*) from 1866 to 1987 was the first period of financial globalization supported by technological infrastucture such as translantic transmission cables which accomodate phone call order and transaction. The second era of financial technology (*fintech 2.0*) was the presence of Automatic Teller Machine (ATM). The Third Era of financial technology (*fintech 3.0*) was the presence of internet banking and mobile banking (Hadad, 2017). Next, the fourth era of fintech (*fintech 4.0*) was the presence of *blockchain* in *cryptocurrencies* and *internet of things* in financial aspect.

In fintech 4.0 integration of cyber space in financial transaction can not be separated. cyber space is a paraspace or nonspace that includes building blocks such as physical conceptual and perpetual space or virtual space, also consider the mediaspace aesthetic space, dataspace, and personal and social space (Strate, 1999). Linkages between fintech and cyberspace could be opportunities for offender to do crime act in fintech industry (cybercrime). According to Zeviar (1998) cybercrime is fraud, unauthorized access, child pornography, and cyberstalking. There is two type of cybercrime, that is cybercrime type I and cybercrime type II (Gordon and Ford, 2006). Characteristics of type I generally a single event from perspective of the victim; often facilitated by crimeware programs e.g keylogger, trojan horse, and theft data by hacking or viruses. Meanwhile cybercrime type II has characteristics it is generally an on-going series of events, involving repeated interactions with the target. For example the target is contacted in chat room by someone who, over time, attempts to establish a relationship. Such as cyberstalking and harassment, child predation, extortion, blackmail, stock market manipulation, complex corporate sepionage, and planning or carrying out terrorist activities.

There are severel studies that show the phenomenon of cybercrime in fintech industry. Study that had done by Corbet and Gurdigev (2017) about the presence of financial digital and correlation with cybersecurity risk finds that the presence of financial technology increase opportunities for financial hacker to exploit institution assets of fintech dan bank. Therefore current evidence suggest that the scale and intensity of the financial crimes are becoming more and more apparent and audacious. Other study by Pejkovska (2018) on negative impact of fintech in financial services sector in Europe Union, USA, and India, finds that presence of fintech bring negative impact on global financial sector such as corruption, data privacy breaching, and abuse of fintech services for illegal purposes. Then, study by Pandya (2018) on cryptocurrencies, suggest that the the virtual currencies, one of many product in the revolution industries 4.0, can facilitate for terrorist financing.

3. Methodology

This study use qualitative approach, which is based on non-numeric data such as article and picture, and filtration of data is done for interpretation from literature review (Creswell, 2003). Review sources from Journal, Report, Books, and article from reliable sources. This study use two theories to explain why cybercrime happened in fintech industry.

4. Discussion

Criminality in fintech industry can be explained by criminology theories. This theories explain phenomenon why and what makes crime in fintech industry occur. Among many theories researcher used to two theories to explain the fintech phenomenon, that is supply and demand of criminal opportunity theories and economic theories of crime and delinquency.

1.1. Theory of Supply and Demand of Criminal Opportunity

The theory of supply and demand of criminal opportunity stated by Cook (1986) this theory explain that crime occur like movement of supply and demand curve. In supply and demand crime opportunities explain correlation between goods prices and in goods quantity in market, then transaction happen when there is equilibrium between supply and demand curve (CNBC Indonesia, 2019). Thus how crime occur, crime ensue because there is prevention capability meet vulnerability of target. Offender will looking for target who have high vulnerability with low force of crime prevention. While victim will always to improve force of prevention when they asses they vulnerability is high. The illustration is showed in figure 1,

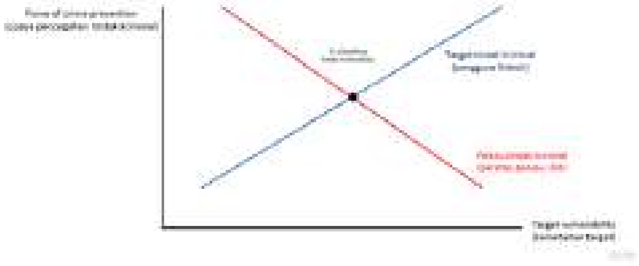


Figure 1. Vulnerability and force of prevention curve

As showed in figure 1 intersection point (T1) between offender curve with victim of crime is equilibrium condition. Equilibrium condition is point that represent crime action occur. Crime happen is when force of prevention target is consider low (equal with offender capability to do crime) by offender while the vulnerability is high. In perspective of victim when force of prevention equal with offender capability (low prevention force orientation) and the vulnerability is high, that is condition where crime occur.

The characteristic of victim curve as if supply curve in economics. The slope is positive, because when the vulnerability is high, the force of prevention is increase too, works like supply curve. In other side the characteristic of offender curve as if demand curve in economics. The slope is negative, because the offender always looking for potential victim that has low force of prevention with high vulnerability. So if the force of prevention is decreased the vulnerability will increase.

The factor that influence for the vulnerability is fear crime. Fear crime is model that propose by Balkin (1979) his model provides some useful insight about three functional relationships, each of which is written in linear from, the model is as shown below:

$$R = \frac{C}{X} \text{ .... } (1)$$

Fear crime (R) is a rational responses to actual a rational incidence of crime, where discrepancies appear it is because of faulty objective measures of crime incorrectly calibrating the real risk (Balkin, 1979). Fear crime is a ratio between observed victimization rate (C) to exposure (X) (Balkin, 1979). The relationship between the observed victimization rate (C) and Fear (R) may be either positively or negatively correlated with fear, e.g elderly people and rustic people are attractive targets for swindler of illegal fintech because of their low literacy vulnerability; their relatively low civtimization rates may result from their being more careful when using technology.

Exposure has a time dimension; for example data theft by a hacker may be measured as the time spent using internet from smartphone or PC. Exposure is related to victimization patterns of offender. Identifying victimization patterns we need is a list of the determinants of victimization risk. The analysis that is used is the criminal's perspective as a basis for generating such a list attractive targets for offender will suffer high rates of victimization. We used the attributes to the example of fraud victimization in Fintech Industry lately. A users of fintech services suicide after borrow some money from fintech institution,

a. Propinquity. Swindlers tend to minimize the probability of potential victim by reducing the number of people that use smartphone with availability of fintech apps in the smartphone. People who use fintech apps on smartphone have benefit in economics aspect to be hacked, compared with smartphone user who does not have. Swindlers will persuade the potential victim to join the financial institution using apps that they can download to their phone.

b. Payoff. Swindlers are mostly in it for economics beneficial. People with low literacy in technology and finance and require for financial support will be more attractive targets than high literate user of smartphone. Generally new user of smartphone, elderly people, housewife, or field worker are the most attractive targets of all in this respect.

c. Vulnerability. Swindlers want to complete the fraud successfully and to avoid involvement of law enforcement to their business. Therefore people who have higher education, established job, or high literate in technology will be less victimization by swindlers. While, poor man, illiterate people, and low educated people will be relatively vulnerable for swindlers.

d. Access to Law Enforcement. Swindlers want to minimize the probability and severity of punishment. One reason vulnerable victims are attractive to swindlers is that fraud that can be completed without indication of crime and seems like has benefit for both side. Therefore illegal fintech institution do not want to register the business to Authority of Financial Services (OJK). Beside that the target of swindle will be choose the one who have limited acces to law enforcement.

By identifying the determinant factor why the offenders do the crime, the regulator can reduce the number of fraud, data theft, and hacking to payment system.

Using the theory of supply-demand opportunities of crime, we can synthesize that cybercrime occur because high level of vulnerability of potential victim and low force of prevention. In cybercrime case vulnerability represent of people, process, and technology. People aspect in cybercrime case is literation of financial and technology of person, education, jobs, and income. the cybercrime case that we used in this study when the taxi driver borrow money from fintech institution without knowing the term and condition agreement, that was the vulnerability of the potentioal victims. In the other side the victims have no intention to increase the knowledge of how fintech works and effort to check the financial institution legality to Authority of Financial Services (OJK), that is indication of low force of prevention of the victim.

The swindlers that spot the high vulnerability of victim make use of opportunity to exploit the victim by charging high interest loan. Afterthat the swinlers create circumtances that push the debitor to immidiately pay the debt plus high loan, by calling the colleage and family that the contact is obtained from personal contact in smartphone. This circumtances makes the debitor stressful and end up with suicide.

Through suicide case because of fintech, can be infered that there is cybercrime type II in fintech industry. the crime occur because lack of prevention will and high vulnerability of fintech user. Therefore Authority of Financial services have to improve consumer protection strategiesand encourage the fintech institution to regist their business to minimize the number of cybercrime type II in fintech industry as force of prevention.

4.2.Economic Theories of Crime and Delinquency

Further approach to explain the actions of someone who did cyber crime by using economic theories of crime and delinquency. Economic theories of crime and delinquency stated by Jacob (2011). Jacob (2011) explains that decision-making taken by an individual to commit a criminal act considers of rational decisions that hoping to get benefits from a criminal act committed. There are two economic of crime models to explain this theory, there is (1) rational model of crime and (2) myopic model of crime (Jacob, 2011).

The rational model of crime is a model based on the future-oriented approach. The rational model of crime assumes that crimes committed by individuals will consider using the principle of cost-benefit analysis in committing a crime (McCarthy and Chaudhary, 2014). The decisions that criminals will take will be considered rationally by considering (1) the opportunity to commit criminal acts, and (2) the costs and benefits they will get when committing a crime. The case of a rational model of crime is a woman who loses a bank because of the online game transactions she does. Initially the woman made an online game purchase transaction through a virtual account, but the money from the woman was not deducted. Woman who know that the money is not reduced, try to make the transaction several times during one year. Based on the model of the rational of crime, the woman has committed a crime repeatedly by considering the costs and benefits she gets when the money she uses through the virtual account does not deduce when making online game purchases, she can continue to gain the benefit from playing online games without having to spend money. The woman also thought of the opportunity to return to a crime when she first bought something related to online gaming using her virtual account but was not deduce, the woman tried to do it a second time, but the second time, the crime was committed again because of the money she had still not cut off. Therefore, she continued to commit the crime up to several times a year, because without having to pay she could continue to play online games.

Another model in the economic theories of crime and delinquency is the myopic model of crime. Myopic model of crime is a model of crime based on a present-oriented approach. This model explains criminal behavior committed by individuals considering the direct benefits that the perpetrator will receive when committing a crime. It can be said that the offender who commits a crime wants to immediately benefit directly from the crime he committed. Criminals think to be able to get profits in the near term when he commits a crime. An example of this is the hacker who broke into the financial system of one of the domestic banks. The criminal acts hacking in the bank's financial defense system, which then changes the verification of the customer's account data, then transfers the balance to the offender's account. From this case, the perpetrator intentionally commits a crime by hacking the bank's financial defense system, so that he can get his profits in the near term, by transferring the balance from the customer's account that has been hacked by his account data.

5. Conclusions and Recommendation

Based on theory of supply and demand of criminal opportunity, criminal acts, especially cybercrime, occur when there is a meeting between prevention of criminal acts committed by potential victims with the vulnerability of criminal targets. Cybercrime occurs when the level of vulnerability of potential victims is high and the prevention efforts of criminal targets are low. The example case is a taxi driver who commits suicide is due to his inability to pay debts to a fintech company that provides loans.

Whereas, based on the economic theories of crime and delinquency, criminal acts committed by an individual consider rational decisions by expecting to get the benefits of the criminal acts committed. This theory is divided into a rational model of crime and myopic model of crime. Both of these models both expect to benefit from the criminal acts committed. However, there are differences from these two models, in which in a rational model of crime individuals who commit criminal acts will consider the use of the principle of cost-benefit analysis in carrying out their criminal acts. They will consider (1) the opportunity to commit criminal acts, and (2) the costs and benefits they will get from the crimes they commit. An example of cybercrime based on this model is the loss of one domestic bank by women who make purchase transactions related to online gaming. The woman committed criminal acts repeatedly due to opportunities and costs and benefits she got when making purchases related to online games, the virtual account used to pay was not deducted. In myopic model of crime, individuals who commit criminal acts will consider the benefits or benefits that will be obtained in the near future when he commits a criminal act. An example of this is the hacking of the banking defense system of one of the domestic banks. Criminals hack the system and change the verification of data owned by the customer, and then move the customer's account balance to his account.

This study has limitations, including the theory used to explain cybercrime crimes in the fintech industry in only two theories. Future studies are expected to add some theories or use other theories to explain the crimes of cybercrime in the fintech industry.

Acknowledgement

I would thanks to all lecturer and civitas academica of Indonesia Defense University and my all researcher that incorporated in this team.

References

[1] Arner, D. W., Barberis, J., & Buckley, R. P. (2015). *The Evolution of FinTech: A New Post-Crisis Paradigm?* Hongkong: The University of Hongkong.

[2] Balkin, S. (1979). Victimization Rates, Safety, and Fear of Crime. *Social Problems, 26*(3), 343-357.

[3] CNBC Indonesia. (2019, March 13). *Bos OJK Buka-bukaan Soal Arah Pengembangan Fintech*. Retrieved from CNBC Indonesia: https://www.cnbcindonesia.com/fintech/20190312113806-39-60089/bos-ojk-buka-bukaan-soal-arah-pengembangan-fintech

[4] Cook, P. J. (1986). The Demand and Supply of Criminal Opportunities. *Chicago Journals* , 1-27.

[5] Corbet, S., & Gurdgiev, C. (2017). Financial Digital Disruptors and Cyber-Security Risks: Paired and Systemic. *Journal of Terrorism and Cyber Insurance, 1*(2), 1-20.

[6] Creswell, J. W. (2003). *Research Design Qualitative, Quantitative, and Mix Methods Approaches (2nd ed).* California: Sage Publishing.

[7] Gordon, S., & Ford, R. (2006). On the Definition and Classification of Cybercrime. *Jounal of Computer Virology*, 13-20.

[8] Hadad, M. D. (2017). *Financial Technology (Fintech) di Indonesia*. Jakarta: Otoritas Jasa Keuangan.

[9] Jacob, Anupama. (2011). Economic Theories of Crime and Delinquency. *Journal of Human Behavior in the Social Environment, 21:270-283.*

[10] McCarthy, Bill., Chaudhary, Ali R. (2014). Rational Choice Theory and Crime. *Encyclopedia of Crime and Criminal Justice*

[11] Micu, I., & Micu, A. (2016). Financial Technology (Fintech) and its Implementation

on The Romanian Non-Banking Capital Market. *SEA Practical Aplication of Science*, 379-384.

[12] Pandya, A. (2018). *Cryptocurrencies A New Scourge of Terror Financing*. New Delhi: Vivekananda International Foundation.

[13] Pejkovska, M. (2018, 04 24). Potensial Negative Effect of Fintech on The Financial Services Sector. Helsinski: Metropolia University of Applied Sciences.

[14] Shim, Y., & Shin, D. H. (2016). Analyzing China's Fintech Industry from the Perspective of Actor-Network Theory. *Telecomunication Policy, 40*(2-3), 168-181.

[15] Strate, L. (1999). The Varieties of Cyberspace: Problems in definition and delimination. *Western Journal of Communication, 63*(3), 382-412.

[16] Zeviar, G. (1998). The State of The Law on Cyberjurisdiction and Cybercrime on the Internet. *Gonzaga Journal of Internasional Law*.

The Innovation of HR Cybersecurity Capacity Building through "Born to Protect"

Marina Christmartha A J, Jutan Martdupanus Manik
Indonesia Defence University, Bogor, 16810, Indonesia

E-mail: marinachristmartha@gmail.com mjutanmartdupanus@gmail.com

Abstract. According to the Internet World Stats, Indonesia made the fifth country with the highest number of internet users around the world in 2019. However, the number of internet users comes along with the number of vulnerabilities, due to threats in the form of minor disruption such as malware up to exploitation by hackers or foreign cyber army. This study focuses on the innovation made to protect Indonesia cyberspace by the Ministry of Communication and Information Technology of the Republic of Indonesia synergizing with PT. Xynexis International in conducting Born to Protect, a hacking contest program to capture human resources expert on cybersecurity. This program is to find generations with interest, talent, ability, and passion to be Indonesian IT gladiators who are willing to build up themselves and contribute to Indonesia's defense strategy. By using the study literature method, this research will describe how this innovation went in purpose to raise capable IT human resources from young generations in a fun and professional way.

1. Introduction

The world now is in its greatness where technology advance plays an important role in the evolution of globalization. Due to the advancement, people from around the world, societies, and cultures become integrated through the network of communication and trade. As if there are no more boundaries among countries, it is much easier to conduct multinational corporations in global markets, foreign trade, cross-cultural exchange, and many more, as positive sides humans can get from the outcomes. Computer and internet technology has created a new world or called cyberspace that contains citizens called 'netizens' who carry out various communications, interactions, and movements through the internet.

However, technological development has resulted in such a new wave of cyber threats to human life. This is marked by the development of the Internet which has been the fastest-growing area of technical infrastructure development. Through the information and communication technologies (ICTs) as the form of digitization, internet and computer integrate and function to produce products especially for electricity supply, transportation infrastructure, military services and logistics, and to the many ICT applications, such as *e-banking*, *e-commerce*, *e-trade*, *e-business*, *e-government*, *e-education*, and *e-retailing*. Nevertheless, in turn, ICT applications can potentially lead to new and serious threats that harm society in critical ways. Online fraud and hacking attacks are some of the examples of computer-related crimes that are becoming more severe by times. Despite the convenience offered through efficient channels that enable us to interconnect in a wide range of basic services in remote and rural areas, the disadvantages such as only identity theft and people's credentials or personal information are risks that must be dealt immediately.

The rapid development of Internet consumption eventually brings in harms, better known as Cybercrime. Cybercrime is a criminal act or crime utilizing computers of the internet. Cybercrimes can aim to the malfunction of computers, such as hacking or illicit use of computing systems, disfiguration of web sites, or creation and malicious dissemination of computer viruses. Cybercrimes can be also the instrument of perpetration that happens in the virtual world of the Internet, such as criminal harassment, fraud, or the sale of illegal substances.

According to the Indonesia Cyber Security Report 2017 published by ID-SIRTII in 2016, there were 135,672,948 total cyberattacks which have increased by more than 50% compared to 2015 with 89,691,783 attacks. The country with the most attacks on Indonesia originates from America which mostly sent DDOS attacks. The loss of space and limits shows that cybercrime is categorized as a borderless crime - conflict without boundaries of space and time. The major reasons that caused Indonesia vulnerable to cyberattacks are people's ignorance of the dangers of cybercrimes, and the inapplicability of a good security system despite the implemented digitalization in many companies. In 2019, Indonesia still becomes a country with the highest number of internet users around the world. The data from the Ministry of Communication and Informatics of the Republic of Indonesia shows that internet users in Indonesia have reached 171.17 million from a total population of 264 million Indonesians. However, all the occurrences happening in Indonesia concerning cyberattacks still indicate that Indonesia is still weak in cyber-security and is a country which produces hackers who endanger cybersecurity on an international scale.

The recent news showed three Indonesian hackers in Surabaya allegedly hacked thousands of websites and information technology systems in 44 countries. Those hackers are still 21 years old, majoring in information technology, and are members of the Surabaya Black Hat Community. Their purposes of hacking are to hack personal and corporate property system, make money by offering repayments, and damage system when they are rejected. An electronic government system in Los Angeles, United States is one of the victims, where the FBI revealed that the culprit uses an IP Address in Indonesia, precisely Surabaya.

Regarding the intensity of the cyberattacks that led to Indonesia, it's therefore crucial to a country to strengthen the internal security strategy to be able to cope with the challenges of the dynamic and global twenty-first century. The rise of cybercrime requires attention and seriousness in developing cybersecurity for a country including Indonesia. With the rise of cybercrimes, it can be said that Indonesia is still weak in its cyber-security. The nation is urged to enhance cybersecurity and protect critical information to keep the nation's security and economic well-being. Therefore, according to The Global Cybersecurity Agenda, there are seven main strategic goals in cybersecurity, which are built on five work areas: 1) Legal measures; 2) Technical and procedural measures; 3) Organizational structures; 4) Capacity building; and 5) International cooperation.

This research paper will focus on the fourth point which is *Capacity Building* which focuses on elaborating strategies for capacity-building mechanisms to raise awareness, transfer know-how and boost cybersecurity on the national policy agenda. Technological mastery is still a major problem in the development of cyber-security policies. It needs the development of HR capacity as a thing that must be considered.

Accordingly, The Ministry of Communication and Information Technology (KOMINFO) cooperates with PT Xynexis see this vital need for capable and expert human resources in handling cyberattacks by encouraging and capturing the younger generation's talents to become gladiators, the forerunners of Indonesian cyber network for all sectors. The Born to Protect Program, is based on the attempt to prepare human resources to protect the Indonesian state from cyber network attacks. Cybersecurity was a priority issue in the digital era and became one of the government's main agendas in entering the 4.0 industrial era that is based on the internet of things (IoT).

There's still a considerable gap between the needs and readiness of HR cybersecurity for both government and private and industrial sectors. The specificity in the IT field in Indonesia has not entirely been able to accommodate and teach cybersecurity which can be directly applied to the industry. Through Born to Protect, it is hoped that the gladiators could become cybersecurity experts who hold to the right ethics and disciplines.

2. Framework

Cybersecurity

Cybersecurity is a secure way to safeguard any kind of confidentiality and privacy to avoid disruption of data, computers, or mobile devices attacks. Cybersecurity, also known as computer security or IT security, is protection for computer systems from kinds fo damage that harms hardware, software, or information or disruption of the service it provides. The term 'cybersecurity' was hardly known in general speaking or public about two decades ago, but nowadays, the cybersecurity topic and issues are on top due to frequent cybersecurity attacks that harm many large companies or even state bodies. Cybersecurity has become a major concern to all levels of societies which in its practice needs advanced monitoring and surveillance but still preserve people's freedom.

Compared to physical security, cybersecurity is much different in many aspects. The digital information contained in cyberspace is immaterial and easily duplicated and exchanged to anyone in any place with extremely fast process and zero cost. This easiness however potentially results in a large-scale danger related with spread-out malware or attacks launched by a single person. Since digital information has no borders, maintaining cybersecurity is much harder than any other form of security.

Hence, The Global Cybersecurity Agenda (GCA), a global framework purposed for international cooperation in coordinating the world's response to the developing challenges to cybersecurity, aside from building confidence and security in the information society, formed five work areas of seven main strategic goals: **1. Legal measures**, which focuses on how to deal with legislative challenges of criminal actions over ICT networks in an internationally appropriate manner, **2.Technical and procedural measures**, focus on the key enhancement and approaches to improve security and also risk management in cyberspace, encompassing protocols, schemes, and standard, **3. Organizational structures**, which focuses on crisis management, prevention, detection, and response to the cyberattacks which enables protection of vital information infrastructure systems, **4. Capacity building**, which focuses on mechanisms of raising awareness, transfer know-how, and enhancement on cybersecurity as the national policy agenda, **5. International cooperation**, which focuses on international cooperation, coordination, and dialogue in making strategy dealing with cybercrimes.

Furthermore, cybersecurity is defined as all mechanisms which are carried out for protecting and minimizing disruption of confidentiality, integrity, and information availability. The main elements of cybersecurity are:

1. **The security policy document** is a standard document used as a reference in carrying out all related information security processes.
2. **Information infrastructure** is media which plays a role in operations continuity which includes hardware and software. The examples are routers, switches, servers, operating system, database, and website.
3. **Perimeter Defense** is media acts as a defense component on information infrastructures such as IDS, IPS, and firewall.
4. **The Network Monitoring System** is a media whose role is to monitor feasibility, utilization, and information infrastructure performance.
5. **System Information and Event Management** is a media that plays a role in monitoring various events on the network including occurrences related to security.
6. **Network Security Assessment** is an element of cyber-security that acts as a controller mechanism

and provide a measurement level for information security.

7. **Human resource and security awareness** relating to human resources and the awareness of information security.

Cybersecurity Capacity Building

Cybersecurity Capacity Building is defined as the way to empower individuals, communities, and governments to achieve development on the ability to reduce digital security risks got from accessing and using Information and Communication Technologies (ICT). The definition shows that cybersecurity building stresses on the importance of managing risks which of using ICT that mostly can affect economies and societies by building resilient systems that can withstand and recover from attacks, accidents, or threats that can lead to incidents. This concept especially is not only framed as an intergovernmental issue only, but this requires a multi-stakeholder approach from national or even various jurisdictions.

Cybersecurity Capacity Building (CBB), in fact, covers a set of activities besides a comprehensive approach. Explained by The Global Cyber Security Capacity Centre's (GCSCC) National Cybersecurity Capacity Maturity Model (CMM) which provides a framework for understanding the capacity of national cybersecurity. It is illustrated that there are five CMM's dimensions with various factors that depict that raising awareness is as much as creating legal frameworks and enhancing technical expertise which encompasses five dimensions: 1. *Cybersecurity Policy and Strategy,* 2.*Cyber Culture and Society,* 3.*Cybersecurity Education, Training, Skills,* 4.*Legal and Regulatory Frameworks, and* 5.*Standars, Organizations, Technologies.* This shows that cybersecurity is not only a small scope of raising awareness but also needs normative understandings of other needs such as technical challenges, and even political judgment-calls. The capacity building services in practice should be adjusted according to the countries or organizations that provide the service. The exact services should be considered and prepared as they carry out the projects, for there might be great potentials on the violation towards many cybersecurity capacities and techniques. Given that some security assistance, in reality, can cause human rights abuses that are purposed for malicious purposes. Accordingly, in implementing cybersecurity capacity building, it should be considered wisely who the actors are that adequate to set the values and policies in the practice. The Cybersecurity Capacity Building in practice contains actors and activities from various sources, such as a variety of governments, regional, and international organizations, also non-state actors who are responsible to increase cybersecurity capacity. The National Governments often lead coordination efforts, though the responsibility for cybersecurity capacity building is shared by many stakeholders. The regional and international organizations also substantially contributed to cybersecurity capacity building. The example given for this case in the global level is how cybersecurity capacity building is part of the mandate of the International Telecommunications Union (ITU), the United Nations' specialized agency responsible for ICTs. Then Non-State Actors, which include technical and non-profit organizations, research institutions, and the private sectors, carried out projects and often raised awareness or help individuals in improving their cybersecurity expertise. The contribution that is so far done by non-state actors is like the development of a number cyber maturity model, that allows a country to assess and also benchmark their cybersecurity maturity, and the policymakers to define defense policy strategies.

Cybersecurity Innovations

In practice, the Government, regional or international organizations, and non-state actors need innovations and creativity in their cybersecurity collaborations. The innovations and creativity will provide chances of digital economy growth which can accelerate innovations to support state policy in e-commerce. The digital economy growth can be also got from cybersecurity human resources escalation to contribute to national cyber-security policy.

The cybersecurity innovation is expected to be able to increase the synergy between the government and the industry in improving HR competencies through more tangible technical cooperation. According to the president's vision to place Indonesia as the largest digital economy country in Southeast Asia by 2020, the country has put attention on the considerable potentials in Indonesia which can be a digital economy country.

The attempts to overcome the threats trend in 2019, Cyber and National Encryption Agency (BSSN) has prepared strategic steps, including 1) regulations establishments and public sentiment enhancement towards the protection of personal data, 2) the development of *Advances Threat Protection* (ATP) technology to detect APT, 3) *Multi-Factor Authentication* will become standard on all online transactions, 4) Many organizations need Cyber HR who are proficient in cybersecurity, 5) Discussion of cybersecurity agreements including cyber diplomacy.

Born to Protect

Born To Protect is a program that is held responding to the human resource requirements in the current era who are capable of handling cyber attacks, whether for government or the private and industrial sectors. This urgent need to encourage the Ministry of Communication and Information (KOMINFO) to capture younger generations' talents to become IT gladiators who will be forerunners for the Indonesian Cyber Network in all sectors. The Born to Protect program emerged based on the idea of preparing human resources to protect the Indonesian state from cyber network attacks. This program is fully supported by the Ministry of Communication and Information Technology cooperates with PT Xynexis.

Besides the aim of identifying new talents in the field of Cyber Security, this program is also purposed for gathering young people who have a passion for Cyber Security who during the process will be educated well so that they can directly help the industry and government in maintaining information security.

The Roadshow was held in 10 selected cities to find talents with the potential of Cyber Security. This program collaborates with universities in each city to make it easier to reach talent. The selected countries are Medan, Palembang, Jakarta, Bandung, Jogjakarta, Malang, Samarinda, Denpasar, Makassar, and Manado. The selected cities are chosen through the collaboration with IPKIN & APTIKOM, to simplify the process finding the intended human resources in IT.

3. Research Methods

The method used for this research is descriptive and non-experimental writing which is to analyze the innovation made by the government and other organizations to raise HR cybersecurity through Born to Protect program. The researcher uses secondary data types which are acquired from academic books, journals, news, scientific articles, and websites. The references used are current and relevant to this research.

4. Discuss

Innovation in Capacity Building through Born to Protect

As one of five work areas formed by The Global Cybersecurity Agenda (GCA), the capacity building enforcement of Born to Protect is shown by how the collaborations made among the government and the other organizations and non-state actors. Born to Protect coordinated by the Ministry of Communication and Information Technology (KOMINFO) as the government, with PT. Xynexis International – the local pioneer in Security Security Service in Indonesia, The Association of Computer Science University (Aptikom) – in helping to provide and preparing the top ten universities with IT potentials, and Noosc Academy which is engaged in developing a technical system to provide hacking games need for this program.

The innovation in this program is shown by the manifestation of Cyber and National Encryption Agency (BSSN) strategic steps which is the collaboration of many organizations with the government in an attempt to find young Cyber HR who are proficient in cybersecurity through technical cooperation. The innovative and creative strategy made is at how they targetted you generations with a passion for Cybersecurity to be well educated so they can contribute to the nation and also help industries and governments in maintaining ICT in Indonesia. The age group of the participated gladiators was 16-22 years. This shows how big are the potentials of the Indonesian people. This also helps the industries to have qualified human resources in IT who are fresh graduated and ready to work to be the agents dealing with the cyber threats for now and later.

Although there have been other typical hacking contests held in Indonesia, the innovation which makes this program is different is that the *hacking contest* phase in Born to Protect is just one of the processes before the real training itself which would equip the gladiators with the needed skills to overcome the current cyberattacks. The program was held in four phases, which is in phase one, Born to Protect attract 8,661 people through online registration. From the online registration, the registrants would get barcode which is used for the next step; the audition. In the next step, the auditions were held in ten selected cities that have great potentials in cybersecurity. Accordingly, the organizers collaborated with universities in the cities to reach their talents. From the auditions conducted in the cities, 1,000 people were chosen to continue to the semifinal round where their online expertise would be competed through the capture the flag (CTF) platform and awarded international certification from the ec-council. The step was then continued to the most awaited part; digicamp. In this part, the best 100 gladiators would be specifically educated and trained. During two weeks of training and digicamp, the gladiators were so enthusiastic and showed their talents extraordinarily. The 100 participants learned *network defender* and *ethical hacking*. The gladiators were forged with international standardized CND (Certified Network Defender) and CEH (Certified Ethical Hacker) materials combined with simulations of real working experience in the form of individual and group CTF (capture the flag). The great opportunity was continued until the end part, the industrial day. This event is the moment where the organizers would provide great industries to present their industry to the finalists/gladiators to provide depictions of the cybersecurity needs in Industries and to provide information of what benefits the participants could get if they joined the company. In Industrial day, the organizers bridging the individuals and groups with CND certification to the needs of HR IT security who are ready to work and tough which at the end they received international certification.

All industries which have transformed their businesses into digital and ICT will certainly need the prepared talents through this program. The organizers were optimistic that the Born to Protect will help the government in reducing unemployment and in improving the quality and creativity of human resources in the IT world, especially in cybersecurity. Not only that, to support this program, the gladiators were fully-accommodated: rooms, food, and transportations. The trainers were all qualified in IT which almost of them have been well known for this field both nationally and internationally.

This program was initially named Born to Control which afterward was criticized by the Minister of Communication and Information Technology for the reason that people could misinterpret the name as the way to control and threat people's freedom and privacy. The recommendation made was to change the name into '*Born to Protect*' or '*Born to Secure*' which is better to hear and to understand. The only problem was then people had already registered in the Born to Control website, but when this was changed, there was a switched system that made some of the online registration not successful. This happened as a small technical problem that then was recovered soon after.

The organizers expect that this program can be conducted continuously every year. If it is consistently conducted, there would be chances for international world to see this program and would be interested to build relationship and cooperation with Indonesia HR cybersecurity. Similarly, China and Vietnam who are currently developing a human resources program in cybersecurity, Indonesia has also great chances to dominate the world with IT talents and skills that in the future will contribute to cybersecurity.

The main purpose of Born to Protect is with the big number of citizens and internet users, Indonesia can provide big numbers of HR cybersecurity altogether to deal with the greater threats to the nation's cyberspace in the future. The sustainability of this program is the only concern for this time being since the program can potentially give benefits and solutions in dealing with digital threats.

5. Conclusion

Based on this research results which has been discussed in the previous chapter, it can be concluded that the innovation of cybersecurity program in Born to Protect can be seen by the collaboration aspects and innovative process that make it different from the other hacking contests at usual. To be seen by the implementation of the program, it is hoped that the collaboration between the Ministry of Communication and Information Technology (KOMINFO) with other organizations and non-state actors could be maintained in the future to raise the potentials of HR cybersecurity.

Born to Protect program can potentially give more opportunities in choosing suitable kinds of job that suits these generations' talents and abilities. The upcoming threats and digital wars have gradually changed and evolved, and so will the needed employments in the future. The recommendation could be given to this program is for the government to keep the sustainability of this program, so it is not only to be a seasonal event but may become a fixed annual event to escalate Indonesia's reputability of Human Resources cybersecurity in the worldwide.

References

1. Albrow, M. (1990). Globalization, Knowledge, and Society. London: Sage Publication.
2. Ardiyanti, H. (2014). Cyber Security dan Tantangan Pengembangannnya di Indonesia . Politica Vol. 5 No 1, 95 -110.
3. Arifah, D. A. (2011). Kasus Cybercrime di Indonesia. Journal Bisnis dan Ekonomi (JBE), 185-195.
4. Baker, N., & Stephens, A. (2006). Making Sense of War: Strategy for the 21st Century. Cambridge: Cambridge University Press.
5. Briliyant, O. C., & Ashari, R. A. (2018). Rencana Penerapan Cyber-risk Management Menggunakan Nist CSF dan Cobit 5. Journal of Information System, Volume 14, Issue 2, 83-90.
6. Conteh, N. Y. (2016). Cybersecurity: risks, vulnerabilities, and countermeasures to prevent social engineering attacks. International Journal of Advanced Computer Research, Vol 6 (23), 31-38.
7. Gercke, M. (2012). Understanding cybercrime: phenomena, challenges, and legal response. Geneva: International Telecommunication Union (ITU).
8. Hohmann, M., Pirang, A., & Benner, T. (2017, March 6). Advancing Cybersecurity Capacity Building. Retrieved June 6, 2019, from the Global Public Policy Institute: www.gppi.net
9. James, C. (2016, November). Cybersecurity Threats Challenges Opportunities. Retrieved June 6, 2019, from ACS: https://www.acs.org.au
10. KOMINFO. (2018, Mei 2). Born to Protect Siap Lahirkan SDM Cyber Security yang Tangguh. Retrieved June 6, 2019, from KOMINFO, Sorotan Media: https://kominfo.go.id
11. KOMINFO. (2018, Oktober 5). Born to Protect, Siapkan Gladiator Dunia Siber Indonesia. Retrieved June 6, 2019, from KOMINFO, Berita Kementerian: https://www.kominfo.go.id/
12. KOMINFO. (n.d.). Born to Protect. Retrieved Mei 20, 2019, from https://www.borntoprotect.id/
13. Lewin, N. (n.d.). All Change for Industry 4.0. Retrieved June 6, 2019, from Festo Didactic: https://www.festo-didactic.com/int-en/
14. Podhorec, M. (2002). Cyber Security within the Globalization Process. Journal of Defense Resources Management, 19-25.
15. Pratama, M. S., Miftach, F., & Ali, Y. (2018). The Cyber Security Strategy of General Elections Commission in Facing the General Election 2019. Journal of Asymmetric Warfare, Volume 4, Number 3, 77 - 94.
16. Smith, M. (2015). Research Handbook on International Law and Cyberspace. Cheltenham: Edwar Elgar Publishing Limited.
17. Subagro, A. (2015). Synergy on the Facing of Cyber Warfare Threat. 1-23.

Technology Readiness Level Assessment of Green Gasoline to Support Energy Security

Margareta E. Rindu S.[1,a], Andre Amba Matarru[1,b] , Nugroho Adi Sasongko [1,2,c]
[1] Energy Security Graduate Program, Indonesia Defense University (UNHAN),
Indonesia Peace and Security Centre (IPSC), Bogor 16810, Indonesia
[2] Agency for The Assessment and Application of Technology (BPPT), M.H. Thamrin
Road No.8, Jakarta 10340, Indonesia

Email : [a] margaretaega.rindu@gmail.com ,[b] andreambamatarru@gmail.com ,
[c]nugroho.adi.sasongko@gmail.com

Abstract. National development continues to be pursued primarily through technological innovation. Especially in the transportation sector, if the energy needs dominated by fuel continue to increase, the energy crisis will occur. Indonesia's energy development priorities are carried out by transforming fossil fuels into biofuels by utilizing CPO into green gasoline. To measure preparedness the results of these innovations are realized in TRL (Technology Readiness Level). Each level level shows the development and readiness of green gasoline as an alternative to fossil fuel substitutes. TRA (Technology Readiness Assessments) in the development of green gasoline is used to determine the maturity of new technologies based on the level of success and acceptable risk. TRA results are aspects to then enter the TRL stage. On a scale of level 1 to 9 the TRL (Technology Readiness Level) of green gasoline in Indonesia has succeeded in co-processing green gasoline for commercial scale. Therefore, the commitment of all relevant stakeholders is expected to lead Indonesia to achieve national energy independence and security.

1. Introduction

National development continues to be pursued primarily through technological innovation. As the country with the largest energy consumption in the Southeast Asia region in primary energy consumption, Indonesia has been a net oil importer since 2004. Especially in the transportation sector, if energy needs are dominated by fuel continues to increase without any changes in usage patterns, technological innovation, and transformation fuel from fossils into biofuels is not done, then sustainability and energy security in Indonesia will be disrupted. The energy crisis is a real threat because of the depletion of fossil energy that is increasingly depleting. The 2017-2050 period with an average GDP growth of 6.04% is estimated to drive an increase in Indonesia's energy needs in the future [1]. Referring to this, certainly the target of reducing Indonesia's greenhouse gas emissions by 2030 will be difficult to achieve.

In order to achieve national energy independence and security as stated in PP No. 79 of 2014 concerning National Energy Policy, the RUEN (Rencana Umum Energi Nasional) Regulation prioritizes Indonesia's energy development by maximizing the use of EBT that pays attention to economic levels, minimizes the use of petroleum, optimally utilizes natural gas and new energy and makes coal a mainstay of national energy supply. Efforts to support Indonesia's energy development priorities need to be done by alternative fuel preparedness before transforming fossil fuels into biofuels and being commercialized.

As an archipelagic country, Indonesia's transportation sector is dominated by land transportation which supports the activities of all sectors of energy users. Energy needs in the transportation sector are projected to grow by 4.6% per year and will require 4.6 times more energy by 2050. Therefore, increasing the role of New and Renewable Energy in meeting domestic energy needs is needed to maintain the balance of energy supply.

Systematic measurements are carried out at the level of technological preparedness to obtain the optimal level of technological readiness. The use of one derivative of Crude Palm Oil (CPO), namely Refined Bleached Deodorized Palm Oil (RBDPO) to green gasoline is expected to deliver Indonesia to the new era of Vegetable Fuel Industry and answer the global challenge of producing environmentally friendly fuels while replacing fossil fuels thinning. For the country's economy, the presence of green gasoline can reduce the country's balance of payments pressure on imported crude oil. The success of the development began with B20 and B30 which began to be tested on vehicles in 2019, and continued to be increased to reach 100 percent or become green gasoline. Development continues to be carried out by compiling tables consisting of level 1 to level 9. In each level level shows the development and readiness of green gasoline as an alternative to fossil fuel substitutes. The FRL (Fuel Readiness Level) in the development of green gasoline is used to regulate and track the development position of the theoretical process, laboratory tests, certification, and distribution for commercialization activities or entering TRL 8, which is just waiting for Pertamina's role in commercializing Green Gasoline (TRL 9). In this paper, the author tracks the level of green gasoline preparedness on a level 1 to 9 scale on TRL (Technology Readiness Level).

2. Research Method

The method used in this paper is a review of journals and environmental reports related to the development of green gasoline and FRL, especially in the land transportation sector. Each level in the FRL has an Operating Procedure Standard in which each detail has been verified.

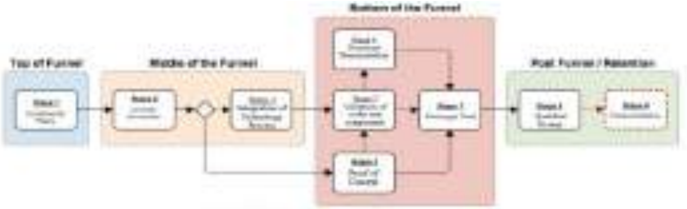


Figure 1. Flow Chart of TRL Green Gasoline

3. Technology Readiness Assessments

Technology readiness assessment (TRA) is the level at which organizations try to determine the maturity of new technologies including performance goals (technical and non-technical such as costs, interim failures, etc.), TRL Evaluation, and level of research and development difficulties [2]. TRA assists in determining whether technology has an acceptable level of risk, based on the extent to which they have been tested under real operating conditions. TRA results are reports that are aspects that must be passed before entering the Technology Readiness Levels stage.

4. Technology Readiness Level

A qualitative approach to assessing the maturity level of new technologies is known as the level of technological readiness (TRL). Technology Readiness Level (TRL) is a systematic metric / measurement system that supports the assessment of certain technological maturity and within the scope of imagined applications. This method evaluates the maturity of technology using the Technology Readiness Level (TRL) scale pioneered by NASA in the 1980s as a tool to select technology vendors that fit their needs, in order to reduce the risk of failure. The TRL scale ranges from 1 (basic research) to 9 (system successfully used). Figure 1 provides an overview of the TRL scale, including summary correlations to various stages in the development and maturation of technology. This approach can be used for utilities to decide when to deploy technology or communication systems in the smart grid [3].

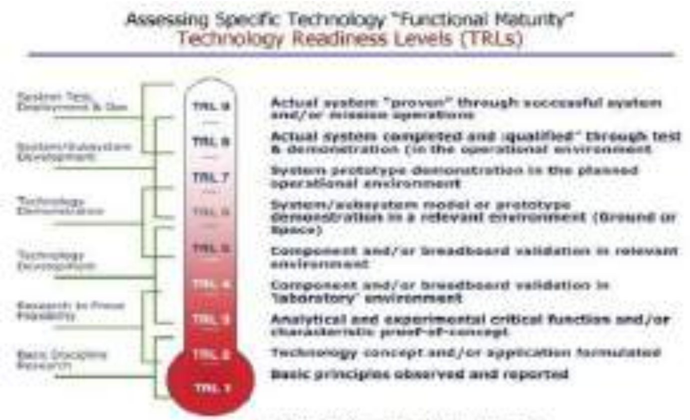

Assessing Specific Technology "Functional Maturity"
Technology Readiness Levels (TRLs)
System Test, Deployment & Ops
System/Subsystem Development
Technology Demonstration
Technology Development
Research to Prove Feasibility
Basic Discipline Research
TRL 9
TRL 8
TRL 7
TRL 6
TRL 5
TRL 4
TRL 3
TRL 2
TRL 1
Actual system "proven" through successful system and/or mission operations
Actual system completed and "qualified" through test & demonstration (in the operational environment
System prototype demonstration in the planned operational environment
System/subsystem model or prototype demonstration in a relevant environment (Ground or Space)
Component and/or breadboard validation in relevant environment
Component and/or breadboard validation in "laboratory" environment
Analytical and experimental critical function and/or characteristic proof-of-concept
Technology concept and/or application formulated
Basic principles observed and reported

Figure 2. Overview of the TRL scale

TRL does have some advantages in the smart grid as a way to report and record progress during development. TRL for smart grid must be a documented verification that must be updated along with development, helping to successfully implement smart grid communication in the electricity network [4]. Figure 2 illustrates the path of technological performance maturation vs. technology risk.

In the author's view, TRL can be used in developing smart grid communication technology to report and record progress during development, commissioning and disposal.

4.1. Green Gasoline Technology Readiness Level (TRL):

TRL 1: Basic principles of technology have been researched and recorded.

The first stage of Co-Processing as one of the options for green fuels production methods through the processing of raw materials of vegetable oil with petroleum simultaneously into hydrocarbons is used as a green gasoline processing technology. RBDPO Co-Processing is done in Residue Fluid Catalytic Cracking Unit (RFCCU) Refinery Unit III. This process is carried out by RBDPO injection in stages starting from 2.5% -7.5% wt on RFCCU feeds. The arrangement of the feedstock composition between Hot M / HVGO and RBDPO is done to maintain the RFCCU System Heat Balance Reactor-Regenerator. Plant test in the first stage was carried out for 7 days of RBDPO injection operation.

TRL 2: Technology Concepts and / or Formulated Applications.

The second stage is mapping and preparing facilities and facilities such as Line, Tank, Jetty. The RFCCU Technology Readiness Assessment (TRA) Mapping was carried out. Technology and tool readiness is carried out, proven trials have succeeded in producing quality products that are environmentally friendly and have the potential to reduce imports of crude oil, as well as high Tingkat Komponen Dalam Negeri (TKDN) content. RBDPO loading was carried out at PT SAP Mariana and unloading and preparation of RBDPO Dry Stock at T-202 Tank. At this stage the technology enters the peak stage of laboratory development which will include several variable comparisons of time and the addition of a number of chemical and physical processes. Comparison of the time of engineering treatment gives some results of significant comparisons of some of the chemical properties of physics.

In the process, CPO is neutralized to separate gum from dissolved compounds such as pospatida, high free fatty acids using steam in a vacuum with the addition of alkali. If the content of low free fatty acids is enough to add NaCO3. Bleaching is done for decolorization aimed at removing dyes in oil. This is done by adding an absorbing agent such as activated charcoal, clay or by treating chemical reactions after the dye is absorbed and then the oil is filtered. The latter deodorizing aims to eliminate odors that have the potential to affect oil receipts by consumers. The compounds removed are aldehydes and ketones [5].

The pilot test at Pertamina RTC with the Advanced Cracking Evaluation (ACE) test showed that RBDPO could potentially be processed in the RFCCU unit, through co-processing with valuable yield products that are still typical with the yield of existing conditions. It is technically found that CoProcessing technology is more perfect with chemical processes, resulting in high quality green gasoline fuel (octane 91.3).

Figure 3. Level 1 and 2 TRL Green Gasoline

PERTAMINA
Dry Gas
Green LPG
Green Gasoline
LCO
Slurry Oil

Figure 4. *Co-Processing* RBDPO Technology in RFCCU

TRL 3: Proof-of-concept and analytical and experimental characteristics.
The analytical and experimental stages of proof of concept note that co-processing produces high quality

green gasoline with the lowest octane 90.7 at 2.5% injection and highest octane 91.3 with 7.5% injection. In the Base condition the value of the octane barrel of gasoline has increased by 1.6% from 1,220 to 1,240 when compared with injection co-processing of 7.5%. Green gasoline production reaches 405MB / month or 64,500 kilo liters / month is considered able to reduce the crude intake by 7.36MB per day equivalent to USD 160 million per year.

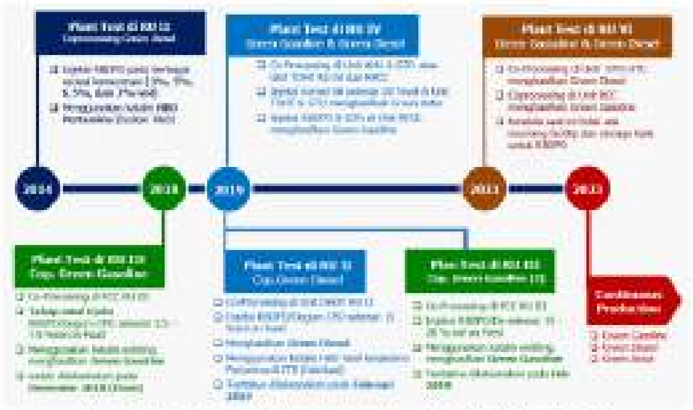


Figure 5. Plant Test of Co-Processing Technology RBDPO in RFCCU

TRL 4: Verify in controlled environmental conditions.

Following a successful "proof-of-concept", basic technology components are integrated to ensure that each of these components can operate. Pertamina announced that the Plaju Refinery Unit (RU) III Plaju, South Sumatra's Residue Fluidized Cracking Catalityc Unit successfully tested co-processing of palm oil into green gasoline, green LPG and smaller percentages of green propylene. Co-processing is done by injection of Refined, Bleached, and Deodorized Palm Oil (RBDPO) to 7.5% on feed [6]. So that green gasoline enters the TRL 4 stage.

TRL 5: Validate the code, components and or collection of components in the relevant environment.

Verification of components and / or use of technology licenses as a place to provide intellectual rights can be established at this stage. Basic technological components are integrated with supporting elements that are realistic enough so that technology can be tested to meet regulations to the standards in an environment that is simulated under controlled conditions. Green Gasoline components need to be tested to meet the requirements for co-processing compatibility. The framework obtained from this stage provides an overview of the determination of components or research facilities to determine them in the right environment.

The development of catalysts is expected at this stage to be immediately implemented to the renewal of existing development technologies. Subsequent tests will be held on co-processing technology in mixing fossil oil production. The co-processing that has been successfully carried out at the Plaju III refinery and Cilacap IV refinery.

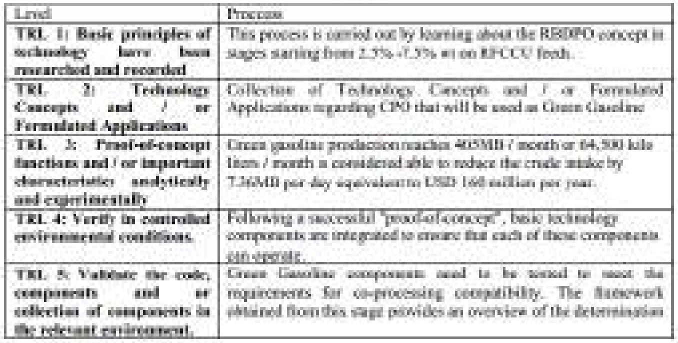
TRL 6: Stage system / sub-system model or prototype demonstration in the appropriate environment.
This level represents a big step in the readiness shown by technology. At this level, the reliability of the first product of Green Gasoline has been demonstrated and documented. TRL6 level means the communication system is ready for pilot scale demonstrations. Successful pilot scale trials, together with appropriate support and maintenance, show that the Green Gasoline production system is ready for large-scale implementation.

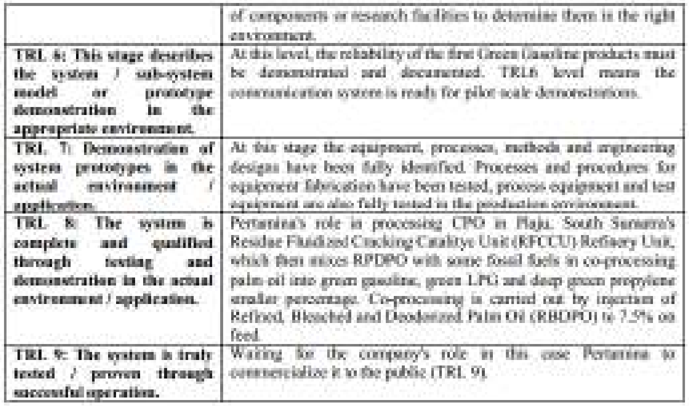
TRL 7: Demonstration of system prototypes in the actual environment / application.
At this stage the equipment, processes, methods and engineering designs have not been fully identified. The process and procedures for equipment fabrication have been tested, process equipment and test equipment have also been fully tested in the production environment. Design to cost has been well calculated, and fabrication is not well understood. Large-scale production processes for business and commercialization are still in process. From this test, there are still many further tests that must be done to ensure the specifications of the product, optimization of mixing and other technical matters as well as economic feasibility to be able to further scale up the business.

TRL 8: The system is complete and qualified.
Through testing and demonstration in the actual environment / application. At this stage the overall indicators for TRL 8 have not been fulfilled. Products cannot be produced in full capacity. Pertamina's role in processing CPO in Plaju, South Sumatra's Residue Fluidized Cracking Catalityc Unit (RFCCU) Refinery Unit, which then mixes RPDPO with some fossil fuels in co-processing palm oil into green gasoline, green LPG and deep green propylene smaller percentage. Co-processing is carried out by injection of Refined, Bleached and Deodorized Palm Oil (RBDPO) to 7.5% on feed.

TRL 9: The system is truly tested / proven through successful operation.
This final stage is getting closer to proof of RBDPO Co-processing, starting from operational concepts, technology investment estimates that have been made, technology that is tested in actual conditions, productivity at a stable level, estimated production prices compared to competitors, and subsequent competitor technology studied and known. Until waiting for the company's role in this case Pertamina to commercialize it to the public (TRL 9).

Table 1. TRL Summary of Green Gasoline





Level	Process
TRL 1: Basic principles of technology have been researched and recorded	This process is carried out by learning about the RBDPO concept in stages starting from 2.5% -7.5% wt on RFCCU feeds.
TRL 2: Technology Concepts and / or Formulated Applications	Collection of Technology Concepts and / or Formulated Applications regarding CPO that will be used as Green Gasoline
TRL 3: Proof-of-concept functions and / or important characteristics analytically and experimentally	Green gasoline production reaches 405MB / month or 64,500 kilo liters / month is considered able to reduce the crude intake by 7.36MB per day equivalent to USD 160 million per year.
TRL 4: Verify in controlled environmental conditions.	Following a successful "proof-of-concept", basic technology components are integrated to ensure that each of these components can operate.
TRL 5: Validate the code, components and or collection of components in the relevant environment.	Green Gasoline components need to be tested to meet the requirements for co-processing compatibility. The framework obtained from this stage provides an overview of the determination of components or research facilities to determine them in the right environment.
TRL 6: This stage describes the system / sub-system model or prototype demonstration in the appropriate environment.	At this level, the reliability of the first Green Gasoline products must be demonstrated and documented. TRL6 level means the communication system is ready for pilot scale demonstrations.
TRL 7: Demonstration of system prototypes in the actual environment / application.	At this stage the equipment, processes, methods and engineering designs have been fully identified. Processes and procedures for equipment fabrication have been tested, process equipment and test equipment are also fully tested in the production environment.
TRL 8: The system is complete and qualified through testing and demonstration in the actual environment / application.	Pertamina's role in processing CPO in Plaju, South Sumatra's Residue Fluidized Cracking Catalytic Unit (RFCCU) Refinery Unit, which then mixes RPDPO with some fossil fuels in co-processing palm oil into green gasoline, green LPG and deep green propylene smaller percentage. Co-processing is carried out by injection of Refined, Bleached and Deodorized Palm Oil (RBDPO) to 7.5% on feed.
TRL 9: The system is truly tested / proven through successful operation.	Waiting for the company's role in this case Pertamina to commercialize it to the public (TRL 9).

5.Conclusion

To measure the preparedness of alternative fuel technologies for transportation, especially land, it can be started with TRA to then continue to use TRL. The energy crisis and Indonesia's energy development priorities are pursued through green gasoline. Innovation in Green Gasoline technology prepared by coprocessing green gasoline for commercial scale on TRL 8 and then waiting for Pertamina's role to commercialize to the community (TRL 9). From the results of this test there are still many improvements and further tests that must be done to ensure the specifications of the product, optimization of mixing and technical matters up to the stage of economic feasibility which can then be scaled up for business scale.

In conclusion, Co-processing is more effective so that it is chosen to be implemented in the near future with consideration:

- Low Investment Cost, with a minor modification unit of the existing refinery.
- High Operation Flexibility, where two feeds are used (fossil and vegetable) so as to anticipate uncertainty in the amount of raw material supply and price.
- The time needed for EPC is relatively faster.
- Enables the option to feed 100% vegetable oil.

Green fuel production is related to efforts to reduce the country's balance of payments pressure on imported crude oil. This effort strongly supports the Government in reducing the use of foreign exchange, where Pertamina can save crude imports by 7.36 thousand barrels per day or in a year can save USD 160 million.

Synergy between related energy stakeholders is expected to be able to accelerate the strategy of transforming fossil energy into green energy while still observing sustainability aspects.

Acknowledgements

Our great gratitude goes to the teachers and friends who have supported us in developing this research. This paper is dedicated to researchers who want to know the readiness of technology in processing Green Gasoline. Inspiration was obtained from learning meetings held at the Indonesia Defense University, especially the Defense Management Department, majoring in Energy Security.

The authors obtained several sources of information about the development of Green Gasoline from fellow workers in the Energy Security class and lecturers who taught about Energy Technology. We hope that Green Gasoline technology can become a sustainable Indonesian energy alternative in the future.

Reference

1. BPPT Outlook Energy Indonesia 2018
2. J. Meneses Ruiz, C.F. Garcia Hernandez 2015 Technology Readiness Levels Applied to Smart Grid Communications. XII Congresso Internacional sobre Innovation y Desarrollo Technolico, 25 – 27 de marzo, Cuernavaca Morelos, Mexico.
3. J.C. Mankins 2009 Technology Readiness Assessments: A retrospective, Acta Astronautica, Volume 65, Issues 9–10, Pages 1216-1223, ISSN 0094-5765.
4. Dadi Sugiana 2019 Rencana Implementasi Green Fefinery di Pertamina (PPT), Sinergi Energi, Pertamina.
5. Anggirasti 2008 Gliserolisis RBDPO (Refined Bleached Deodorized Palm Oil) dengan Lipase untuk Sintesis MDAG (Mono-Diasilgliserol), Sekolah Pascasarjana Program Studi Ilmu Pangan, IPB.
6. https://www.bpdp.or.id/id/energi/indonesia-menuju-era-industri-bahan-bakar-nabati/

Mosintuwu Institute, Portrait of Transformation of Women Survivor Poso Conflict as Agent of Peace

Sekar Arum Ngarasati, Tri Mardiana
Peace and Conflict Resolution Study Programme of Indonesia Defense University, Citeureup, Bogor, 16810, Indonesia.

E-mail: sekararumngarasati@gmail.com , nanakecild@gmail.com

Abstract. The Poso conflict is a horizontal conflict between youths which later turned into a communal conflict which occurred from 1998 to 2007. Some efforts to resolve the conflict have been made by the government, such as the establishment of the Malino Declaration, however, peace agreement merely created a negative peace. A great number of Poso women became victims, women as a vulnerable group is becoming an object of violence, despite the fact that women had significant roles in building and creating peace during the conflict by protecting each other in spite of the difference in faiths. The severity of the Poso conflict opened many people's eyes to contribute and make their own effort to build sustainable peace. Mosintuwu Institute then used the opportunity to initiate peace building in the land of Poso by improving the women's empowerment. This paper attempts to explore the transformation of the Poso conflict carried out by women who became victims through a case study approach. Data was collected by interviewing the founder of Mosintuwu Institute. This paper will describe the struggle of Poso women in building a positive peace even though they are the victims of the conflict itself and the front guard in peacebuilding.

1. Introduction

Indonesia is a portrait of a pluralistic country in the world. The diversity of religions and beliefs becomes its own color in the life of the nation and state. This difference in fact once incised a conflict that struck deep trauma for who experienced. Poso conflict that happened in Indonesia. Although, religion is not the root of this conflict but later developed into a conflict that dragged the feud between the Muslims and Christians who lived there. Dave Mc Rae, an Australian researcher wrote that the Poso Conflict occurred over four periods (McRae, 2016) [1].

First, it occurred in 1998-2000 which involved young people in Poso villages and then spread into riots between rivalry of established patronage networks. 2nd the period May-June 2000 when the conflict had spread to various regions in Poso and there was widespread murder involving Christian leaders and combatants. As a result of this incident 246 people were killed. Third, the period of conflict broke out between the two groups from 2000-2001. The Poso Muslim group received reinforcements from Mujahideen from outside Poso who showed feelings of revenge and solidarity among fellow Muslims. On the other hand, Christian groups strengthened their militia forces with deadly weapons to reduce attacks by Muslim groups. In this phase, through government mediation, there has been a Malino peace agreement between the two camps. However, from the camp of the Muslim group, because they felt that their ammunition and strength were strong enough and did not believe in the agreement, they continued to carry out acts of violence.

Fourth, the period of the conflict took a long time, namely between 2002 and 2007. In the period of the year there were sporadic attacks, both bombings, shootings, or murders. Local people, especially from Muslim groups was tired of the conflict. In fact, within the internal Mujahideen groups there are conflicts related to whether they really jihad or just taking revenge.

From day by day the authorities continue to look for the mastermind behind the riots. The police have even identified several people as suspects, even though their identity has been kept secret. The riots in Poso have the potential to cause two models of conflict at once, horizontal and vertical. From the perpetrators of the riots and victims who fell, it is very likely that what happened in Poso was horizontal conflict. Those who are involved in this conflict are entirely civilians who have similar interests, but are not based on fair competition spirit. What happened later, conflict spread between them.

In addition to the emergence of horizontal conflicts, rots in Poso also contain a vertical conflict between comunity and goverment. This can be seen from how seriously the government planted a security posse in Poso. For security officers, the right way to restore security in Poso is to coat the existing battalion with the next force. This method certainly has implications for two things whether security is guaranteed or just the opposite ie the anger of the time is mounting.

Dave McRae said that Poso was an arena where history of violent conflict between religions could be witnessed. At the end of his research, McRae was pessimistic about

Poso's future. About the lack of organizational resources needed to change the situation quickly is one of them. The country's response is not too effective, and another reason why the conflict in Poso is still in the future. However, there are positive things that can be felt for the future, namely the feeling of fatigue between the conflicting parties so that they both want peace. This prolonged conflict does not mean that it cannot be resolved and undermines a threat to the Indonesian state. In the course of the four periods of the Poso conflict, a peaceful effort was carried out by the government in the form of the 2001 and 2002 Malino Declarations.

A non-governmental organization concerned with women's issues estimates that around 5,000 women in the Poso region, Central Sulawesi (Central Sulawesi), are victims of sexual crimes [1]. Women who are victims of violence prefer to remain silent and not report. The factors also vary, including the inability of victims and / or their families to gain access to legal services because of their ignorance in reporting to whom, lack of legal fees and living costs while in town and transportation costs. Based on this experience, conflict and sexual violence against women are two things that are difficult to release. Nevertheless, there are unique things about women during the Poso conflict.

Based on the results of a report from the National Commission on Violence Against Women about the social conflict in Poso in 1998, 2005, women were very brave enough to go to the general area and enter areas considered dangerous enemy territory. In addition to maintaining the survival of his family, some Poso women realized that prolonged conflict would permanently destroy them. Many of them realize that this conflict must be stopped. Some Poso women activists bravely entered the conflict area to strengthen and find out about the conflict.

The severity of the Poso conflict opened the eyes of all human beings to contribute to efforts to build sustainable peace. Sustainable peace building is often referred to as conflict transformation. John Paul Lederach in his book entitled "Conflict Transformation" defines conflict transformation as follows:

"Conflict transformation is to envision and respond to the ebb and flow of social conflict as life-giving opportunities for creating constructive change processes that reduce violence, increase justice in direct interaction and social structures, and respond to real-life problems in human relationships."

Based on these writings conflict can be used or provide an opportunity for a thorough and constructive process of change. However, there are several conditions that must be fulfilled, namely: changes that occur must eliminate violence, change brings justice in direct interaction within the community, especially for those in conflict, and conflict can be used to build character that is more tolerant. So that it can be said that through conflict transformation it is expected that a change process can occur where violence can be eliminated and all parties can build on each other. For this reason, the author tries to examine how women victims of the conflict in Poso can fight to become agents of peace in Poso.

2. Research Methods

Qualitative researches have a several methods of data collection are known. According to Sugiyono, data collection techniques consist of: in-depth interviews (intensive / in-depth interviews), observation or field observations, namely using interview techniques or face to face between one or more than two people, and reported several case studies [3].

The assessment carried out by researchers used a case study. Data sources used by researchers include quotations from interviews, field notes, photos, videos, personal documents, notes or memos, and other official documents. The results of the research will be presented in the form of qualitative research which is divided into 3 parts, enormity of the Poso conflict, the study of women and the transformation by victims of conflict into agents of peace, and the Mosintuwu Institute as the Poso Women's Empowerment Institute.

3. Research Results and Discussion

The Enormity of Poso Conflict

Poso is a district that lies in the province of South Sulawesi, with an area of 8,712.25 km2, and the city of Poso as the capital city. Poso was the place for communal conflict between Christians and Muslims between 1998 and 2001. The background of this conflict originated in the past history in the pre-colonial period, namely indigenous groups who were originally from Christianity had settled in living coastal areas with Muslim sea merchants so they converted to Islam [4]. In addition, there are also ethnic groups in Poso who still adhere to animist beliefs and dynamism.

In the early 1900s, Dutch Protestant missionaries came to Poso to invite people who had faith in your animism and dynamism to join Christianity with headquarters in Tentena. In addition, these missionaries taught Protestants who had just joined as part of an ally who had to oppose the kingdoms in the coastal areas that embraced Islam [5]. The Dutch government provided educational, health, agricultural knowledge facilities, and organizations within the local bureaucracy to the people who had just entered Protestantism were called allies. With the attitude of supplying Christians to fight Islam, Christians created a situation of discomfort in the environment, resulting in anti-colonial resistance. The Dutch mission center was in Tentena, Poso which was known as the most successful Christian mission in the Indies [6].

The historical background above has made the Poso community have a grudge in the past, making the conflict protracted for years experiencing conflict between the two religions namely Islam and Christianity. The conflict in Poso itself has a period of time in each conflict because the conflict continued from year to year, namely the conflict in the first episode from 1998 to 1999; second episode, three, and four in 2000; in episode five in 2001 before the Malino Declaration; and episode six after the Malino Declaration.

This Poso conflict reflected religious divisions triggered also by local elites who encouraged the violence. According to a former Deputy Regent, the Poso conflict was not because of religion during a conflict someone burned churches and mosques to extend the conflict. The longer the riots, the more money will be spent, so that someone will benefit from the Poso conflict [7].

Referring to the results of the LIPI study in (Suharno: 2013), the Poso conflict began on December 24, 1998 on Christmas Eve for Christians to coincide with the month of

Ramadan for Muslims. The conflict was motivated by the presence of young people from Christians who visited Muslim youth who were in Darussalam Mosque, Kampung Sayo due to feeling noisy with voices echoed from the mosque on Christmas Eve. On the evening of December 24, 1998 Christians were busy preparing everything to welcome Christmas Day, which was the day the Christians were waiting. Unlike the Muslims who on the night of the month of Ramadan perform sunnah worship namely Tarawih prayer by doing other activities at the mosque at night. One Christian young man hit a young man from Islam as a result of the intensity he experienced to welcome Christmas Eve before dawn. The incident was witnessed by several residents who eventually spread from residents to residents, causing Muslims to attack the homes of residents who are Christians. Hearing this news, Muslims had a combined power of residents from Tokorondo, Parigi, and Ampana while Christians with a combination of residents from Sepe, Silanca, and Tentena carrying their machetes attacked each of the two groups until December 29, 1998. The conflict became more and more uneasy it even spreads beyond the city borders along 3 main lines [8]. This violent conflict was called the beginning of the Poso conflict which was the first episode.

The conflict in Poso lasted about a week, there was a time to ease the conflict between Muslims and Christians. However, the second episode continued not long after the Poso conflict subsided, which was marked by de-escalation of the conflict. This relief of conflict resulted from the election of June 1999 and the Regent's Election in October 1999 so that the leaders took advantage of this situation to seek support from the two conflicting blades so that in their politics they began to form the movement of two camps due to the desire to win elections. People who initially felt that the Poso conflict had ended, but not long after that until April 2000 carried out several attacks carried out by Muslims with Christians.

In the Poso conflict there was a third episode that took place in April 2000, starting from a fight between Muslim youth and Christian youth on April 16, 2000 at the Poso bus terminal, Lombogia village, where the area was predominantly Christian. As a result of this, the Muslims felt threatened by their existence and thus avenged the treatment of Christians by burning the Christian Church. Christians did not receive their houses of worship burned by Muslims, and finally there was a counter-attack on the burning of Muslim mosques. It didn't stop at episode three, the conflict continued in the fourth episode.

The fourth episode began in May 2000 which was marked by more organized attacks. The conflict began under the leadership of Fabianus Tibo from a Christian group known as the Bat Troop or ninja who had killed 3 Muslims in the village of Mo-Engko [9]. Conflict escalation occurred when the attack was carried out in Kampung Situwu Lemba, which is an area of Islam whose population is mostly from migrant origin from Islamic Javanese tribes. The transmigrants owned the Wali Songo Islamic boarding school in the Situwu village area which caused 70 santris to be killed or held captive by Christians [10]. This has caused many residents to flee outside the city because areas with a majority Muslim population must be the main target for attacking weapons for Christians. The conflict in the fourth episode has begun to use their respective weapons, Muslims have begun to lift their weapons because they feel they have been harmed by the victims of Muslims who have fallen in their Islamic boarding schools. The case of escalation of conflict in the fourth episode caused the TNI and POLRI to carry out more stringent safeguards by lowering their members more than before considering the intervention of the Government was important for an effort to resolve conflicts in Poso. Not only in episode four, the Poso conflict continues in the next episode.

The fifth episode was marked by the involvement of President Abdurrahman Wahid in a peaceful meeting known as Rujuk Sintuwu Maroso in August 2000 with a total of 14 traditional leaders from Poso District. This meeting was organized by the provincial government, officials from Poso district and 4 Governors from Sulawesi [11]. The results of Rujuk Sintuwu Marosa did not bring better results, because in April 2001 escalation escalated, causing Muslims to declare requests for death sentences for three Christians, on behalf of Fabianus Tibo as leader of the attack, Marinus Riwu, and Dominggus Dasvila who became a suspect in the Poso conflict in the fourth episode.

In July 2001, members of Laskar Jihad originating from Java emerged and became involved in the Poso conflict due to a sense of solidarity among Muslims who wanted to fight to defend their fellow people. So that Muslims in Poso are getting stronger in conflict because they have the support of Laskar Jihad members from Java. Conflict temporarily dampened the burning at the places of worship of each religious group. Then continued in December 2001 an attack led by Muslim groups in the Batalembah area to Sanginorasaat. The conflict in the fifth episode began to stop the violence from both parties, namely Muslims and Christians. Both parties are willing to stop all types of violence that have been carried out due to the non-violent conflict resolution through the Malino Declaration.

The Malino Declaration is a declaration given by the government to the people in Poso, namely for Muslims and Christians. In the Malino Declaration, a religious approach was used, so that at the conference the reading of the Malino Declaration as a conflict resolution to stop non-violent actions in Poso was carried out before local religious and traditional leaders. In the reading conference the Malino Declaration was attended by 48 people from the government, while 25 people came from Muslims, and 23 people from Christians. The discussion conference on the Malino Declaration took place on December 5, 2001 in Poso and Tentena, December 14, 2001 in Makassar, December 19, 2001 in Malino, and last December 20, 2001 in Malino.

Women and Conflict Transformation in Poso

In times of conflict, women are always the target, both the target of subjugating the community and the target of sexuality. Being targeted by the community is because women are close to children so that women become community representations. Often, sexual violence occurs in community subjugations, such as rape and sexual abuse that harms a woman's body. This shows that women in conflict situations are considered vulnerable groups.

Lian Gogali (2019) revealed that in fact some in Poso conflicts had occurred, women were subjected to community subjugation through their bodies of various violent activities especially when there was military intervention because often in the community to get security links women were usually told to be close to security forces, so that if there is a family attack it can be protected. However, it was troubling for women when there was a relationship with the security forces so that the frequent placement of security forces in a village must have been pregnant or raped, then the security forces were moved to other areas so they were abandoned. As a result, many pregnant women are unwanted, this becomes a disgrace to the family, women are forced to marry anyone, so that the stigma of pregnant women emerges as "ex-other people", so that women feel hardness of heart. Then when they choose not to married, they will be ostracized by the family, this makes women very psychologically disturbed and shows that the consequences of the conflict make women very vulnerable.

The Poso conflict shows that women and children are victims of conflict. This conflict takes a lot of victims both from women, men, and children. The number of women and children victims is very high, because women are considered as a vulnerable group in conflict, besides that women and children are considered to have low individual resilience so that when a conflict is not ready to deal with it, what happens is that many become victims.

In resolving the Poso conflict, there was little involvement of women in the formal peace process, when in fact when there would be an attack and there were some women who saw it, through their speaking skills they gave woro on Poso radio or directly by gathering citizens. In fact, through this method, the people who will be attacked are better prepared to deal with the coming attacks, but this group is not considered as one of the factors that can reduce conflict. At the Malino meeting, there were three women involved in the peace process, two from the Christian community and one from the Muslim community [12]. However, the presence of these three women does not mean bringing women's issues to the meeting table, because they have to support the broader agenda of the male-dominated team. Issues such as trauma healing and sexual violence are not discussed in negotiations, even though this issue is a crucial issue because many women are victims.

During the conflict, women play a role as a liaison between divided Muslims and Christians, even though their men are in conflict but these women provide a place as a form of protection from conflict. Providing a place for the safety of women and children victims is something that is not considered important for women's involvement in conflict, even though in reality this situation is very important for women victims who have low individual resilience. The role of women is also more proactive, because of the support of NGOs that have women as program staff and provide training to women regarding peace efforts, reconciliation and opportunities to earn a living [13].

According to Lian Gogali (2019) in the interview the author did, stated that actually Poso women helped each other not fully as reported in the mass media, for example how Muslim women gave headscarves to Christians so they would not be killed and put into mosques, so that Muslims protect Christians into mosques. Or the Christian gives food to Muslims who die of hunger in the middle of the forest, so they can survive. When Christians ride a truck following a public vehicle that passes from Tentena to Sayo, to inform their Muslim brothers in the next village there will be an attack so that Muslims have been on guard to save themselves from the attack.

Women are considered a vulnerable group, but in fact some women have high individual resilience when they are victims of conflict, because women must be empowered for themselves and their children. This shows that what is on the minds of women is not only themselves, but children are also important to be saved, but the role of women is not addressed in the conflict, there is actually gender inequality in female victims. The need to deal with victims of conflict with a gender perspective, because to reduce the forms of gender discrimination experienced by women. When women and children have become victims of conflict, plus experiencing discrimination in handling conflict, the burden that must be overcome is very heavy because in addition to thinking about the physical and psychological individuals also think about the physical and psychological impacts that occur on their children.

In the Poso conflict, women did not plan to kill each other but how to plan to defend life but never told the mass media. Access to critical education is very much needed to fight for women's rights, besides that it is also a space for women to tell stories so they can build peace. Women are the frontline for building peace in Poso, but always the role of government is appointed as if women have no role. Therefore, education is used as a space to build new communication, as well as communication to come forward to fight for their rights so as to initiate the emergence of women's schools.

Mosintuwu Institute, Overview of Women Empowerment

The Mosintuwu Institute is a community organization in Poso with members of the Poso conflict survivors. The Mosintuwu Institute has a vision of sovereignty over economic, social, cultural and civil political rights. With the mission of strengthening the discourse and the struggle for popular sovereignty over economic, social, cultural and civil political rights. The background of the establishment of the Mosintuwu Institute was because of the concerns of survivors of violent conflict in the name of religion, besides that there were also economic and political interests which ended in the management of natural resources controlled by elites and marginalized poor people [14].

The Mosintuwu Institute comes from various ethnic and religious backgrounds in Poso and Morowali Regencies. Mosintuwu comes from the Pamona language which is one of the tribes in Poso with the meaning of working together. Whereas the Institute itself describes the spirit of Mosintuwu as a critical space for channeling all aspirations of the community, especially victims of the Poso conflict in dealing with various social, economic, political, cultural and so on phenomena in Poso District. In addition, Mosintuwu is a critical study that can develop various forms of programs that benefit the people of Poso and its surroundings.

Such programs are in the fields of education, organizing, media and campaigns, and economic solidarity. In the education program there is a Mosintuwu women's school, which is a women's school which is specifically for grassroots communities which is held for one year, collected from various villages, religions, and tribes. In this women's school, there are nine curriculums studied, namely, religion; tolerance and peace; gender; women and poso culture; sexual health and reproductive rights; women and politics; speaking and reasoning skills; community service rights; economic, social, cultural and civil political rights; and community economy. These women's schools often hold group discussions as a space for storytelling among women about the Poso conflict experienced, while also using lectures, games, field trips, role playing or theater, watching movies, making short films, singing and dancing, and debating used a place to train women to speak in public.

In the field of education, there is a diversity school which is used as a space for dialogue between religious leaders and theological students from across religions to develop pluralism that can make the people of Poso more peaceful and fairer. In addition, there is also a mobile library or called Project Sophia provided by the Mosintuwu Institute with the aim that children and women victims of the Poso Conflict can meet, add insight by reading books, playing, and expressing themselves again after being victims of conflict. Project Sophia was developed into a Sophia library that provides books for children and the public so that they can add insight and knowledge to the Poso community, especially women and children victims of conflict. The Mosintuwu Institute also holds a joint stage as a venue for dialogue and art and cultural activities for Poso youth to preserve the culture in Poso.

The Mosintuwu Institute also provided material on organizing with the aim that women victims of the Poso conflict could fight for justice and peace through village development and regional development to advance Poso. In this case women as village reformers are a space for the meeting of all women in Poso by preparing themselves to uphold justice and peace, active in involvement in decision making. Because in the meantime women are often ignored in the decision-making process, so that the involvement of women is felt capable of strategic policies in village development. After the women were organized, they divided the village business team, children's team, house and women's protection team, media team and village facilitators. The Mosintuwu Institute also provides a circle of discussion and action in the face of economic, social, political and cultural dynamics so as to create schools and pass its members as agents of peace. In the field of organizing there are also houses for women and children protection, as a space for advocating litigation and non-litigation on cases of violence against women and children. In addition, it also serves as a space for anti-violence campaigns against women and children so that in this protection area there is a guarantee of protection for victims of the Poso conflict in order to create justice.

The Mosintuwu Institute also provides teaching in the field of media and campaigns, to ensure that people's sovereignty is gained by the Poso community so that Mosintuwu's programs in the economic, social, cultural and political fields can be known by the entire community. Therefore, the Mosintuwu Institute provides Community Radio and the Poso Women's Newspaper. This Community Radio aims to remind the history of the Poso people who are just and peaceful before conflict so that peace can be restored after the Poso conflict, and connect the community with the programs carried out by Mosintuwu through certain topics and themes. Poso Women's Newspaper as a space for campaigning on Mosintuwu's vision and mission so that it can influence public opinion and spaces of opinion regarding public opinion in the fields of social, economic, political, and cultural.

In the field of economic solidarity, it is a program that develops the economy of the people in the Poso region by wisely utilizing natural resources and paying attention to long-term sustainability. Utilization of these natural resources such as Dodoha Mosintuwu, namely developing workplaces and sharing for the public through bamboo houses which serve as restaurants and places for organizing activities organized by Mosintuwu and by outside parties, thus increasing the economic income of the surrounding community. Furthermore, through Eko Wisata, introducing the beauty of Poso, a diverse culture at the national and international levels so that people outside of Poso know not only on the side of violent conflict but look at the Poso natural resources that they have developed. In addition, there are also Village Enterprises, by utilizing village natural resources and human resources in Poso to develop economic patterns through the creation of employment opportunities by making superior products of Poso that can be introduced to the wider community.

Based on the explanation above regarding the Mosintuwu Institute programs, it is proven that women are empowered, women have the ability to be post-conflict post-conflict survivors. The programs provided by the Mosintuwu Institute to women and children are a manifestation that women must rise from adversity due to the widespread Poso conflict and bring down thousands of victims so that women who are still living and living in Poso must develop creative ideas to build peace. When the attack occurred, women who saw it from a distance immediately provided information so that the attacked village was prepared, through community radio the women provided the information so that all Poso residents who heard it immediately gathered to disperse the attack. This shows that women have a major influence on the failure of the attacks which led to peace in Poso.

The abundant natural resources in the land of Poso are also utilized as well as possible through economic management of the Mosintuwu Institute program, so that the general public who visit Poso not only know Poso as a place of violent conflict, but as a place that has natural beauty that has been cared for by Poso women. So that more and more people who visit Poso because of their curiosity, through the results of Poso women's management, shows that the addition of regional income and can improve the economy of Poso residents which rapidly deteriorated due to the Poso Conflict. Poso women provide mobile library services so that women and children can open insights and entertain from the suffering they experience, because this mobile library is a space for the meeting of Poso people who both want to read.

The Mosintuwu Institute also provides shelter for women and children, where in this house there are women and children who are protected from being exposed to the Poso violent conflict. When the attack occurred, these survivors invited other women and children to take refuge in the house, the purpose being not to get hit by weapons or clashes with Poso residents. Women who try to save themselves and the lives of other women and children do not see any religion, because they have one goal to save other people's laughter regardless of ethnicity and religion. This shows that women are very empowered both during conflict and post-conflict to create peace. Poso women became agents of peace after the Poso conflict through creative skills developed for the sake of creating positive peace.

4. Conclusions

Poso was the place for communal conflict between Christians and Muslims on 1998 and 2001. The conflict was motivated by the presence of young people from Christians who visited Muslim youth who were in Darussalam Mosque, Kampung Sayo as a result of feeling noisy with voices that echoed from the mosque on Christmas Eve. The conflict between the two youths then spread into a religious conflict because each religion felt that they did not accept the youth of their treated religion so that they brought representatives of religious advocates from outside Poso to make the escalation of the conflict escalating.

The Poso conflict has thousands of victims including women and children who are vulnerable, but in contrast to the Poso area, women are very empowered because they are able to create the Mosintuwu Institute initiated by survivors of victims of the Poso conflict. The Mosintuwu Institute was able to arouse the enthusiasm of women who were victims of conflict, so that after the conflict Poso women were not only resigned to staying in refugee camps but were able to create a more peaceful and fair Poso. In times of conflict, women save themselves and children, post-conflict women begin to build peace through social, political, economic and social programs provided by the Mosintuwu Institute. Women are the frontline in building peace in Poso, the Mosintuwu Institute as a space to build new communication, as well as communication for women to be brave to come forward to fight for women's rights.

References

1. McRae, D 2016 *POSO: Sejarah Komprehensif Kekerasan Antaragama Terpanjang di Indonesia Pasca Reformasi* (Tangerang Selatan: Margin Kiri)

2. LPK 2006 *5000 Perempuan di Poso Menjadi Korban Kejahatan Seksual* https://www.merdeka.com/peristiwa/5000-perempuan-di-poso-menjadi-korban-kejahatan-seksual-4cdsis1.html accessed on May 4, 2019

3. Sugiyono 2007 *Statistika Untuk Penelitian* (Bandung: Alfabeta)

4. Trihartono, A and Viartasiwi, N 2015 Engaging the quiet mission: Civil society in breaking the cycle of violence in the post-conflict Poso, Indonesia" *Procedia Environmental Sciences* 28 pp 117

5. Schulte Nordholt, H. G. C. 2001 *A Genealogy of Violence in Indonesia* Lisboa: CEPESA Press pp 33-62

6. *Ibid*

7. Ecip, S 2002 *Rusuh Poso Rujuk Malino* (Jakarta: Cahaya Timur)

8. Suharno, Samsuri, and Iffah N H 2013 Pengembangan Model Resolusi Konflik untuk Masyarakat Multikultural (Studi Implementasi Kebijakan Resolusi Konflik di Sampit, Poso, dan Ambon) *Artikel Jurnal Hibah* pp 5

9. *Ibid* pp 6

10. *Ibid*

11. *Ibid*

12. Lembaga Ilmu Pengetahuan Indonesia Current Asia and the Centre for Humanitarian Dialogue 2011 Pengelolaan Konflik di Indonesia – Sebuah Analisis Konflik di Maluku, Papua dan Poso, *Centre for Humanitarian Dialogue*

13. *Ibid*

14. Mosintuwu Institute http://www.mosintuwu.com/tentang-kami/ accessed on June 6, 2019

Ready-to-Eat Irradiated Food as Food Assistance in Natural Disaster Relief: A Review

Henni Widyastuti[1], Indra Mustika Pratama[1], Deudeu Lasmawati[1]

[1]National Nuclear Energy Agency, Lebak Bulus Raya Street Number 49, South Jakarta 12440, Indonesia.

E-mail: henni.widyastuti@batan.go.id, imp84@batan.go.id, deudeulasmawati@batan.go.id

Abstract. Indonesia is a country located in the Ring of Fire region. In the period 2018 - May 2019, 4,565 natural disasters caused 1.4 million victims affected and displaced. To avoid more casualties, the availability of appropriate logistics need during this disaster response. Technological innovation through the application of food irradiation can support the availability of healthy and nutritious food logistics for disaster victims in the shelter. Food irradiation is giving an amount of radiation exposure that comes from radiation sources to food products. The advantages of irradiated foods include a longer shelf life while keeping nutrients on food products. Irradiation technology applied when natural disasters occurred in Palu and Lombok in 2018. At that time, 1500 packs of food irradiation, the ready-to-eat beef curry, sent. The ease in storing and distributing makes irradiated ready-to-eat processed foods an opportunity to support humanitarian logistics in the future.

1. Introduction

Geographical conditions in the Pacific Ring of Fire cause the Indonesian region has many active volcanoes with high activity in the meeting zone between 3 active plates, the Eurasian plate, the Indo-Australian plate, and the Pacific plate. Therefore, Indonesia has fertile land and biodiversity-rich due to the presence of volcanic material, which naturally functions as a nutrient for plants. However, the advantages of this fertile region make an alert to Indonesia because prone to deadly natural disasters.

Disaster is defined as an adverse event that overwhelms an individual's, an agency's/organization's, or a jurisdiction's capacity to respond [1]. Disasters occurred due to natural or man-made (technology). Natural disasters are disasters caused by events or a series of events induced by nature, including earthquakes, tsunamis, volcanic eruptions, floods, droughts, hurricanes, and landslides. Throughout 2018 to May 2019, there were 4,565 natural disasters occur in Indonesia, caused 1.4 million victims affected and displaced [2].

To avoid the worse social impact of disaster requires good disaster management. Technological innovations can contribute to disaster management more effectively and efficiently at the stage pre-disaster, emergency, and post-disaster response process. At the time of disaster emergency response conditions, logistics is an important factor to support the survival of disaster victims and avoid the increase in casualties due to illness. One of the technological innovations discussed in this paper is the application of nuclear technology in food irradiation to support the availability of healthy and nutritious food logistics for displaced victims.

2. Disaster Management in Indonesia

Natural disaster management in Indonesia is regulated through Laws of the Republic of Indonesia number 24 of 2007 concerning Disaster Management [3]. Those laws stated that disaster management is a series of activities related to disaster observation and analysis as well as prevention, mitigation, preparedness, early warning, emergency handling, disaster rehabilitation, and reconstruction. According to Article 16 of those laws, there are three stages in disaster management, including pre-disaster actions, during an emergency, and post-disaster response. Disaster emergency response is a series of activities carried out immediately to deal with the adverse effects, which include rescue and evacuation of victims, property, the fulfillment of basic needs, protection, management of refugees, rescue, and restoration of infrastructure and facilities.

One aspect of disaster management is logistics management, which referred to humanitarian logistics. Humanitarian logistics is different from commercial logistics where humanitarian logistics have specific challenges ranging from logistical issues to political considerations [4], types of disasters, phases of disaster relief, and types of humanitarian organizations [5]. Furthermore, the accuracy and logistics delivery speed is an important factor during disaster response to avoid the scarcity of basic needs, especially food [6]. For food logistics, the quality of food must remain good until it accepted by consumers. Therefore, the distribution process is an important factor to maintain safety and quality of food products [7].

3. Food Irradiation Technology

Food Irradiation

Irradiation of food is giving an amount of radiation exposure that comes from radiation sources to food products. Radiation used is gamma-ray radiation from radioactive material Co-60 or Cs-137, high-energy electrons from electron beam machines or X-rays produced by X-ray machines [8]. Radiation dose measurements using absorbed dose parameters. Absorbed dose is a number of ionization energies absorbed per unit mass of a medium. In radioactive elements Co-60 or Cs-137, unstable elements will emit gamma radiation at certain energy until the element becomes stable. This radiation then used in food preservation by setting the dose rate according to the intended purpose.

Regulation

An important aspect related to food for consumption is food security and consumer protection. In the world, systematic research on irradiated food started in the 1960s. During the period 1970-1982, an International Project in the Field of Food Irradiation (IFIP) was formed, involving 24 countries supported by the IAEA, FAO, and WHO to study chemical analysis of irradiated food and animal studies. During the project, an FAO / IAEA Joint Joint Organization/ WHO Expert Committee on the Wholesomeness of Irradiated Food (JECFI) was formed to assess the feasibility of irradiated food for consumption. In 1981, JECFI then produced publications related to irradiated food security. The results of this publication later became the standard for irradiated food contained in the Codex Alimentarius "General Standard for Irradiated Foods" published in 1983 while the standard for irradiation facilities in the Codex Alimentarius "Recommended International Code of Practice for the Operation of Radiation Facilities" was published in 1979. In 1983-1984, the International Consultative Group on Food Irradiation (ICGFI), was formed under the auspices of the FAO, IAEA, and WHO aiming to assist the implementation of food irradiation in United Nations (UN) member countries.

Recommendations for the application of irradiation food from the UN then adopted and developed by many member countries, including Indonesia. Application development of food irradiation tailored to the needs and conditions in each country through long research. The results of the research then became a standard for irradiated food, which recorded in Regulation on Irradiated Food and Indonesia National Standard (SNI). Since 2012 until now, 8 SNIs have been developed to regulate irradiated food. SNI 7764.1: 2012 concerning Sterile Beef Curry, SNI 8275: 2016 concerning Ready-to-eat Foods at Medium Dose (2 kGy - 10 kGy), SNI 8276: 2015 concerning Guidelines Irradiated Standard of Processed Meat and Poultry Products in Packaging, SNI 8352: 2017 concerning Ready-to-eat Foods at High Doses (10 kGy <dose ≤ 65 kGy), SNI 8353: 2016 concerning Selection and use of packaging materials for irradiated foods, SNI 8354: 2016 concerning Practical guidelines for fish irradiation and water invertebrates are used as food for control of pathogenic microorganisms and decomposers, SNI 8355: 2016 concerning Irradiation of spices, herbs, and dried vegetable spices to control pathogenic microorganisms and other microorganisms, and SNI 14470: 2014 concerning Requirements for development, validation and routine control of the radiation process using ionizing radiation for food treatment.

The development of SNI refers to Laws of the Republic of Indonesia number 18 of 2012 concerning Food, Government Regulation number 69 of 1999 concerning Food Labels and Ads, Government Regulation number 28 of 2004 concerning Food Safety, Quality and Nutrition, Government Regulation number 33 of 2007 concerning Safety of Ionizing Radiation and Radioactive Sources, Government Regulation number 29 of 2008 concerning Licensing for the Use of Ionizing Radiation and Nuclear Materials, Minister of Agriculture Regulation Number 35/Permentan/OT.140/ 7/2008 concerning Requirements and application of good methods of processing agricultural products (Good Manufacturing Practices), Head of National Agency of Drug and Food Control (BPOM) Regulation Number HK.00.06.1.52.4011 of 2009 concerning Maximum Limit of Microbial Contaminants and Food Chemistry, Head of BPOM Regulation number 26 of 2013 concerning Supervision of Irradiated Foods, Head of BPOM Regulation number 3 of 2018 concerning Irradiated Foods as a replacement of Minister of Health Regulation No. 701 / MENKES / PER / VIII / 2009 concerning Irradiated Foods. The Head of BPOM Regulation concerning Irradiated Foods includes the number of doses needed for food irradiation for certain purposes (Table 1). Moreover, in accordance with regulations regarding food labels and advertisements, irradiation products must use RADURA (Radiation durable) symbol to distinguish between irradiated and non-irradiated food products (see Figure. 1).

All existing regulations are made to ensure food irradiation is in accordance with the expected objectives and to obtain optimal results in the use of irradiation in food products at the pre-irradiation stage, during irradiation procedures, and post-irradiation. The radiation dose used must be within the range of acceptance where the use of the dosage range must minimize the losses incurred in terms of physical quality of foodstuffs and nutritional aspects [9,10,11,12,13,14,15].

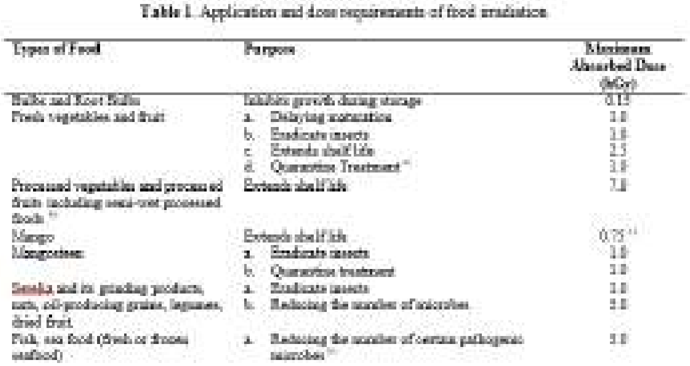
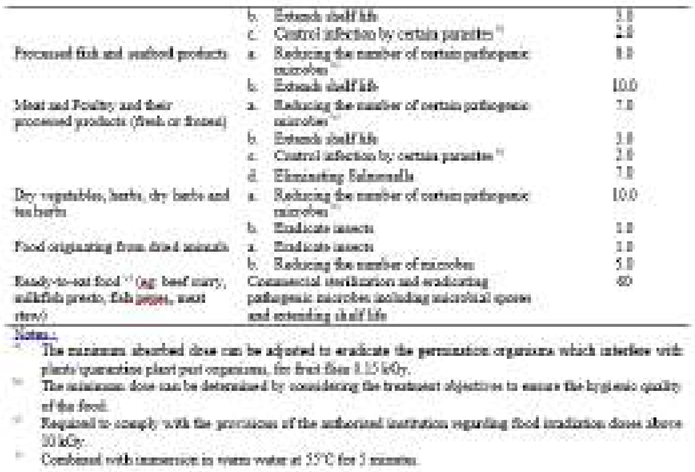


Table 1. Application and dose requirements of food irradiation

Types of Food	Purpose	Maximum Absorbed Dose (kGy)
Bulbs and Root Bulbs	Inhibits growth during storage	0.15
Fresh vegetables and fruit	a. Delaying maturation	1.0
	b. Eradicate insects	1.0
	c. Extends shelf life	2.5
	d. Quarantine Treatment *)	1.0
Processed vegetables and processed fruits including semi-wet processed foods **)	Extends shelf life	7.0
Mango	Extends shelf life	0.75 ****)
Mangosteen	a. Eradicate insects	1.0
	b. Quarantine treatment	1.0
Serealia and its grinding products, nuts, oil-producing grains, legumes, dried fruit	a. Eradicate insects	1.0
	b. Reducing the number of microbes	5.0
Fish, sea food (fresh or frozen seafood)	a. Reducing the number of certain pathogenic microbes **)	5.0
	b. Extends shelf life	3.0
	c. Control infection by certain parasites **)	2.0
Processed fish and seafood products	a. Reducing the number of certain pathogenic microbes **)	8.0
	b. Extends shelf life	10.0
Meat and Poultry and their processed products (fresh or frozen)	a. Reducing the number of certain pathogenic microbes **)	7.0
	b. Extends shelf life	3.0
	c. Control infection by certain parasites **)	2.0
	d. Eliminating Salmonella	7.0
Dry vegetables, herbs, dry herbs and tea herbs	a. Reducing the number of certain pathogenic microbes **)	10.0
	b. Eradicate insects	1.0
Food originating from dried animals	a. Eradicate insects	1.0
	b. Reducing the number of microbes	5.0
Ready-to-eat food ***) (eg. beef curry, milkfish presto, fish pepes, meat stew)	Commercial sterilization and eradicating pathogenic microbes including microbial spores and extending shelf life	60



Notes :

*) The maximum absorbed dose can be adjusted to eradicate the germination organisms which interfere with plants/quarantine plant pest organisms, for fruit than 0.15 kGy.

**) The minimum dose can be determined by considering the treatment objectives to ensure the hygienic quality of the food.

***) Required to comply with the provisions of the authorized institution regarding food irradiation doses above 10 kGy.

****) Combined with immersion in warm water at 55°C for 5 minutes.

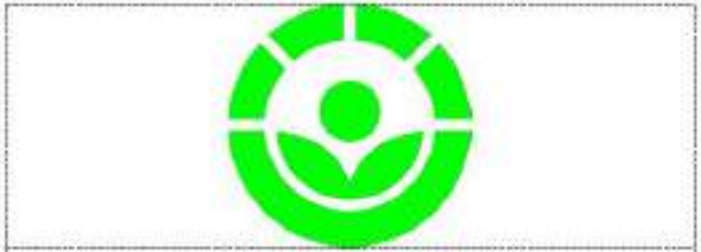


Figure 1. Radura Symbol (Source : TRS 481 IAEA)

Food Irradiation Procedure

Certain doses given to food product will interact with packaging and food substances creates certain effects. Radiation and food substances interactions at certain doses will kill a number of parasites, pathogens, and decay microorganisms which are harmful to food [16] through the mechanism of terminating phosphodiester bonds and hydrogen bonds on the strands of microbial DNA so that growth is inhibited [17].

In pre-irradiation conditions, ready-to-eat processed food must fulfill requirements, including Good Radiation Practices (GRP), Good Manufacturing Products (GMP), and Hazard Analyze Critical Control Points (HACCP). Irradiation cannot improve poor product quality but can optimize the shelf life of products that were previously of good quality. Before irradiation, the product must be stored in a vacuum package to avoid unwanted contamination from the air. Selected packages must fulfill safety standards and approved by applicable regulations, its physical properties are resistant to ionizing radiation, not turn into toxic to food when there is interaction with radiation during food irradiation processes, and can protect the products from damage due to physical, chemical, and biological [18].

Then, the product must be frozen to avoid microbial contamination until the irradiation process begins. When irradiated, the product must be stored in a styrofoam box containing dry ice (solid CO2) and irradiated under these conditions for a certain time. Products storage in styrofoam boxes containing dry ice (solid CO2) aims to avoid free radicals formed during the irradiation process [19]. After irradiation, the product conditioned according to the specific type of product. Then, the product stored at room temperature. It should be noted that this procedure is a general procedure for food irradiation. Product conditioning can vary for each type of product. This procedure follows the standards published by the National Standardization Agency of Indonesia (BSN) in Indonesia National Standard (SNI) [20]. The process is shown in Figure 2. The irradiation facilities used are shown in Figures 3 and 4.

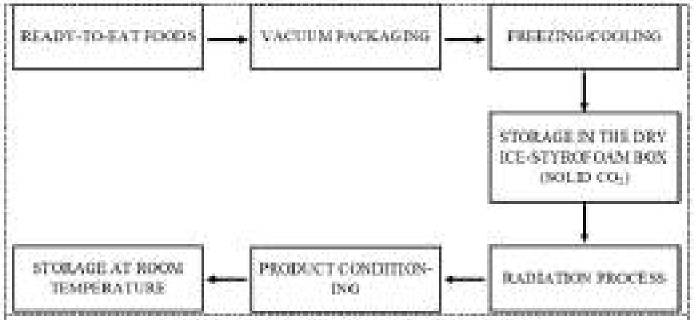


Figure 2. Food Irradiation Procedure (Source : SNI doc)

Figure 3. Multipurpose Rubber Irradiator (IRKA), Center of Isotope and Radiation Application, National Nuclear Energy Agency (BATAN). Source: BATAN document.

Figure 4. Multipurpose Rubber Irradiator Control Room (IRKA), Center of Isotope and Radiation Application, National Nuclear Energy Agency (BATAN). Source: BATAN document.

4. Application of Food Irradiation Technology in Disaster Management

BATAN as research institutions for Nuclear application technology has developed food preservation through irradiation procedures that have some advantages in terms of process safety, not using chemicals, and high quality than other food preservation techniques such as canning, freezing, or processing of chemicals, and can maintain the nutrient content (vitamins) in food [21,22,23]. Some of the irradiated sterile food products that have been developed by BATAN are beef curry [24], meat stews, chicken stews, chicken pepes, and fish pepes [25,26]. This irradiated product lasts up to 18 months with stored at room temperature (Figure 5).

In 2016, as part of a collaborative project with the International Atomic Energy Agency (IAEA) with project code RC 15760/R3, a study was conducted to determine the potential use of gamma-irradiated ethnic ready-to-eat foods to improve the nutritional status of landslide victims in Pemalang, Central Java. The study concluded that irradiated food derived from plants origin with a dose of 8 kGy and animals with dose at 45 kGy, can be given to victims of natural disasters to improve their nutrition in the shelter[27].

In 2018, there were earthquakes in Lombok and Palu, which caused severe damage to residents and infrastructure in the two cities. Access to basic needs limited because the logistics supply infrastructure is damaged while basic needs are indispensable to avoid increasing the number of deaths due to illness or lack of adequate healthy and nutritious food supplies in the shelter [28,29]. Logistical assistance needs to fulfill the basic needs of victims who are displaced or in medical care because of injuries. One of them is food logistics that quality, nutritious, practical, that can be stored for a long time, without requiring special conditions [30]. In emergency response conditions after the earthquake, BATAN sent food assistance in the form ready-to-eat food that has been preserved using irradiation technology to earthquake victims in Lombok in Dopang Tengah Hamlet, Dopang Village, Gunungsari District, West Lombok Regency and earthquake victims in Palu. The provision of food logistics assistance aims to overcome the problem of lack of nutritious food intake, which commonly occurs in post-disaster victims in the shelter.

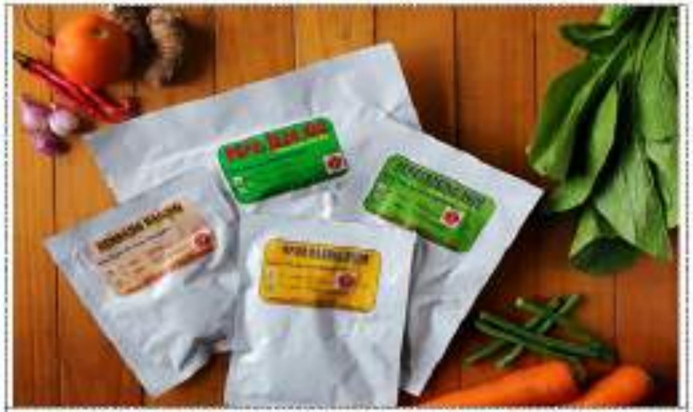


Figure 5. Irradiated food products. (Source: Partnership Dissemination Center doc)

5. Conclusions

Nuclear technology innovation in ready-to-eat food irradiation has gone through a long stage of research and has established a standard in its procedures to ensure that the products are following food safety, toxicology standards, and nutritional adequacy in addition to practicability in distribution and long shelf-life. By paying attention to these advantages, irradiated food technology can contribute to natural disasters management through supporting the logistics of food.

Acknowledgements

The author would like to thank the parties who have helped in this writing activity.

References

1. Haddow G D, Bullock J A and Coppola DP P 2017 International Disaster Management in *Introduction to Emergency Management* (New York : Elsevier).Badan Standarisasi Nasional (BSN) 2012 Pangan Iradiasi – Rendang Daging Sapi Steril. *SNI 7764.1:2012.*
2. http://bnpb.cloud/dibi/beranda accessed on May 15, 2019.
3. Anonym 2007 Law of Republic Indonesia Number 24 of 2007 concerning Disaster Management.
4. Onyango M A, Uwase M dan Health P 2017 Humanitarian Response to Complex Emergencies and Natural Disasters *International Encyclopedia of Public Health Second Edition*, 4, pp 106-116.
5. Gyöngyi K dan Spens K 2009 Identifying challenges in humanitarian logistics *International Journal of Physical Distribution & Logistics Management*, 39(6), pp.506-528.
6. Holguín-veras J, Taniguchi E, Jaller M, Aros-vera F, Ferreira F & Thompson R G

2014 The Tohoku disasters : Chief lessons concerning the post disaster humanitarian logistics response and policy implications *Transportation Research Part A* ,69, 86–104.

7. Marucheck A, Carolina N, dan Hill C 2016 Product Safety and the Food Supply Chain. In *Reference Module in Food Science* pp 1-7.
8. Ehlermann D.A.E 2016 The early history of food irradiation *Radiation Physics and Chemistry*, *129*(1953), 10–12.
9. International Atomic Energy Agency (IAEA) 2015 *Manual of good practice in food irradiation: sanitary, phytosanitary and other applications* (Vienna : IAEA).
10. International Atomic Energy Agency (IAEA) 2002 *Dosimetry for Food Irradiation* (Vienna : IAEA).
11. Vapnek J dan Spreij M 2005 *Perspectives and guidelines on food legislation, with a new model food law FAO Legislative Study* (Italy : FAO).
12. World Health Organization (WHO) 1994 *Safety and nutritional adequacy of irradiated food* (Geneva : WHO).
13. Badan Standarisasi Nasional (BSN) 2016 Proses radiasi - Pangan Siap Saji Dosis Sedang (2 kGy – 10 kGy). *SNI 8275:2016.*
14. Badan Standarisasi Nasional (BSN) 2017 Proses radiasi - Pangan siap saji dosis tinggi (10 kGy < dosis ≤ 65 kGy). *SNI 8352:2017.*
15. Anonym 2018 National Agency of Drug and Food Control of Republic of Indonesia (BPOM) Regulation Number 3 of 2018 concerning Irradiated Foods.
16. Natalia, L., Priadi, A., Irawati, Z 2009 Pengaruh Iradiasi terhadap Daya Hidup Bakteri Kontaminan dalam Makanan, *JITV,* 14(1), pp 58–65.
17. Putri N F A, Wardani A K dan Harsojo 2015 Aplikasi teknologi iradiasi Gamma dan penyimpanan beku sebagai upaya penurunan bakteri patogen pada Seafood : kajian pustaka. *Jurnal Pangan Dan Agroindustri*, *3*(2), pp 345–352.
18. Badan Standarisasi Nasional (BSN) 2016 Pemilihan dan penggunaan bahan kemasan untuk pangan yang diiradiasi. *SNI 8353:2016.*
19. International Atomic Energy Agency (IAEA) 1982 *Training Manual on Food Irradiation Technology and Techniques* (Vienna : IAEA).
20. Badan Standarisasi Nasional (BSN) 2014 Iradiasi pangan - Persyaratan untuk pengembangan, validasi dan

pengendalian rutin proses radiasi menggunakan radiasi pengion untuk perlakuan pangan. *SNI 14470:2014.*

21. Irawati Z, Pertiwi K, Zakaria-Rungkat F 2010 Uji Toksisitas Terhadap Kadar Malondialdehida dan Kapasitas Antioksidan Pada Rendang Steril Iradiasi : In Vitro *Jurnal Aplikasi Isotop dan Radiasi,* 6(1) pp 31-45.
22. Irawati Z dan Sani Y 2012 Feeding studies of radiation sterilization ready to eat foods on sprague dawley rats *Natural Science*, 4(2) pp 116–122.
23. Odueke O B, Farag K. W, Baines R. N dan Chadd S. A 2016 Irradiation Applications in Dairy Products: a Review. *Food and Bioprocess Technology*, *9*(5), pp 751–767.
24. Badan Standarisasi Nasional (BSN) 2012 Pangan Iradiasi – Bagian 1: Rendang Daging Sapi Steril. *SNI 7764.1:2012.*
25. Badan Standarisasi Nasional (BSN) 2015 Panduan Standar Iradiasi Produk Daging dan Unggas Olahan dalam Kemasan. *SNI 8276:2015.*
26. Badan Standarisasi Nasional (BSN) 2016 Pedoman praktik untuk iradiasi ikan dan invertebrate air yang digunakan sebagai pangan untuk kendali mikroorganisme patogen dan pembusuk. *SNI 8354:2016.*
27. Irawati Z, et. al 2016 Potential Use of Gamma-Irradiated Ethnic Ready-to-Eat Foods to Improve the Nutritional Status of Landslide Victims. *Foods,* 5(53) pp 1-10.
28. Gulati D 2015 Food and nutrition in natural and manmade disasters in *Public health nutrition in developing countries*. (India : Woodhead Publishing).
29. Wrabel M dan Caiafa K 2018 Food Emergency Operations After Natural Disasters in *Encyclopedia of Food Security and Sustainability* (New York : Elsevier).
30. Pothiawala S 2015 Food and Shelter Standards in Humanitarian Action *Turkish Journal of Emergency Medicine*, *15*(Suppl 1), pp 34–39.

Global Complexity in Digital Policy Making: The Challenges of "Cyber Attack"

Frega Wenas Inkiriwang[1]

[1]The London School of Economics and Political Science, Houghton St, Holborn, London, WC2A 2AE, United Kingdom

E-mail: F.Wenas-Inkiriwang@lse.ac.uk

Abstract. Within the last decade, the world has been more interconnected through the cyber world, which relies on internet connection. Nonetheless, such fact has also brought challenges which have shocked the world. There has been an increasing number of global cyber threats in the digital age recently. These include cyber attacks, as well as disruptions on government and electoral commission websites. Unfortunately, the attacks targeted critical infrastructures like hospitals which interrupted the service. Additionally, they also hindered the public from accessing government websites which provide information and online service. Furthermore, they also stormed the electoral commission website, which impacted on the democratic process. Thus, this paper attempts to outline the global cyber attacks experienced by both the developed and developing world. Through desk research, the paper identifies the key findings of current security problems in the digital policy-making era. Referring to the actual facts, this paper recommends a move in raising awareness on potential global cyber threat. It also proposes the formulation of legal measures. Lastly, it endorses the development of comprehensive and collaborative efforts in tackling cyber problems.

1. Introduction

Recently, the global *ransomware* virus attack targeted numerous hospitals' database. It hijacked the data which impacted on the service. Unfortunately, not only did it hit a developed country like the United Kingdom but also developing one such as Indonesia. Such a phenomenon may pose a further detrimental impact should it target other vital sectors, like a financial institution or government agency. Additionally, numerous attacks on government websites have also occurred recently. This development has become more complicated with the rapid and massive expansion of mobile devices, which increases the complexity and difficulty of cyber security. [1] In the digital policy-making era, more online services are provided through the government website. Thus, the attacks also potentially slow down public service. Moreover, black campaigns have also been performed through the internet to influence the democratic process in, as witnessed in the last U.S. presidential election. Policy making is part of a democratic process. However, interruption on the process by cyber threats may also result in the interference on digital policy-making. These findings spark attention on the urgency of mitigating the risk of cyber attack in the era of digital policy-making.

2. Globalization and interconnectivity in the digital era

The globalization has connected the world. With the advancement of Information and Communication Technology (ICT), the world has been interconnected. This shares an advantage for everyone since dissemination of information can take place at the real time without any disruption. A person in one country can speak to another person in a different country directly by using even a video call, which is difficult to find in the past. ICT facilitates the quicker exchange of information without regard to physical locations and temporal dimension. [2] Hence, this privilege has grown heavy reliance on the internet and the cyber world, in developed and developing countries. Indonesia is ranked seventh among the top countries which have the most significant number of internet users in 2018. [3] There are 95.2 million people in Indonesia have used the internet (see Figure 1).

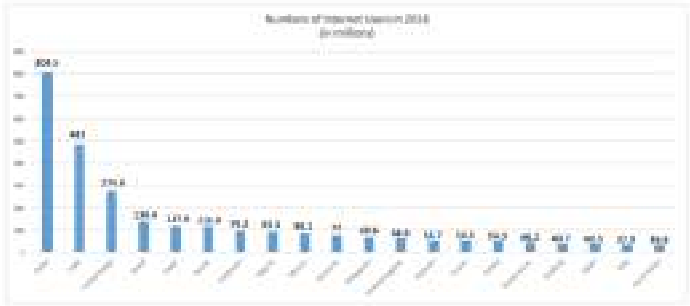


Figure 1. Numbers of Internet Users in 2018 (in millions) [4]

3. Key findings: cyber attacks pose a new threat to policy making in the digital age

Despite its positive contribution in the globalization, the ICT development itself has also created a negative effect. A group of people has misused such an opportunity for achieving their ends. The significant development in the cyber sector is expected to increase significantly as the Internet of Things emerges. [5] Concurrent with the increasing global use of the internet, there has been a substantial escalation of cyber attack cases. Cyber attack is defined as "an illegal attempt to harm someone's computer system or the information on it, using the internet." [6]

The cyber attack has challenged the process of policy making in the digital era. It is clear that policy-making is closely related to public service and democracy. Hence, with the fact of recent global attacks, policy making has been challenged. Despite its status as either a developing or developed one, every country is now vulnerable to cyber attacks. The attacks have initially been used for crimes oriented motive, yet, it has developed to target vital and strategic infrastructures. Moreover, Violent Extremism Organisations (VEOs) also use cyber technologies for achieving their ends, such as for their communication and decision-making process. [7] Sadly, the world is not well prepared to deal with global cyber attacks, even for an advanced country like the United States. [8]

Ruining key infrastructures

Latest global cyber attack hit many countries and institutions in both the developing and developed world. The unexpected attack of *WannaCry ransomware* surprised the world in May 2017. The United Kingdom, a country with advanced ICT development, was also targeted. Cyber attacks hit NHS' GPs and hospitals in the country, which resulted in the obstruction of access to patients' data and diversion of ambulances. These impacted on the public medical service. [9] The attacks may aggravate the condition should they target infrastructures in other vital sectors, like the financial agency or energy infrastructures. The recent research performed by Dutch security engineer, Willem Westerhof, suggests that cyber-attack on solar panels may potentially take out country’s power grids. [10] This makes cyber attacks as the most feared threats in the digital age since they can disrupt public service, which is part of the policy-making process.

Disrupting government websites

Not only, critical infrastructures did they assault, but also government websites. Cyberspace transcends the geographical boundary where a group of ten hackers attacking a site can quickly turn into one thousand, converging on the objective from across the globe. [11] A government website in Washington State, the United States, was hacked in June 2017. The hack planted propaganda message of the Islamic State of Iraq and Syria (ISIS). Several similar attacks also occurred in different states in Ohio, Maryland, and New York. [12] The US, which is known as the most advanced country with its cyber defence capability has been challenged and disrupted.

Cyber attacks also target government websites in developing countries. They are more susceptible to the threats due to their limitations and incapability in tackling the problems. Ironically, hackers use developing countries as their testing ground for launching cyber attacks before deploying them to other targets in developed countries. [13] Surprisingly, attacks on developed countries are performed by hackers from developing countries, like Indonesia. This country contributes to 38 percent of the world's malicious traffic, even surpassing China. [14]

Damaging the political process

Additionally, cyber attacks have also been used to intervene in the political process in other countries. The political process determines the success of the policy-making. With the rising cyber attacks, which also target electoral commission websites, the political process has been affected. Though they may not necessarily alter the result of an election, they may slow down the overall process. According to Associated Press, hack on the Polish Election Commission forced the country to alter to manual count. [15]

Besides, hackings also occurred in different parts of the world. Massive data breach which exposed all Philippines voters took place three years ago. [16] Moreover, the Ghana Electoral Commission website was hacked in December 2016. [17] Pakistan official Election Commission website faced a similar problem in the same period. [18] The U.S. Intelligence Agency even identified the intervention of Russia's cyber attack in influencing the latest Presidential election in the country. [19] Russia was also blamed for 'massive hacking attack' at Macron's campaign team ahead of the French presidential election. [20]

It is evident that the internet has contributed to connecting the world. However, it has also created vulnerabilities to both the developed and developing world. Despite its positive contribution, the internet has facilitated the recent cyber attack incidents which have created negative impacts. Among the first one is the damaging and slowing down of public services due to the targeting of critical infrastructures. Similarly, disruption of government websites also impeded public services. This is possible since, in the digital policy-making, many public services are linked to government websites. Moreover, a further negative effect has also been experienced in the election process. The intercept of the electoral commission website or even interference in the presidential election has damaged the implementation of the political process, which is the key to policy making. Without a proper political process, it will be challenging to perform an ethical policy making in the digital era.

4. Three key recommendations: awareness, legal measures, and collaboration

Having dealt with these critical issues, it is essential for both developed and developing world to develop a reasonable and appropriate strategy. First, awareness is the key to generate more attention to the issues. Second, the presence of legal framework is also critical to set a foundation for coping with the issues. Also, lastly, joint efforts may be required to enhance the process in tackling the issues. Therefore, the paper highlights three recommendation based on these critical viewpoints.

Raise awareness on potential global cyber threat

Despite the massive global cyber attacks which have impacted on critical infrastructures and government websites which provide public service, there is still a lacking of awareness on the peril of cyber threats. This has become one of the critical challenges in dealing with cyber threats. [21] The paper identifies three factors which may have driven the circumstance. First is the limitation of countermeasure capability to deter cyber attacks. Second is the reluctance of "old style" peoples to alter their lifestyle in using ICT. Moreover, lastly is the gap between countries in tackling cyber threats, especially between developing and developed states. Thus, raising the awareness on the danger of global cyber threat is pertinent to the mitigation of risk posed by such threats. One of the effective ways to raise cybersecurity awareness is through the education channel. [22] Hence, education should be highlighted as a top priority in the strategy to raise awareness.

Propose the formulation of legal measures

Legal measures are critical in dealing with global cyber attacks which have impacted on the policy-making in the digital age. However, up to date, there is no binding international law which specifically outlines and regulates the mechanisms in tackling global cyber attacks. Without proper legal measures, it will be difficult to counter any future cyber attacks. UN charter article 51 inherits a right to self-defence; nevertheless, this is insufficient in adopting the right response to prevent or counter cyber attacks. Hence, the proposal of legal measures which deal with such matter is crucial to driving success in coping with the threats mentioned above.

Similarly, in the national context, there has been no specific Law produced by the Government of Indonesia to deal with cyber threats. The country has issued two Presidential Decrees on the establishment of the National Cyber Encryption Agency (BSSN) which supervise any cyber-related issues. Nonetheless, these decrees are not strong enough to facilitate the overarching responsibilities of various stakeholders in the cyber sector.

Cyber is not only a crime issue, but it is a more strategic issue that may threaten national security and defence. Both Law No 2/2002 on Polri and Law No 34/2004 on TNI have not included cyber threat in their articles. Surprisingly, the cyber threat was firstly introduced in an official document in the Law No

11/2008 on Information and Electronic Transaction. [23] Nevertheless, the interpretation of cyber in this Law is limited to crime context. Later, Indonesia produced Law No 17/2011 on Intelligence, which articulates the cyber war. [24] This legal document perceives cyber as a threat to national security. Despite this articulation, the document has not provided a sound legal framework for dealing with cyber threats in the country.

Endorse the adoption of comprehensive and collaborative efforts

Although domestic and international efforts have been established, they have not effectively helped reduce the threats of cyber attacks. A comprehensive strategy should be formulated at national, regional, and international level. This also includes collaborative efforts which incorporate interagency approach, in particular, related stakeholders. There should be a similar scheme developed at both regional and international level. Partnerships which implement comprehensiveness and collaboration are crucial to success.

Since cyber offense and defence capabilities have continued to advance significantly, several issues pertinent to cyber policies and practices will become more critical. This circumstance, hence, requires comprehensive national security and foreign relations strategies. [25] Both strategies should be driven by a mature cyber intelligence capability. [26] Therefore, it is critical for Indonesia to optimize the collaboration between related stakeholders in the cyber sector, which is currently being supervised by BSSN. As a consequence, other stakeholders with sophisticated cyber capabilities like Polri, TNI, BIN, and various other agencies should wholeheartedly support the national effort led by BSSN.

A similar approach should also be developed in the regional and international context. Engagement with other ASEAN and ASEAN Plus countries will help Indonesia refine its efforts in dealing with cyber threats. The recent development has indicated that terrorist groups have employed cyber technologies to seek their objectives. [27] For instance, Boko Haram hacked Nigeria's Secret Service's databases, which stored personnel records in 2012. [28] Indonesia is struggling to cope with terrorism within its national boundary, which is linked to global terrorism network like ISIS. Thus, it is essential to nurture international cooperation with partner countries in the region and those who possess advanced cyber capabilities to help enhance Indonesia's cyber capabilities. This cooperation should incorporate the transfer of knowledge as well as the exchange of information which are fundamental in improving the existing system and mechanism of cyber defence.

Regarding the formulation of the national strategy in dealing with cyber threats, it should also incorporate both active and passive cyber defence principles. Active cyber defence is interpreted as "direct defensive action taken to destroy, nullify, or reduce the effectiveness of cyber threats against friendly forces and assets." [29] Meanwhile, the passive version refers to "all measures, other than active cyber defence taken to minimize the effectiveness of cyber threats against friendly forces and assets." [30] This passive approach is oriented at making cyber assets more resilient to any possible attack. Indonesia should take these two views into account in refining its national cybersecurity and defence strategy.

5. Conclusion

Within the last few months, there has been a rise in global *ransomware* virus attacks. Sadly, they targeted critical infrastructures, including hospitals' database. And not only did it hit a developed country but also developing one. Adverse impacts on critical infrastructures that may also include financial or other public sectors have become one of the most challenging issues.

Additionally, attacks on government websites which are connected to public services have also restricted their use by the public. Such a phenomenon may result in a toxic environment that can affect the policy-making process in the digital era. Policy-making has now become more closely connected to the internet in regards to public services. Thus, with those unbearable cyber attacks, public services have been interrupted. This, of course, is critical since policy-making is to create a better environment for everyone.

Furthermore, interruption or even interception to influence the electoral process is another difficult challenge for policy making in the digital era. Not only black campaigns but also hackings have also been performed through the internet to influence the democratic process in other countries as witnessed in the last U.S. presidential election. Policy making is closely related to the democratic process. Thus, such interruption may hinder the implementation of good digital policy-making. Based on these key findings, this paper endeavours to share plausible recommendations that may help to tackle the challenges. A move in raising awareness on the potential global cyber threat, a formulation of legal measures and also an endorsement of comprehensive and collaborative efforts in tackling the problems, are the three key points offered by this paper. They are necessarily required to set a foundation for facing any future similar or even worse challenges in cyber security and defence.

Acknowledgements

The author wishes to acknowledge support from the Indonesian Endowment Fund for Education (LPDP), Indonesia and the London School of Economics and Political Science (LSE), United Kingdom which has allowed to contribute this paper in the IIDSS 2019.

References

1. Mandt E J 2017 Integrating Cyber-Intelligence Analysis and Active Cyber-Defence Operations,

Journal of Information Warfare Vol. 16 Issue 1 pp 31-48 (p 45)

2. Bezweek S A and Egbu C O 2010 *The impact of information technology to facilitate communication and collaboration in Libyan public organisations*, Conference Paper (University of Salford, Manchester) Accessed 28 May 2019 http://usir.salford.ac.uk/12835/1/530.pdf
3. Statista 2019 *Number of Internet Users Worldwide 2018* Accessed 25 May 2019 https://www.statista.com/statistics/271411/number-of-internet-users-in-selected-countries/
4. Adapted from Statista 2019 *Number of Internet Users Worldwide 2018* Accessed 25 May 2019 https://www.statista.com/statistics/271411/number-of-internet-users-in-selected-countries/
5. Mandt 2017 Integrating Cyber-Intelligence Analysis and Active Cyber-Defence Operations p 45
6. Cambridge Dictionary 2017 *Cyberattack* Accessed 20 May 2019 http://dictionary.cambridge.org/dictionary/english/cyberattack
7. Derrick D C, Ligon G S, Harms M and Mahoney W 2017 Cyber-Sophistication Assessment Methodology for Public-Facing Terrorist Web Sites *Journal of Information Warfare* Vol. 16 Issue 1 pp 13-30 (p 13)
8. Perlroth N 2017 A Cyberattack 'the World Isn't Ready For' *nytimes.com* Accessed 20 May 2019 https://www.nytimes.com/2017/06/22/technology/ransomware-attack-nsa-cyberweapons.html
9. BBC 2017 *NHS cyber-attack: GPs and hospitals hit by ransomware* Accessed 20 May 2019 http://www.bbc.co.uk/news/health-39899646
10. Cimpanu C 2017 *Cyber-Attack on Solar Panels Could Shut Down Power Grids via Domino Effect* Accessed 25 May 2019 https://www.bleepingcomputer.com/news/security/cyber-attack-on-solar-panels-could-shut-down-power-grids-via-domino-effect/
11. Shallcross N J 2017 Social Media and Information Operations in the 21st Century *Journal of Information Warfare* Vol. 16 Issue 1 pp 1-12 (p 3)
12. Andone D, Shortell D and Rehbein M 2017 Hack that plants ISIS message hits another state government website *CNN* Accessed 25 May 2019 http://edition.cnn.com/2017/06/26/politics/websites-hacked-isis/index.html
13. Frenkel S 2017 Hackers Find 'Ideal Testing Ground' for Attacks: Developing Countries *nytimes.com* Accessed 20 May 2019 https://www.nytimes.com/2017/07/02/technology/hackers-find-ideal-testing-ground-for-attacks-developing-countries.html
14. Jakarta Globe 2013 *Hacker's Paradise or Host Nation? Indonesian Official Weigh Cyber Threat* Accessed 25 May 2019 http://jakartaglobe.id/news/hackers-paradise-or-host-nation-indonesian-officials-weigh-cyber-threat/
15. WPR 2014 Polish Election Commission Hacked Accessed 20 May 2019

http://www.worldpoliticsreview.com/articles/14487/polish-election-commission-website-hacked

16. Estopace E 2016 Massive data breach exposes all Philippines voters *telecomasia.net* Accessed 25 May 2019 https://www.telecomasia.net/content/massive-data-breach-exposes-all-philippines-voters
17. Iaccino L 2016 Ghana election: Electoral commission website hacked as vote counting underway *IBT* Accessed 25 May 2019 http://www.ibtimes.co.uk/ghana-election-electoral-commission-website-hacked-vote-counting-underway-1595498
18. Rahul 2016 Pakistan's Official Election Commission Hacked by Malayalee Hackers! *entecity.com* Accessed 28 May 2019 http://entecity.com/news/pak-election-commission-website-hacked-by-malayalee-hackers/
19. Lee K 2017 What does Trump mean when he says 'other countries' hacked the election? *LA Times* Accessed 25 May 2019 http://www.latimes.com/nation/la-na-pol-trump-russia-hacking-20170706-htmlstory.html
20. Henderson B and Graham C 2017 Russia blamed as Macron campaign blasts 'massive hacking attack' ahead of French presidential election *Telegraph* Accessed 20 May 2019 http://www.telegraph.co.uk/news/2017/05/05/macron-campaign-blasts-massive-hacking-attack-ahead-french-presidential/
21. European Economic and Social Committee 2018 Cybersecurity: Ensuring Awareness and Resilience of the Private Sector Across Europe in Face of Mounting Cyber Risks – Study p 17
22. Ibid
23. Government of Indonesia 2008 Law No 11 on Information and Electronic Transaction *Explanatory Addendum*
24. Government of Indonesia 2011 Law No 17 on Intelligence *Explanatory Addendum*
25. Kshetri N 2014 *Cybersecurity and International Relations: The US Engagement with China and Russia*, Conference Paper for FLACSO-ISA (University of Buenos Aires, Argentina) Accessed 28 May 2019 http://web.isanet.org/Web/Conferences/FLACSO-ISA%20BuenosAires%202014/Archive/6f9b6b91-0f33-4956-89fc-f9a9cde89caf.pdf
26. Mandt 2017 Integrating Cyber-Intelligence Analysis and Active Cyber-Defence Operations p 45
27. Derrick D C, Ligon G S, Harms M and Mahoney W 2017 Cyber-Sophistication Assessment Methodology for Public-Facing Terrorist Web Sites p 13
28. Baken D N 2013 Cyber Warfare and Nigeria's Vulnerability *E-International Relations* Accessed 28 May 2019 https://www.e-ir.info/2013/11/03/cyber-warfare-and-nigerias-vulnerability/

29. Denning D E 2014 Framework and Principles for Active Cyber Defence *Computers and Security* Vol. 40 p 109 (pp 108-113)

30. Ibid

Defense Strategy

Defense Management

National Security

Defense Technology

ANALYSIS OF RADIOACTIVE AND NUCLEAR MATERIALS ILLICIT TRAFFICKING THREAT IN INDONESIA TO PREVENT RADIOLOGICAL DISASTER AND MAINTAIN NATIONAL SECURITY

Dewi Apriliani[1*], Reno Alamsyah[2], Deny Widy Anggoro[3] and IDK Kerta Widana[4]

[1,3, 4]Disaster Management Study Programme, Faculty of National Security of the Indonesia Defense University, Kawasan IPSC Sentul, Desa Tangkil, Kecamatan Citeureup,, Bogor 16810, Indonesia
[1,2]Nuclear Energy Regulatory Agency of Indonesia (BAPETEN), Jl. Gajah Mada No. 8, Jakarta 10120, Indonesia
[3,4]Indonesia National Army (TNI), Jl. Cilangkap Raya, Cilangkap, Cipayung, Jakarta Timur 13870, Indonesia

*Corresponding author: dewiapriliani2631@gmail.com

Abstract

A study has been carried out to enhance Indonesian national nuclear security system to response radioactive and nuclear materials illicit trafficking. This study is very important considering that those materials have been widely use in Indonesia and in the world. The descriptive-analytic qualitative method was used to analyse the current strategic environmental conditions in Indonesia. Case studies was used to analyse the material smuggling occurred in the world. As for comparison, the study also review narcotics and psychotropic substances smuggling case in the country. Then, the threat of the materials illicit trafficking in Indonesia were analysed. Finally, lessons learned from the likewise cases in the world were also overviewed. The study concluded that Indonesia has a potential threat to illegal trade activities involving radioactive sources and nuclear materials. Hence, there are some steps need to be taken. Among others, Indonesia needs to establish an integrated national plan for detection and response to nuclear security events. The plan should be identify and assess national threat and be updated regularly. It should enable national responsible entities, or competent authorities, to effectively and efficiently respond any such incident, and to prevent the development of the incident into a radiological disaster.

1. Introduction

The use of radioactive sources and nuclear materials in Indonesia has been widely spread. They are used in the fields of industry, health, as well as in the fields of research and education. Based on data from the Nuclear Energy Regulatory Agency (BAPETEN), as of April 8, 2019, there were 12.039 licenses of radioactive sources and nuclear materials which were distributed throughout the country. Most of these are licenses of radioactive sources used in the health and industrial fields. Instead of their usefulness for the human being, radioactive sources and nuclear materials also have their own hazards and threats if they are not under control. Therefore, they must be controlled since the time they were made, transferred, used, stored, and even when they later on will be stated as nuclear waste. Those control are not only for safety reason, but also for preventing nuclear illegal activities such as smuggling or illicit trafficking and for malevolent activities, including sabotage.

The widespread use of radioactive sources throughout Indonesia, as described above, indicated that the traffic of radioactive sources and nuclear materials are not something happened in an uncommon basis. In addition, the strategic geographical location of Indonesia made it as one of the most important trade routes in the world, which is also to include the trade of radioactive sources and nuclear materials. As an archipelagic country, of the 8.3 million Km^2 area of the Indonesia archipelago there are 6.4 million Km^2 area covered by ocean, with the coastal line of 108 thousand Km Error! Reference source not found.. Therefore, illegal trade activities is a real threat for Indonesia, either for transit or for the target of operation such as in the case of narcotics and psychotropic substances [2]. Figure 1 shows the world main shipping routes which also include the traffic around Indonesia archipelagic area.

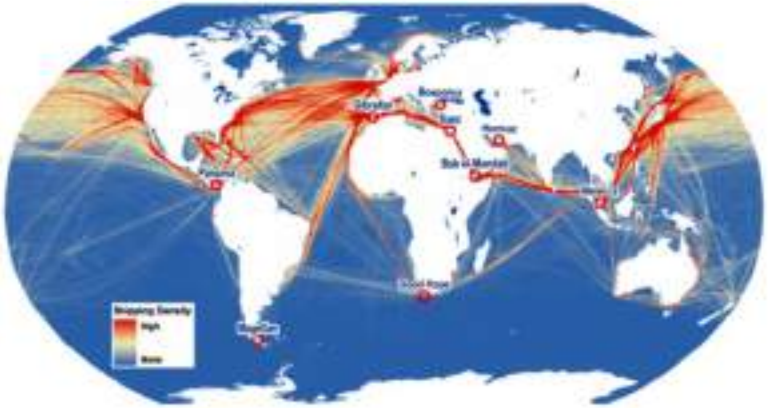


Figure 1. Indonesia position in the world main shipping routes [3]

An illegal traffic of radioactive sources and nuclear materials could not only threaten national security of a state. It also threatens the security in the region as well as in the worldwide. Allison (2004) argues that there are state and non-state actors who are ambitiously want those radioactive sources and nuclear materials for their nuclear weapon program or at least for making dirty bomb **Error! Reference source not found.**. In the perspective of Indonesia, the illicit trafficking of radioactive sources and nuclear materials that make Indonesia only as a crossing or transit area increases radiological disaster threat in other country. Likewise, if Indonesia is the target then it is the real threat for radiological disasters within Indonesia and hamper the sustainability of its national development. Therefore, problems of nuclear smuggling or illicit trafficking has become a global issue, hence it requires synergic cooperation not only at the national level, but also at regional and international level.

Faced with the existence of global nuclear security threat, Indonesia without exception should also develops its ability to prevent, detect and to respond to any illicit trafficking or illegal activities involving radioactive sources and nuclear materials. In 2017, BAPETEN in coordination with other relevant stakeholders such as the Directorate General of Customs and Excise (DJBC) of the Ministry of Finance, National Police (POLRI), Maritime Security Agency (BAKAMLA), Port Managements, Port Health Offices (KKPs) of the Ministry of Health and National Agency for the Border Management (BNPP) have developed guideline for detection and response in the case of radioactive and nuclear illicit trafficking [5]. The document also stated that BAPETEN and other relevant stakeholders have responsibilities to prevent illicit trafficking.

Further development of national level documentation might be needed to ensure effective and efficient prevention and detection measures, and that effective response measure can be carried out in timely manner. Therefore, the objective of this paper are to analyze the radioactive and nuclear illicit trafficking threat in Indonesia and to analyze the detection and response strategies of the existing infrastructure in order to prevent the development of a nuclear security event into a radiological disaster. This study is very important, since the results are expected to contribute to the efforts of maintaining national security.

2. Methodology

The research used a qualitative design approach. The nature of the study was descriptive and analytic. This method was used based on consideration that the research results will provide an overview of the radioactive and nuclear illicit trafficking threat in Indonesia, an overview of the efforts to detect and to respond to radioactive and nuclear illicit trafficking of the existing infrastructure and an overview of the efforts to prevent radiological disasters from radioactive and nuclear illicit trafficking events. The strategy used in the research is a case study. Some cases of radioactive and nuclear materials illicit trafficking occurred in the world were analyzed. As the comparison, it also analyzed cases of narcotics and psychotropic substances smuggling in Indonesia. The discussions and analyses were important to provide a comprehensive analysis of potential threat of the radioactive and nuclear illicit trafficking in Indonesia

Primary data was obtained through experience and observation of the nuclear security practices regulated by BAPETEN, as well as through focused group discussions (FGDs) with participants from relevant institutions. The FGDs held during September-November 2017 were aimed to formulate guidance for detection and respond to radioactive and nuclear illicit trafficking. Records and notes taken during discussions were primary data that support the research. Secondary data used in this study were national documentation such as regulations, international standards, and institutional guidelines and procedures as well as other relevant literatures. Due to the fact that Indonesia utilizes radioactive sources and nuclear materials without any integrated national plan for the security of those sources and materials, therefore this research should be aimed to improve the existing national plan.

3. Results and discussions

The Ministry of Defense (2015) stated that the development of science and technology in the fields of chemistry, biology, radiology or nuclear, and explosives together with the advancement of transportation and information communication equipment has increased the mastery, use and spread of CBRNE science and technology materials and to human welfare interests. In other side, the use and spread of science, technology and hazardous materials have increase the threat to the security and safety of the people. In case of Indonesia, the country is still facing threat from terrorism and radicalism activities. This condition causes Indonesia to have a significant threat from possible CBRNE weapons if they are not handled in accordance with the regulations, guidelines and procedures. The International Atomic Energy Agency (IAEA, 2013) in the IAEA Implementing Guide No. NSS-21 explained that radioactive and nuclear materials if they are not under control of the regulator and the licences/owners could lead to criminal or terrorist acts. Such acts are: criminals or terrorists attempt to acquire and use nuclear materials to build an improvised nuclear device (IND) or to deliberate radioactive materials by the construction of a radiological dispersal device (RDD) or radiation exposure device (RED) [6]. In addition, the openness of Indonesia territorial waters and ports due to limited control capabilities have also increased the potential illicit trafficking threats which may causes Indonesia to become a trade, crossing and spreading area of CBRNE materials illegally [6].

The IAEA (2007) describes that criminal incidents involving illegal radioactive material in a country will always be of concern to the international community. A nuclear security event in a country can provide valuable information for assessing nuclear security threat in other countries. This information helps other countries' governments in identifying potential nuclear security threat that might occur in their country or elsewhere [8]. Furthermore, IAEA (2007) in the Safety Standard Series No. GS-G-2.1 suggests that dangerous radioactive sources that are not properly under controlled and are in public area may cause radiological emergencies that may cause radiation exposure both externally and internally above permitted values for people within immediate vicinity of the sources or materials [9]. It should be noted also that an improper emergency response may lead to the escalation of emergencies into a radiological disaster.

Quoting the UN-ISDR (2009) terminology, disaster is a serious disruption of the functioning of a community or a society that causes widespread losses of human life, material, economic or environment and beyond the capability of the community to overcome by using their own resources [10]. According to Act No. 24 of 2007 on Disaster Management, disasters are events or series of events that threaten and disrupt the lives and livelihoods of people caused by natural factors and or non-natural factors and human factors resulting in human casualties, environmental damage, property losses, and psychological impact [11]**Error! Reference source not found.**. According to Maarif (2012), the risk of disaster is related to three factors, they are: disaster risk hazard, vulnerability and capacity [12]**Error! Reference source not found.**. One of the efforts to reduce the risk of radiological disasters within Indonesia territory is by reducing the vulnerability of the illicit trafficking of radioactive sources or nuclear materials together by increasing the capacity for detection and response capabilities to the illicit trafficking of the source or materials. Such efforts are by having an adequate radiation detection infrastructure, such as installation of radiation portal monitors (RPMs) at the entrance to Indonesia territory (international ports, airports and land borders), and by increasing the capabilities of the frontline officer in order to have capability to prevent an illegal entry of the sources or materials into Indonesian territory. Furthermore, a synergic cooperation and coordination among relevant stakeholders involved in detection and response of radioactive or nuclear illicit trafficking are needed to be maintained and improved in order to be able to formulate an integrated national plan.

Apriliani (2014) stated that as part of the international community, Indonesia has actively participated in various international cooperation efforts in the field of nuclear security, including effort to prevent nuclear illicit trafficking. Through Nuclear Security Summits the Government of Indonesia affirms a joint commitment to enhance regional and multilateral cooperation to ensure global nuclear security. Based on awareness of the serious threat to nuclear security and the need for cooperation to achieve the goal of securing all nuclear materials, nuclear facilities, radioactive sources and radiation facilities throughout the world. The Indonesian Government's commitment is affirmed by installing RPMs at some international ports, endorsing amendments to the Convention on the Physical Protection of Nuclear Material, ratified with Presidential Regulation No. 46 of 2009 and ratifying amendments to the International Convention for the Suppression of Acts of Nuclear Terrorism, ratified with Act No. 10 of 2014 [13].

3.1 Radioactive and nuclear illicit trafficking threat

There are many nuclear illicit trafficking cases that have been known worldwide. Among others are: the case of Prague in 1994, the case of Munich airport in 1994, and the case of Sadakhlo in 2003 [14] [15]. At the case of Prague, on 14 December 1994, Police in

Prague, Czech Republic, arrested three suspects in a car. The Police found 12-inch cylinders inside the car which contained 2.73 kg of 87.7% High Enriched Uranium (Uranium Oxide powder, UO_2). Lesson to be learned is material was transported undetected from its origin to the seized place. At the case of Munich airport, on 10 August 1994, a German Police sting operation intercepted the material on a flight from Moscow to Munich. The Police arrested three suspects and seized 560 grams of Plutonium and Uranium Oxide powder and 210 grams of Lithium-metal in a suitcase. Lesson to be learned is the suitcase containing plutonium were checked in without detection. At the case of Sadakhlo, on 26 June 2003, radiation portal monitor at Sadakhlo border crossing point at Georgian-Armenian border gave off a signal. Radiation was detected on a taxi travelling to Armenia. Inside the car trunk a tin (tea) box was discovered containing two plastic bags with blackish powder. After investigation they revealed that it was 89% High Enriched Uranium in two chemical forms of Uranium Oxide, they are U_3O_8 and UO_2. Lesson to be learned is border detection equipment can play important role in detecting illicit nuclear trafficking.

Toktas and Selimoglu (2012) analyzed that the rate of transnational organized crime has been increased dramatically since 1990s. They made an illustration from the case of nuclear illicit trafficking. Where as in 1994 there were only 46 known incidents of nuclear trafficking worldwide, however based on the IAEA data there were more than 400 cases of nuclear trafficking occurred between January 1993 and December 2001 worldwide [16]. Another research conducted by K. Smith et al (2008) indicated that the number of illegal nuclear trafficking cases was more than 650, involving 82 States in total between 1995 and 2004 [17]. From national security point of view, such cases posed a potential threat to the security of the State concerned as well as for the international peace and security if they were associated with the global nuclear terrorism threat.

Fortunately, there was no radioactive or nuclear illicit trafficking event that has been reported in Indonesia so far. For comparison, currently the real threat in Indonesia is related to illicit trade of narcotics and psychotropic substances. There were 176 cases of narcotics and psychotropic substances smuggling in 2015, 289 cases in 2016, and 346 cases in 2017 [2]. In 2018 from January to March 2018 alone, there were already 80 cases [2]. Throughout the eradication of narcotics and psychotropic substances in Indonesia, those substances are known to enter Indonesian territory by land, sea and air. From the DJBC data, it is known that as many as 80 percent of those substances enter by sea [2]. The mode of smuggling by sea remains a favorite. The vastness of Indonesia's sea area with many islands is a weakness point that is utilized. The syndicates find a way to enter Indonesia through rat ports that lack of supervision.

Furthermore, having learned from the cases in Prague, Munich and Sadakhlo above, if narcotics and psychotropic substances can be smuggled or illegally traded in Indonesia then it may not impossible to smuggle or illegally trade the radioactive sources/ nuclear materials. As discussed in [4, 16, 17] there are strong indications that global terrorism threats are already going to the nuclear terrorism direction. Those conditions will also influences Indonesia's dynamic strategic environment. Thus, vigilance against the threat of nuclear terrorism is always needs to be maintained and improved, especially to prevent the occurrence of radiological disasters within Indonesia territory.

3.2 Efforts to detect and to respond to the illicit trafficking

Lesson learned from case of Sadakhlo at Georgian-Armenian border, as discuss above, is border detection equipment can play important role in detecting illicit nuclear trafficking. Acknowledge the security conditions in Indonesia, the President of Indonesian, Joko Widodo, through a letter from the Secretary Cabinet number B-201/ Seskab/ Polhukam/ 4/2016 gave direction to the Minister of Home Affairs and the Minister of Transportation to take all necessary steps to install RPMs in all international ports and airports, as well as cross-border posts as a form of supervision and prevention of radioactive sources/ nuclear materials entering/ exiting Indonesian territory illegally. Currently there are six ports installed with RPM equipment, they are: Tanjung Priok, Jakarta; Tanjung Perak, Surabaya; Batu Ampar, Batam; Belawan, Medan; Bitung, Manado; and Soekarno-Hatta, Makassar.

However, there are still many other entrances to Indonesia territory that have not been equipped with the detection equipment. Nevertheless, efforts can be done by using the existing infrastructure available. For example, Indonesia has implemented Indonesia national single window (INSW) in order to control export and import of radioactive sources and nuclear materials as well as to prevent radioactive/ nuclear illicit trafficking. Furthermore, by providing frontline officers with the capability to recognize the presence of radioactive sources/ nuclear materials through scene identification, such as radiation symbols accompany goods or goods resemble images of equipment using radioactive sources. Even though the officers are not equipped with a radiation measuring device, they suspicion in the field can be useful information to be subsequently confirmed to the relevant competent body that has adequate radiation detection capabilities. For this effort a good cooperation and coordination as well as communication chain should be developed and maintained regularly through cross drills or trainings between the frontline officers in the fields and the radiation experts.

The research found that even though cross trainings and exercises have been conducted under Indonesia Centre of Excellence of Nuclear Security and Emergency Preparedness (I-CoNSEP) which is coordinated by BAPETEN and involving other relevant stakeholders such as: Ministry of Foreign Affairs, POLRI, Indonesia National Army, Ministry of Defence, National Disaster Management Agency (BNPB), Ministry of Transportation, National Counter Terrorism Agency (BNPT), DJBC, National Nuclear Energy Agency (BATAN), BAKAMLA, Ministry of Health, Meteorology Climatology an Geophysics Agency (BMKG), and State Intelligence Agency (BIN). However, an integrated national plan that covers this issue has not been established yet. Nevertheless, in case of radioactive and nuclear illicit trafficking, detection and response measures for the safety of radiation protection as well as for the security of radioactive sources or nuclear materials must be immediately carried out to prevent criminal acts in other locations that may be unpredictable later.

4. Conclusions

As Indonesia geographically lies in a strategic cross position and opposed by the sea border which is an open area, this condition could make a potential risk due to illegal trade activities. Those activities not only to narcotics and psychotropic substances but also may include to radioactive sources and nuclear materials, since the use of those materials has been widespread not only in the worldwide but also in Indonesia as well.

Understanding this dynamics of the strategic environment condition, Indonesia should have capability for detection and response to smuggling/ illicit trafficking or illegal activities involving radioactive sources and nuclear materials. Thus, by using all necessary steps and efforts, such as: installing RPMs, implementing Indonesia national single window (INSW) on export and import of radioactive sources and nuclear materials, and providing frontline officers with the capability to recognize the presence of those materials.

Furthermore, an integrated national plan for detection and response to any illicit trafficking or any other illegal activities involving radioactive sources and nuclear materials should be the priority to be established. The plan should be identify and assess national threat and be updated regularly to keep up to date. Based on this assessment, the plan should enable national responsible entities, or competent authorities, to effectively and efficiently respond any nuclear security incident, and to prevent the development of the event into a radiological disaster.

Acknowledgements

The Authors wish to thanks the management of the Directorate of Technical Support and Nuclear Emergency Preparedness (DKKN) BAPETEN and the Disaster Management Study Programme, Faculty of National Security of the Indonesia Defense University for their full support and facilitating this research.

References

[1] Sabar Rusydi, Faris. 2018. Indonesian national territory data reference. *Indonesian science magazine*.. Ed. 82 October 2018 pp 6-8.

[2] Hayyu, Pradany. 2018. The main enemy is called drugs. *Media Finance* ISSN 1907-6320. Vol XIII/ No.127/ April 2018 pp 14-17.

[3] UN. 2014. Maritime Piracy: Part 1 an overview of trends, costs and trade-related implications. *United Nations Conference on Trade and Development* (New York and Genewa: UN) pp 25.

[4] Allison, Graham. 2005. *Nuclear Terrorism: The Ultimate Preventable Catastrophe* (New York: Owl Books) pp 61-86.

[5] Nuclear Energy Regulatory Agency of Indonesia. 2017. *Guideline for the implementation of detection efforts and responses to radioactive sources/ Nuclear materials illicit trafficking* (Jakarta: Nuclear Energy Regulatory Agency).

https://www.bapeten.go.id/site/iconsep-index?tab=others

[6] IAEA. 2013. *Nuclear Security Series No. 21:* Nuclear Security Systems and Measures for the Detection of Nuclear and Other Radioactive Material out of Regulatory Control (Vienna: IAEA)

[7] Ministry of Defense. 2015. *National Defense Strategy* (Jakarta: Ministry of Defense) page. 26-27.

[8] IAEA. 2007. *Nuclear Securities Series No.6:* Combating Illicit Trafficking in Nuclear and Other Radioactive Materials (Vienna: IAEA).

[9] IAEA. 2007. *Safety Standard Series No. GS-G-2.1*: Arrangements for Preparedness for a Nuclear or Radiological Emergency (Vienna: IAEA).

[10] UN. 2009. *UNISDR Terminology on Disaster Risk Reduction*, (Geneva: UNISDR) page. 9.

[11] The Republic of Indonesia. Law No. 24 Year 2007 on Disaster Management (Jakarta: National Disaster Management Agency)

[12] Maarif, Syamsul. 2012. *Thoughts and Ideas for Disaster Management in Indonesia* (Jakarta: National Disaster Management Agency)

[13] Apriliani, Dewi. 2014. The Role of Nuclear Forensics in Investigating Nuclear Security Events in Indonesia. *Proceedings of nuclear safety seminars* ISSN: 1412-3258 pp 86-91.

[14] Ewell, Emily S. 1998. NIS Nuclear Smuggling Since 1995: A Lull in Significant Cases. *The Non-proliferation Review/Spring-Summer 1998* pp 119-125.

[15] Whitney, Craig R. 1995. Smuggling of Radioactive Material Said to Double in a Year. *The New York Times*.

https://www.nytimes.com/1995/02/18/world/smuggling-of-radioactive-material-said-to-double-in-a-year.html.

[16] Sule Toktas & Hande Selimoglu. 2012. Smuggling and Trafficking in Turkey: An Analysis of EU–Turkey Cooperation in Combating Transnational Organized Crime. *Journal of Balkan and Near Eastern Studies*, 14:1, 135-150.

[17] David K. Smith, Michael J. Kristo, Sidney Niemeyer and Gordon B. Dudder. 2008. Documentation of a model action plan to deter illicit nuclear trafficking. *Journal of Radioanalytical and Nuclear Chemistry*, 276 (2), p. 416.

MATERIAL TRANSFER AGREEMENT AND HEALTH SECURITY RISK

Masdalina Pane[1,2,3], Soviaan Aritonang[4], Denny DAR[4], Herlina[4], Fiona Kong[5]

[1]NIHRD, Ministry of Health Rep of Indonesia, Jakarta, Indonesia
[2]Indonesia Epidemiological Association (PAEI), Jakarta, Indonesia
[3]University of Sari Mutiara Indonesia, Medan, Indonesia
[4]Indonesia Defence University, Bogor, Indonesia
[5]City University, Hongkong

*Corresponding author: masdalina.pane@litbang.depkes.go.id, masdalina.pane@gmail.com

Abstract

Indonesia has a mega-diverse ecological system which is vulnerable to exploitation by foreign parties. This is partly due to the limited protection and management of its resources. Possible exploitation includes past attempts to patent the natural resources at the expense of local stakeholders; as well as shipping biological samples which may pose a biological threat and therefore a national security risk. Some of these samples, such as pathogens, may be even used for dubious usage as biological weapons. The aim of the study is to analyse the issues associated with these potential threats and its impact on national defence of Indonesia as an independent state. Individual and or institutional Material Transfer Agreements (MTAs) proposal were analysed qualitatively to identify regulatory issues while normative-empirical law (law applied research) were held to evaluate obstacles and issues linked with the current governance on MTAs. The results have identified the challenges in the bureaucratic processes, national oversight and management limitations of MTAs. Minimal cooperation between the government departments and agencies also contribute to the threat to Indonesia's national interest and its defences. Stronger measures and a unified national or centralised control of biological samples are recommended to protect Indonesia's national interest.

1. Introduction

Indonesia is the sixth fastest emerging markets in the region with a large population of an estimated 245 million people. Indonesia also leads after Brazil as the most biologically diverse nation (mega-diverse) in the world where its rainforests contain 10 percent of the world's flowering plant species; 12 percent of the world's mammal species; 16 percent of all reptile and amphibian species, and 17 percent of the world's bird species. [1, 2] Its diverse environment, rapid economic development and vast ecological resources places it at risk of emerging infectious diseases (EIDs) in Southeast Asia which has been long considered a hotspot.[3] This includes the presence of a vast variety of novel zoonotic pathogens in Indonesia where its sheer geographical size and over 6000 islands with inhabitants, stretching over several thousand kilometres, hamper effective disease control and surveillance. The large domestic commercial livestock industry to small scale broilers and household farms with poor biosecurity practices may further increase the risk for zoonoses of public health significance, such as pathogenic avian influenza.[4] Anthrax is another zoonosis of concern and it is endemic in certain areas of Indonesia where farmers are at particular risk.[5]

In a mega-diverse nation, there are opportunities for research purposes due to the vast presence of biological and genetic samples. However, it requires specialised researchers, laboratory capacities and investment. Like lower-middle-income countries (LMICs), Indonesia has limited physical, research and manpower capacities to carry out essential research on novel EID pathogens or carry out research on novel therapeutic drugs, which may be derived from their own biodiverse environment. That creates a dependency on other wealthier nations to fund on-going research in Indonesia.

1.1 Limited Capacities

While Indonesia has a strong manufacturing capacity and regulatory frameworks pertaining to influenza, it has limited capacities in terms of EIDs.[6] This includes laboratory capacities as well as access to the latest technologies. As an LMIC, it has competing social, economic and health priorities which hamper further investment into biological research, [7] which is often costly due to the type of specialist equipment, maintenance and manpower skills required.

These capacities are also not limited to EIDs, re-emerging and endemic diseases. The limited laboratory networks, biological research and research facilities may also affect agricultural research where the lack of technological or skills may also hamper their capacity to analyse biological samples from plants [8] and animals, not just humans. To overcome these capacity issues, there is little choice but to utilise material transfer agreements (MTAs) to transfer genetic or biological samples between the local Indonesian laboratories and the foreign laboratories globally.

Furthermore, there is a phenomenon known as 'helicopter research' where foreign researchers from wealthier countries, enter into Indonesia, collect samples, export them under MTA loopholes, with minimal consideration of the local regulations and thus, needs depriving the local community of access, benefits and opportunities.[9, 10]

1.2 Material Transfer Agreements (MTAs)

Indonesia does have certain sharing mechanisms of biological and genetic samples which mostly takes place under MTAs. Specific regulations related to the overseas transfer of material for research and health care are set forth in Permenkes No. 657/Menkes/Per/VIII/2009 on Delivery and Use of Clinical Specimens and Biological Materials and Freight Information.[4] For the approval of a Material Transfer Agreement (MTA), the requirement must involve an official research cooperation agreement through Memorandum of Understanding (MoU) and Memorandum of Agreement (MoA), proposal and research protocol. A MoA is a legally binding document where both parties have reached a consensus. If in any time, an agreement is terminated by default due to contractual failure or criminal activities, these agreements have protective legal mechanisms and technicalities, such as legal compensation, sanctions, legal jurisdiction and domicile. The MoU equalises the legal standing of both parties and also provides protection of state interests related to the genetic material especially if two sovereign governments are involved. A MoA is a legal act of one party to declare the intention of providing their samples or resources to another party. An MOU has weak legal standing in Indonesia and often treated like a preliminary agreement which regulates and provide the possibility of a feasibility study prior to an actual contract. There are laws such as Law 37 of 1999 Foreign Relationships [11] and Law 32 of 2004 [12]which govern regional and international agreements in relation to research. These laws may have loopholes when and if the foreign entities are not monitored or supervised, especially by non-government and private organizations, as well as individuals. [12] An MTA is different and does have a legally binding contract with the institutions to set the terms for the obtaining and usage of their materials and/or associated data to another party.

The challenges which lie within the current MTA processes are the rights of the local communities/individual owner which may be infringed by intellectual property rights in any discovery. Furthermore, some communities may hold the cultural interpretation of ownerships where the item of interest is not seen as property, which increases their risk of exploitation at the hands of modern researchers with the knowledge of the legal frameworks surrounding intellectual ownership and patents. As an example, some communities do not see previous 'traditional' or 'old' knowledge of the biological specimen's benefits as 'intellectual property but something which already existed for decades or even centuries passed down generation to the next but someone, external to the community may declare the same knowledge as a 'new discovery' and exploit it commercially at the disadvantage of the local community. [13] These issues will be briefly discussed in the next section on biopiracy.

1.3 *Biopiracy*

Biopiracy is defined as "the unethical or unlawful appropriation or commercial exploitation of biological materials (such as medicinal plant extracts) that are native to a particular country or territory without providing fair financial compensation to the people or government of that country or territory". (*Merriam Webster, 2016*) [14]. Indonesia is no stranger to such occurrences. In the example of tempe, a traditional food for centuries, has five related patents in Japan and 15 patents in the United States which threatened a highly lucrative domestic industry worth an estimated USD 3 billion .[15] The patent period lasts for 20 years with limitation. In the 1990s, Shishedo, a Japanese cosmetic company, attempted to patent the extracted compounds and even the traditional herbs found only in Indonesia – a move which could affect the local communities who depend on the herbs as traditional medicine. [10, 16]

For pathogenic samples, Indonesia does share biological specimens or even genetic material with the World Health Organisation (WHO), especially those of public health significance under its obligations as a signatory of the International Health Regulations (IHR) (2005). However those did result in another incident which highlighted the issues of viral sharing as a form of biopiracy.[10, 17] Under the now defunct but non-legally binding obligation of the former WHO's Global Influenza Surveillance and Response Systems (GISRS) and the current WHO Pandemic Influenza Preparedness Framework for the Sharing of Influenza Viruses and Access to Vaccines and other Benefits ('WHO Framework'), pharmaceutical and biotechnological industries from high income countries may obtain access to the shared information to research and develop novel treatments, usually geared towards commercial purposes. Under the GISRS defunct system, any diagnostic, pharmaceutical (i.e. vaccine) and treatment (i.e. drugs) products, derived from such provided information, are patented and offered back to the country of origin at often unaffordable prices in this long term entrenched system. [18]

Indonesia had initially shared a viral sample with the WHO GISRS which resulted in a pharmaceutical company patenting the virus modified from its sample and allegedly offered them the vaccine at a price.[17] This resulted in Indonesia's refusal to share viral samples with WHO's Global Influenza Surveillance and Response Systems (GISRS) in 2007.[19, 20] As a result of the changes made to prevent such an incident from occurring again, the conditions were to ensure fair, transparent and equitable access to benefits which included intellectual property rights and as a result, most research institutes and commercial firms have to file for a legally binding material transfer agreement (MTA) with WHO. [20]

Even after the incident with the WHO was resolved with the agreement on equitable access, the MTAs still face the risk of biopiracy because of possible loopholes which exist within the governance and legal structure underpinning the MTAs. Following the incidents, Indonesia had gone on to ratify the Nagoya Protocol in 2013 to prevent intellectual theft and illegal usage of its biological diversity. There is the challenge of ensuring to human pathogens material for the purposes of public health preparedness and emergency response under PHEIC (Public Health Emergency for International Concern) within the reference of the Nagoya Protocol to the IHR.[8] Indonesia still holds a duty of care and due diligence to its citizens and national interests, as priority over that of the international community. This will include evaluating the utility of the MTAs; assessing possible threats and their capacities to overcome such threats in terms of the following principles of equality, reciprocity and sovereignty.

1.4 Aim and Purpose of the Study

The aim of this study is is to analyse the issues associated with these potential threats and its impact on national defence of Indonesia as a sovereign state. For the purposes of the paper, we will concentrate on MTAs reviewed by the National Institute of Health Research and Development (NIHRD, the Ministry of Health, Republic of Indonesia). The NIHRD is responsible for evaluating MTAs related to human and healthcare specimens.

2. Methods

The qualitative research methods of normative-empirical law *(applied legal research)* were undertaken to study the gaps between legal provisions within domestic, regional and international (particularly the Nagoya Protocol) law. The relevant domestic legislation was mapped to the regional and international legal provisions to identify any potential loopholes which may present a threat to Indonesia's national interests and security. Data collection and collation consisted of MTA applications from 2009 to mid-July 2016, a detailed document analysis of the MTAs were performed. Variables from the MTAs, such as (but not limited to) date of agreement, foreign/domestic parties, background (e.g. commercial, intergovernmental agencies), countries where the MTA was transferred to, research institutes of origin (e.g. universities, non-government organizations) and types of materials, and domestic Indonesian laws quoted in MoU's and MoA's were extracted from the documents for examination. To supplement the above information, interviews with relevant stakeholders at senior levels were undertaken to evaluate their opinions towards the following factors in research: equality, reciprocity, securitization of hybrid partnerships (i.e. both domestic and international public-private partnerships) and national interest (with a focus on health security). These stakeholders include senior levels of decision makers in research and government institutions (i.e. the Ministry of Research and Technology and the Ministry of Foreign Affairs) involved in overseas collaboration. The data was then triangulated to identify the challenges and potential threats on Indonesia's national security.

3. Result

For the duration of 2009 to July 2016, there were a total of 125 applications submitted to the NIHRD for evaluation. Out of the 125, 114 (91.2%) were evaluated by the committees. The non-evaluated applications were excluded from the study. Of the 114 applications reviewed, 71 (62.3%) were approved for research purposes. The remaining applications were rejected on the basis where the committee have assessed them to be of risk. These risks include accessing and exploiting Indonesia's resources with the potential of no equitable access for the local community with no or minimal benefit to the local researchers, consideration of local regulatory frameworks and/or posing a threat to Indonesia as a sovereign nation.

Table 1: Agreement Review by MTA's Committee in NIHRD, MoH Rep. of Indonesia, 2009– July 2016

Year	Number of Application	Accepted	Rejected	No Need Review	Not Follow up
2009	16	3 (18.75%)	12		1
2010	21	11 (52.4%)	5		
2011	13	8 (61.5%)	2		3
2012	18	16 (88.9%)	1		
2013	16	13 (81.25%)	1	1	
2014	17	10 (58.8%)	1		
2015	6	5 (83.3%)	1		
2016	7	5 (71.4%)	1		

Total	114	71	24	1	4

4. Discussion

Our research have highlighted the key issues which Indonesia face in relation to the gaps in the MTA which facilitate foreign sovereign interests to obtain potentially viable samples of economic and/or military usage. The four key issues of national security interest are the potential biological threat; the threat to local capacity building; increased dependency on foreign entities; and biopiracy. Potential biological threats involve the exportation and weaponisation of pathogens which originated from Indonesia. These pathogens can affect humans and/or animals, and even agricultural crops. Furthermore, the lack thereof local capacity building with the increased dependency on foreign entities means that the current skilled workforce will not have the opportunities to advance their skills, and the laboratory capacities will stagnate. While this can be easily overcome from sending out skilled Indonesian researchers overseas, there were anecdotal cases where they were encouraged by foreign entities to smuggle samples out of Indonesia.

Additionally, threat to the national security and interests of Indonesia is a real concern. Unfortunately, there is no attention to this matter in MTA's review. There's no information and tick form in MTA's form, it never discusses in all review board. The transfer of genetic materials tends to fall under the context of non-military utilisation despite its potential of creating a bioweapon. Assessment of non-military utilisation tends to fall within the domain of other Ministries (e.g. agriculture, health) and the research institutions. Yet with a national security threat arising from the manipulation and use of genetic materials, there is no clear standard operating protocol or policy within each organisation or an established command hierarchy to handle a possible threat. The development and use of biological warfare are not a new idea. There is evidence that biological warfare existed since the prehistoric era, including the use of insects to the pollution of strategic waterways with infected corpses. [23] Records to trace back the manipulation and use of genetic materials may be destroyed if there is certain sensitivity involved. Indonesia is no stranger to similar experiences. After the Japanese occupation in World War 2 (WWII), the Japanese destroyed all the records of vaccine manipulation and cruel and sadistic experiments in the Pasteur Institute in Bandung.[24] There was no trace of what had been done in the Bandung facility and Dr Mochtar, an innocent man, was executed by the Japanese as a scapegoat for a botched vaccine which most suspected had been manipulated by the Japanese themselves.[24] Indonesia cannot afford to let such incidents happen again at the expense of its people. contrary to Indonesia's interests. Assessment of various risks to Indonesia arising from the use of genetic materials should be performed rather than separately on an individual basis.

Threat to the national security and interests of Indonesia is a real concern. The core operation of military defence lies solely with the Ministry of Defence in Indonesia. However, the transfer of genetic materials tends to fall under the context of non-military utilisation despite its potential of creating a bioweapon. Assessment of non-military utilisation tends to fall within the domain of other Ministries (e.g. agriculture, health) and the research institutions. Yet with a national security threat arising from the manipulation and use of genetic materials, there is no clear standard operating protocol or policy within each organisation or an established command hierarchy to handle a possible threat. The development and use of biological warfare are not a new idea.

Potential threat posed to national security of Indonesia. Certain genetic material from Indonesia may be potentially developed in the wrong hands and used against Indonesia. Additionally, there is a lack of capacity to diagnose novel emerging pathogens. Exportation of genetic materials, especially human pathogens, for research by foreign entities which may result in a patent detrimental to Indonesia's national interest. Such detriments include unaffordable preventative and curative treatments to the Indonesian population. Indonesia need a long-term commitment to building manpower capabilities and skills, morale, quality control and biosafety. We recommend for decentralisation of authorities regarding local autonomy as well as separation of research institutes under different auspices and health security review for all MTA's application to the committee.

Acknowledgements

We would like to acknowledge to Dean of Defence Strategy Study Program – Indonesia Defense University (IDU), Director of Humanity and Health Management Research Centre - National Institute of Health Research and Development - Ministry of Health Rep of Indonesia, Head of Material Transfer Agreement Board, Secretariat MTA.

References

1. Keong, C.Y., *Sustainable resource management and ecological conservation of mega-biodiversity: the Southeast Asian Big-3 reality*. International Journal of Environmental Science and Development, 2015. **6**(11): p. 876.
2. Ministry of Environment (The Republic Of Indonesia) *The 5th National Report: The Convention on Biological Diversity*, B.C. Unit, Editor. 2014, Ministry of Environment (The Republic Of Indonesia) ,: Jakarta.

3. Coker, R.J., et al., *Emerging infectious diseases in southeast Asia: regional challenges to control*. The Lancet, 2011. **377**(9765): p. 599-609.
4. Wibawa, H., et al., *Exploring contacts facilitating transmission of influenza A (H5N1) virus between poultry farms in West Java, Indonesia: A major role for backyard farms?* Preventive veterinary medicine, 2018. **156**: p. 8-15.
5. Martindah, E., *Risk Factors, Attitude and Knowledge of Farmers in Controlling Anthrax*. WARTAZOA. Indonesian Bulletin of Animal and Veterinary Sciences, 2018. **27**(3): p. 135-144.
6. Organization, W.H., *Regional Workshop on Implementation of the Pandemic Influenza Preparedness Framework in the South-East Asia Region, Report of the Meeting, Jakarta, Indonesia, 27-29 April 2015*. 2016, World Health Organization.
7. Normile, D., *Indonesia taps village wisdom to fight bird flu*. Science, 2007. **315**(5808): p. 30-33.
8. Secretariat of the Convention on Biological Diversity, *Nagoya Protocol on Access to Genetic Resources and Fair and Equitable Sharing of the Benefits Arising Out of Their Utilization to the Convention on Biological Diversity. Secretariat of the Convention on Biological Diversity, Montreal, Canada* T.C.o.B. Diversity, Editor. 2011.
9. Rochmyaningsih, D., *Study of 'sea nomads' under fire in Indonesia*. 2018, American Association for the Advancement of Science.
10. Mardiastuti, A., *Implementation of Access and Benefit Sharing in Indonesia: Review and Case Studies*. Jurnal Manajemen Hutan Tropika, 2019. **25**(1): p. 35-43.
11. *Law No. 37 of 1999 on Foreign Relations (UUNo 37 tahun 1999 tentang Hubungan Luar Negeri).*
12. *Law No. 32 of 2004 on Regional Government (32 tahun 2004 tentang Pemerintah Daerah).*
13. Bubela, T., J. Guebert, and A. Mishra, *Use and Misuse of Material Transfer Agreements: Lessons in Proportionality from Research, Repositories, and Litigation*. PLoS Biology, 2015. **13**(2): p. e1002060.
14. Dictionary, M.-W., *New York: Merriam-Webster*. Merriam-Webster. com. Web, 2016. **14**.
15. Trisno, S. and T.A. Susetyo-Salim, *The Protection and Preservation of Indigenous Knowledge on Tempe*. The Social Sciences, 2017. **12**(2): p. 284-287.
16. Yulianti, S.W. and M.N. Imanullah, *THE MODEL OF BIOPIRACY DISPUTE SETTLEMENT IN THE FRAMEWORK OF PROTECTING TRADITIONAL KNOWLEDGE*. Jurnal Dinamika Hukum, 2016. **16**(1).
17. Smallman, S., *Biopiracy and vaccines: Indonesia and the World Health Organization's new pandemic influenza*

plan. journal of international & global studies, 2013.

18. Sedyaningsih, E.R., et al., *Towards mutual trust, transparency and equity in virus sharing mechanism: the avian influenza case of Indonesia*. Annals Academy of Medicine Singapore, 2008. **37**(6): p. 482.

19. Kwan, M., *The World Health Organization Framework for Virus Sharing: Law, Recent Challenges and its Compliance*. Public Health Law, Forthcoming, 2018.

20. Halabi, S., *Viral Sovereignty, Intellectual Property, and the Changing Global System for Sharing Pathogens for Infectious Disease Research*. Annals Health L., 2019. **28**: p. 101.

21. Holzhacker, R.L., R.P.M. Wittek, and J. Woltjer, *Decentralization and Governance in Indonesia*. Vol. 2. 2015: Springer.

22. Burgos, S. and S. Ear, *Emerging Infectious Diseases and Public Health Policy: Insights from Cambodia, Hong Kong and Indonesia*. Transboundary & Emerging Diseases, 2015. **62**(1): p. 96-101.

23. Carus, W.S., *The history of biological weapons use: what we know and what we don't*. Health security, 2015. **13**(4): p. 219-255.

24. Baird, J.K., *War Crimes in Japan-Occupied Indonesia: Unraveling the Persecution of Achmad Mochtar*. The Asia-Pacific Journal| Japan Focus Volume, 2016. **14**(1).

COUNTERING VIOLENT EXTREMISM IN INDONESIA PERSPECTIVE

M. Adnan Madjid[1], Adis Nevi Yuliani[2] and Eko G. Samudro[3]

[1] Lecturer on Peace and Conflict Resolution Department, Indonesia Defense University, Bogor, Indonesia
[2] Lecturer on Law Science Department,Cokroaminoto University, Makassar, Indonesia
[3] Assistant Lecturer on Peace and Conflict Resolution Department, Indonesia Defense University, Bogor, Indonesia

*Corresponding author: adnan.madjid@idu.ac.id

Abstract

Various initiatives have been established by Indonesian state agencies and civil society organizations in countering terrorism attack recently. However there should be more effort to make it largely affected the extremists. While there are signs that stakeholders are willing to collaborate and share best practices, the national counter-terrorism agency (Badan Nasional Penanggulangan Terorisme, BNPT) may be more effective if it assumed the coordinating role it was originally mandated to occupy. Instead the BNPT has initiated its own CVE programs, which many observers perceive to be top-down, fragmented and lacking consistent commitment. Hence this research proposes a Countering Violent Extremism effort in Indonesia Perspective. These conditions made the Countering Violent Extremism important to be applied in the entire environment, especially among the society.

1. Introduction

Indonesia as a multicultural country has various types of threat due to the diversity of its society. The differences among societies may determine the different value, goals and also beliefs that may contradict for certain individuals or groups. Thus, the emergence of violent extremist may possibly happened to impose their thoughts or beliefs to the others. The violent extremist threat, which is also related to the terrorism, comes from a range of individuals and groups, for instance the international terrorist groups like al-Qaeda and ISIS. The local offenders or small groups may be radicalized to commit extreme violence at their environment or even attempt to travel abroad to become foreign fighters. Surely, the uses of social media, internet and hatred news are the powerful tools to begin the recruitment and radicalization of individuals and raising the group members. The program of Countering Violent Extremism (CVE) is a proper choice against the irresponsible person in spreading the extreme ideology. Frazer and Nunlist (2015) explained that the violent extremism is no longer associated only with individuals terrorist attacks, but also with conflicts that have caused tens of thousands of deaths and injuries, thus CVE fosters closer cooperation and exchange between the security services and actors in the fields or conflict management and prevention. The violent extremists should be fought through the smart and strategic way, for instance, by tackling the structural cause of violent extremism including the intolerance act, government fraud and failure, political issues, economic factors and social marginalization. Moreover, in Countering Violent Extremism (CVE), it is necessary to engage with relevant local communities, professionals and non-governmental actors in developing strategies to counter the violent extremist narrative that can promote the terrorist acts attempts. The efforts are realized through empowering youth, families, women, men, religious, cultural and education leaders, and all other concerned groups of civil society, and also promoting the idea of living in harmony among diversity. Based on the explanation above, this research proposes a Countering Violent Extremism effort in Indonesia Perspective. These conditions made the Countering Violent Extremism important to be applied in the entire environment, especially among the society. While there are signs that stakeholders are willing to collaborate and share best practices, the national counter-terrorism agency (*Badan Nasional Penanggulangan Terorisme*, BNPT) may be more effective if it assumed the coordinating role it was originally mandated to occupy. Instead the BNPT has initiated its own CVE programs, which many observers perceive to be top-down, fragmented and lacking consistent commitment. Civil society organizations, meanwhile, have strong grass-roots networks, hands-on experience, and the legitimacy required to engage individuals with subversive conviction (Sumpter, 2017).

2. Rudimentary

2.1. Classifying Drivers of VE

When researching the causes of VE it is beneficial to draw on systems of classification of such drivers, as this helps to ensure that potential contributory factors are noticed. It is USAID does not aim to offer a definitive list of potential drivers, but as examples of push factors it mentions social marginalization and fragmentation, poorly governed or ungoverned areas, government repression and human rights violations, endemic corruption and elite impunity, and cultural threat perceptions. Pull factors are said to include access to material incentives, social status, adventure, self-esteem, personal empowerment and a sense of belonging, as well as 'the presence of radical institutions or venues, service provision by extremist groups, and extremist involvement in illegal economic activity. (USAID, 2011).

While USAID proposed the push and pull factors, Khalil, J. and Zeuthen, M. (2016) adapted the following adaptation to this existing typology:

- **Structural motivators.** These include repression, corruption, unemployment, inequality, discrimination, a history of hostility between identity groups, external state interventions in the affairs of other nations, and so on.
- **Individual incentives.** These include a sense of purpose (generated through acting in accordance with perceived ideological tenets), adventure, belonging, acceptance, status, material enticements, fear of repercussions by VE entities, expected rewards in the afterlife, and so on.
- **Enabling factors.** These include the presence of radical mentors (including religious leaders and individuals from social networks, among others), access to radical online communities, social networks with VE associations, access to weaponry or other relevant items, a comparative lack of state presence, an absence of familial support, and so on.

2.2. Psychological Theories

Psychological theories of violent extremism are primarily concerned with understanding and group factors contribute to radicalization and acts of terror. The main area of focus in the discipline and research on the psychological theories of terrorists is the mental functioning and personality of the individuals. Authors of this field are not necessarily psychologists or psychiatrists by profession but rather draw their conclusions on psychological responses to sociological influences or the result of individual mental illness and/or trauma (Brynjar and Katja 2005). Further, psychological profiling attempts have failed to provide a consistent 'terrorist profile' (Al-Lami, 2009). Even looking at only 'jihadist' terrorism there is considerable diversity: some are well-off financially while others are poor; some are highly educated and others not; some are well-integrated and others live in the margins of society; some are single and others are married; some have traumatic childhoods and some come from loving, stable families; some have criminal records and others are law-abiding up until the terrorist attack. About the only thing 'jihadi' terrorists have in common is that they appear to be exceedingly 'normal' under most measures (Al-Lami, 2009). Simple socioeconomic explanations of radicalization are unable to account for this variety. The problem is that this theory presumes that terrorism is instrumentalist and financially motivated. It is assumed that the other factors such as perception of discrimination and also concerning Western government's foreign policy with regard to Muslim countries and peoples can be triggers of frustration that lead to radicalization, irrespective of economic conditions.

2.3. Radicalization

Veldhuis and Staun (2009) define radicalization as "the active pursuit or acceptance of far-reaching changes in society, which may or may not constitute a danger to democracy and may or may not involve the threat of or use of violence to attain the stated goal". Normally, the definitions of radicalization stress difference from societal norms. It can be stated that radicalization is the changing process into extreme perspective towards the certain situation. Thus, the radicalization which is followed by the extreme idea or thought might lead to the violent acts. The literature implies that we know someone is radicalized because they have radical ideas and therefore are radicals.

About the only thing that radicalization experts agree on is that radicalization is a process (Al-Lami, 2009). In fact, several authors point out that radicalization does not necessarily follow a linear path, with some people drifting in and out of radical and more moderate groups (Al-Lami, 2009). To a large degree, CVE policy has kept pace with an expanded understanding of how and why individuals become involved in extremist violence. Over the past ten years, significant social science research has advanced a sophisticated analytic framework of the dynamics of radicalization. This research has led past simplistic explanations for terrorism, and we now understand radicalization as a fluid, nonlinear, highly individualized process.

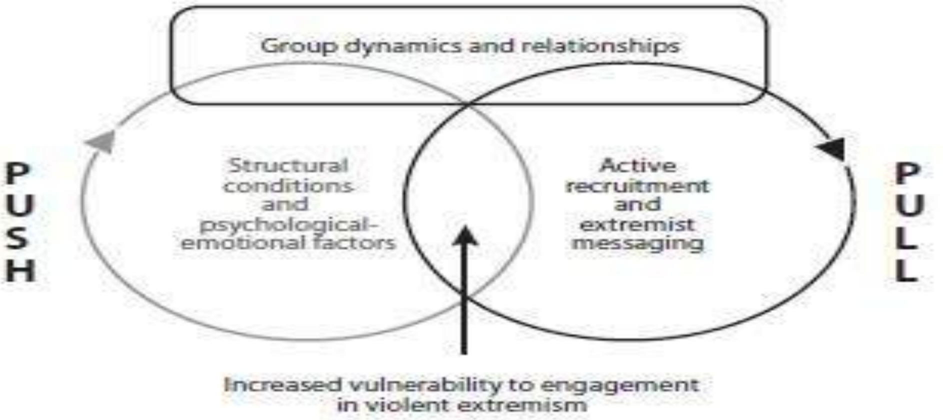

Group dynamics and relationships
PUSH
Structural conditions and psychological-emotional factors
Active recruitment and extremist messaging
PULL
Increased vulnerability to engagement in violent extremism

Figure 1. Dynamics of Radicalization
Source : Al-Lami (2009)

Sageman, M (2008) explained the process reflects the interplay of drivers on several levels:

- Push factors that include structural conditions, such as poverty, and grievances, such as lack of access to political processes or justice;
- Individual psychological and emotional characteristics, such as need for belonging, dignity, meaning, or revenge, or the continuation of cycles of violence brought on by chronic conflict;
- The influence of socialization and group dynamics by family, peers, and schools; and
- The pull of active recruitment to include extremist messaging that inspires violence.

2.4. Network-based CEWERS

Conflict Early Warning and Response System (CEWERS) is a concept which illustrate various activities to conflict prevention. The assumption in CEWERS concept is usually refer to the analogy that conflict as a cycle, which are, conflict prevention step, intervention to stop violence (peacekeeping), negotiation to create peace (peacemaking) and also the effort to develop peace in order establish long-term resillience (ITP, 2005). There are three main activities that should be done for CEWERS. First, creating a conflict background analysis or conflict background report. This step refers to the analyzing of components and process that establish a conflict and peace in the past. Second, creating analysis about current conflict which product is called as the current condition. The aim of this step is to analyze the contribution of each component and process that establish past conflict and peace in supporting the current conflict and peace. The last step is the combination of the first and second step, which is called as CEWERS Report. In order to create good CEWERS Report, the creating process should be developed by using network-based. Network is the source of information as well as the arena for idea and action exchange in order to prevent the conflict (ITP, 2005). The chosen stakeholders will become the member of this network. FGD (Focus Group Discussion) will become the tool for CEWERS practitioners together with the chosen stakeholders to analyze conflict and peace establishment scenario. Thus, the CEWERS activities are the activities that is conducted by, from and for the community network themselves as the stakeholders (ITP,2005).

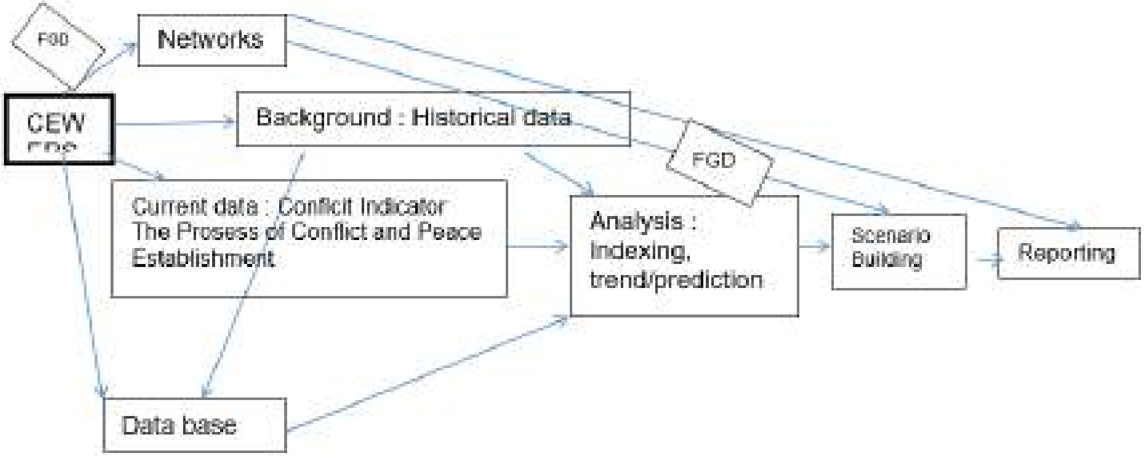


Figure 2. The Activities of Network-Based CEWERS
Source: ITP, 2005

There are steps in designing the conflict background, *first*, composing objective of CEWERS in a specific form. *Second*, creating conflict chronological narratives in the past (concerning important phase from the escalation by 5W1H Method). *Third*, doing SAT analysis (Structure, Accelerator, Trigger) by defining significant components in the phase of escalation and de-escalation. *Fourth*, mapping the important process in the chronological narratives through securitization analysis, which includes "conflict building" and "peacebuilding". The analysis of SAT aims to reframing data which is obtained from 5W1H analysis, especially in the part of "What" and "Why". SAT is realized as objective facts affecting the dynamic of conflict escalation and de-escalation. Structural Factor is also considered as the background which creating pre condition of conflict. For instance, economic dispaties, political exclution, etc. This structural indicator components are used to judge the risk of latent conflict. Accelerator Factor is the events that contribute to the conflcit escalation or even de-escalation. While Trigger Factor is the events that trigger the conflict to be happened.

2.5. The Education of "State Defense" (Bela Negara)

The programme of "State Defense", it is usually called as "*Bela Negara*", is one of the programme led by The Defense Ministry of The Republic of Indonesia. This programme is basically aimed at the citizen attitudes and behavior to increase their sense of belonging and great interest to their own country, Indonesia. As the Article 27, verse 3 UUD 1945 stated that, "Every citizen entitled and required to be participated in the effort of defense and national security". This article should be a guide for the citizen obligations which are concerning about national defense and security. The citizen participation in the effort "State Defense" are realized through civic education, basic military training on a mandatory basis, joining Indonesia Army and serving based on their profession. In the Doctrine of State Defense as stated in the Defense Ministry Regulation, No. 24 in 2004, there are 5 (five) base attitudes of *Bela Negara*, loving the country to defend The Republic of Indonesia, awareness of nation and state in the diversity, convincing Pancasila as the ideal basis and the 1945 Constitution as the constitutional foundation, willing to sacrifice for the sake of the nation and having the early ability of defending states that include both psychic and physical abilities.

3. Results and Discussion

3.1. *"Bela Negara"* and State Defense in Countering Violent Extremism

In the context of CVE, it is related to the Defense Science, especially in Peace and Conflict Resolution Study. The relation between threat and state defense as stated in Constitution No. 3 in 2002 about State Defense that "State Defense is all the effort in defending the sovereignty of the state, the integration of territory and the safety of the citizen from the threat outside the country. In the General Defense Policy of the Year 2015-2019 stipulated by Presidential Regulation No. 97 of 2015 explained that the nature of state defense is all universal defense efforts, whose operation is based on awareness of the rights and obligations of citizens and confidence in their own strength. State defense is based on the principles of democracy, human rights, public welfare, the environment, the provisions of national law, international law, international customs, and the principle of peaceful coexistence by considering the geographical conditions of Indonesia as an archipelagic country and maritime state. Countering-Violent-Extremism (CVE) paired with the nature of state defense, it has 2 (two) emphases on awareness of citizens' rights and duties also the confidence in their own strengths. The belief in its own power implies that efforts or Countering-Violent-Extremism are excavated based on the powers that exist within the Indonesian nation, in this case society as the largest part of the nation. Communities need to be empowered so that they have resilience against Violent-Extremism threats.

3.2. Violent Extremism and Countering Violent Extremism

Bjørgo (2005) mentions, there are no single roots of terrorism, or even a set of causes, but there are preconditions and precipitations of various forms of terrorism. Terrorism in the long run is set in Prerequisites. Prerequisites alone are not enough to cause terrorism. The originator is much more directly affected the rise of terrorism. This is a particular event or situation that directly proceeds, motivates or triggers the outbreak of terrorism. Some things as prerequisites and triggers are described below. *First*, the lack of democracy, civil liberties and the rule of law are a prerequisite for various forms of domestic terrorism. *Second*, the failure or weakness of the state in controlling the violence. *Third*, rapid modernization in the form of high economic growth has also been found to be strongly correlated with the rise of ideological terrorism, but not with ethno-nationalist terrorism. When traditional norms and social patterns are collapse or irrelevant, new radical ideologies may become attractive to certain segments of society. *Fourth*, either religious or religious-based extremist ideologies can at least be the intermediate cause of terrorism, although people usually adopt extremist ideologies as a consequence of fundamental political or personal reasons. According to a study form USAID (2009b), it has identified the driving factors of the rise of violent extremism, namely the denial of basic political rights and civil rights, human rights violations and government repression, rampant corruption, impunity enjoyed by the elite, bad governance, protracted violent conflicts and illegitimate government. These environmental or structural conditions are push factors that force a person to support violent extremism. Research conducted by USAID (2009b) has also highlighted the pulling factor that makes the ideas of violent extremist groups and groups attractive. Among these factors are the social networks and personal relationships, material gains, and social gains from joining extremist groups using charismatic leaders and leaders and interesting ideas and interests.

3.3. Discussion

Counter-Terrorism and radicalism that have been done, less likely to pay the attention in prevention aspects that can be done on these vulnerable communities. The approach used was more on the reactive aspects with the use of force (*Hard Power*), either after the occurrence of terror attacks or after the existence of individuals from vulnerable communities who have become radical. The use of Hard Power by Densus 88 and BNPT, were not considered optimal and even counterproductive. The counterproductive was in the level of trust of some people. For example, due to the mistake in capturing criminals, mis-shot, misinformation, the community lost their trust to these institution.

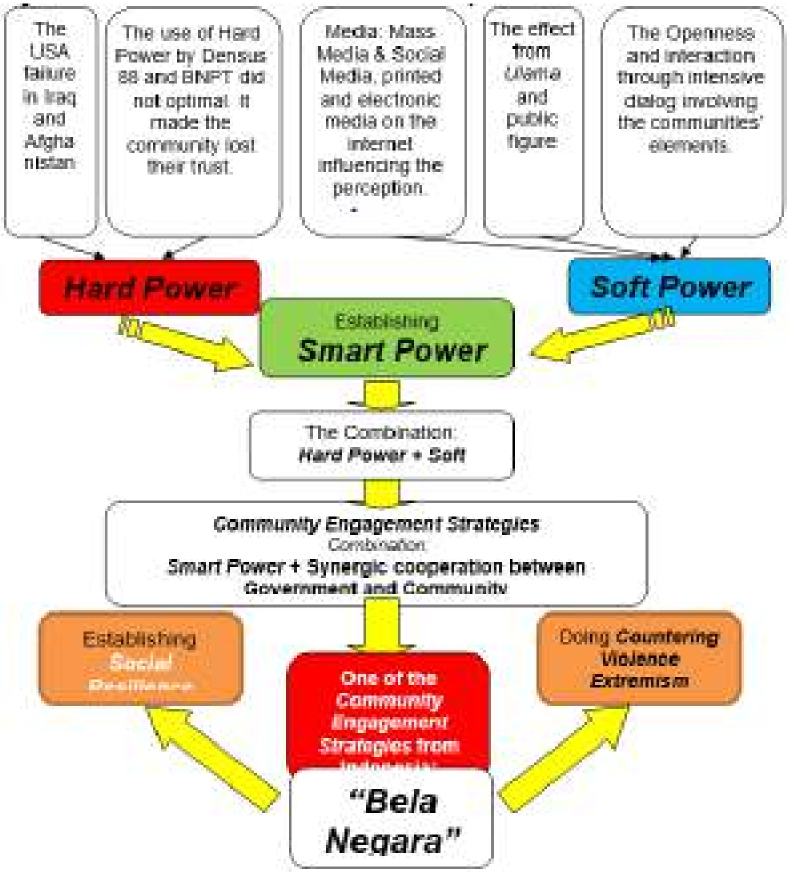

The USA failure in Iraq and Afghanistan
The use of Hard Power by Densus 88 and BNPT did not optimal. It made the community lost their trust.
Media: Mass Media & Social Media, printed and electronic media on the internet influencing the perception.
The effect from Ulama and public figure
The Openness and interaction through intensive dialog involving the communities' elements.
Hard Power
Soft Power
Establishing Smart Power
The Combination: Hard Power + Soft
Community Engagement Strategies
Combination:
Smart Power + Synergic cooperation between Government and Community
Establishing Social Resilience
One of the Community Engagement Strategies from Indonesia:
"Bela Negara"
Doing Countering Violence Extremism

Figure 3. *Bela Negara* (State Defense) as one of the Smart Power & Community Engagement Strategies owned by Indonesia in facing Terrorism and Radicalism.

The Smart Power-based strategy is needed to overcome the problem of terrorism and radicalism in Indonesia. Ways that can be used for example is with Community Engagement Strategies which is a combination of Smart Power accompanied synergy cooperation of the government and society in overcoming the problem of terrorism and radicalism (Figure 5). In Indonesia, the State Defense Program can be considered as a form of Community Engagement Strategies. Due to the increasing love of the homeland, willing to sacrifice for the sake of the nation and state, etc. The society is considered to be able to have a higher Social Resilience and able to perform and apply CVE independently to radical ideology and views that are not in accordance with the spirit of *Bela Negara*. Frequently, terrorism has its roots in economic, political, social and cultural factors mixed with each other, which are then justified by literal and rigorous interpretation of religion; or even deliberately misleading-which is inconsistent with the interpretations agreed upon by authoritative and recognized religious interpreters. The existence of discrimination and the imposition of religion, including the abolition of Islamic law in the past, became the structural root of separatist and terrorist movements. The counterterrorism and separatism should be multi-facetted, multi-track and comprehensive. The military and security response will not be able to handle terrorism. On the contrary, it can be counterproductive and create excesses that can create a difficult "circle of terrorism" to end.

4. Conclusion

Based on the explanation before, there are several conclusions that can be stated in this paper as the guide for the government:

- The importance to improve the community awareness regarding CVE through state defense (*"Bela Negara")* program.
- Conducting intensive discussion between the community and the government elements in order to gain trust through CEWERS Framework.
- Doing social approach to the community by conducting empowerment and education for the community.
- Convincing the community, especially the youth, in realizing diversity and living harmony in diversity.
- Analyzing and correcting the root causes of the problems among the community in order to prevent radical ideology spreading in the community.
- Restricting the media in presenting the quality of the news that may direct the community to the misconception towards the Violent Extremism.

Acknowledgements

The authors would like to acknowledge assistance or encouragement from all colleagues in Indonesia Defense University, special work by all of the informants and also the support from organizations in completing this paper.

References

[1] Al-Lami. (2009). *Studies in Radicalisation: State of the Field Report*: Politics and International Relations Working Paper.

[2] Bjørgo, T. (2005). *Root causes of terrorism: myths, reality, and ways forward*. New York : Routledge

[3] Brynjar, L., and Katja, H-W.S. (2005) Facts and Fiction in Theories of Terrorism - An Expanded and Updated Review of the Literature on Causes of Terrorism, 57pp.

[4] Frazer, O and Nunlist, C.(2015). *CSS Analyses in Security Policy. The Concept of Countering Violent Extremism*. Swiss: CSS, ETH Zurich.

[5] Institute Titian Perdamaian (ITP). (2005). *Mari Mencegah Konflik*. Yayasan Tifa: Jakarta.

[6] Khalil, J and Zeuthen, M. (2016). *Countering Violent Extremism and Risk Reduction. A Guide to Programme Design and Evaluation*. UK: Stephen Austin and Sons, Ltd.

[7] Sageman, M. (2008). *Leaderless Jihad: Terror Networks in the Twenty-First Century*. Philadelphia: University of Pennsylvania Press.

[8] Sumpter, C. (2017). Countering violent extremism in Indonesia: priorities, practice and the role of civil society. *Journal of Deradicalization*. *Summer 2017 Nr. 11*. ISSN: 2363-9849.

[9] USAID. (2011). *Development Response to Violent Extremism and Insurgency*. Retrieved from http://pdf.usaid.gov/pdf_docs/ pdacs400.pdf in March, 7th 2018.

[10] USAID. (2009b). *Development Assistance and Counter Extremism: A Guide to Programming*. Retrieved from https://dec.usaid.gov/dec/content/GetDoc.axd?ctID=ODVhZjk4NWQtM2YyMi00YjRmLTkxNjktZTcxMjM2NDBmY2Uy&rID=MzE0ODgw&pID=NTYw&attchmnt=VHJ1ZQ==&rdp=ZmFsc2U=. in May, 12th 2018.

[11] Veldhuis, T., & Staun, J. (2009). *Islamist Radicalisation: A Root Cause Model*. The Hague: Netherlands Institute of International Relations Clingendael.

THE ROLE OF THE MINISTRY OF DEFENSE OF THE REPUBLIC OF INDONESIA IN THE MANAGEMENT OF MAN-MADE DISASTER

Deny Widi Anggoro[1], Agnes Manuella[2], IDK Kerta Widana[3]

[123]Indonesia Defense University, IPSC complex, Sentul, Bogor 16810, Indonesia

*Corresponding author: deny.widianggoro2007@gmail.com

Abstract

Man-made disasters are essentially threats to national security, which need to be addressed if they occur and need to be assessed to be anticipated and prevented. In the effort to overcome man-made disasters, the relevant Ministries and Agencies as the main element while the Ministry of Defense of RI acts as a supporting element and policymaker in its environment and Indonesian National Army as a technical executor. The purpose of this research is to analyze the optimization of the role of the Ministry of Defense in the handling of man-made disasters in Indonesia. Technical Analysis used is Qualitative Analysis, by using observation, interview, documentation, and combination (triangulation) data collection technique. The results showed that in its policy role, the Ministry of Defense of the Republic of Indonesia has not made a policy to regulate man-made disaster management efforts within the Ministry of Defense and Indonesian National Army environmental, so that its role needs to be optimized through various efforts, namely determining objectives, subjects and objects, appropriate facilities and infrastructure and methods; and carry out efforts in the form of activities that lead to policy making in the form of formulation of ministerial defense regulation on Man-Made Disaster Mitigation in the Ministry of Defense, the Indonesian National Army Environment and propose the making of Presidential Regulation on Man-made Disaster Prevention Efforts.

1. Introduction

Indonesia is an archipelago that has abundant natural resources. In addition to its geographical position to provide benefits, the forest also has various types of plants that become resources and can be utilized for people's welfare. The sea territory of the Republic of Indonesia (NKRI) also provides abundant sea produce. Although land and sea areas yield abundant results, they can also have a bad impact on life if not controlled. All conditions, be it geographical, geological, hydrological or demographic allow for disasters, caused by natural factors, non-natural factors, and human factors that result in fatalities, environmental damage, property losses, and psychological impacts. If this hazard interacts with vulnerability, disaster risk will be formed [1].

To anticipate the disaster that occurred in Indonesia, the government issued Law Number 24 of 2007 concerning Disaster Management. Based on the Law, the causes of disasters include natural, non-natural and human factors. Based on the factors that influence it, disasters can be caused by natural disasters and man-made disasters [2]. Man-made disasters include technological failures, transportation accidents, epidemics of disease, forest fires, acts of terror, social conflicts.

One potential threat is the failure of GMO technology according to the 2006-2009 National Action Plan for Disaster Risk Reduction. GMO is a genetically engineered product through gene transformation or DNA from bacteria, microbes, animals, or viruses for certain purposes. Genetic engineering of GMOs has a detrimental effect, namely the potential toxicity of foodstuffs resulting from the emergence of new chemicals/toxins and other genetic hazards that were previously never encountered in conventional food ingredients. In 1996 the World Health Organization (WHO) explained the emergence of various types of new chemicals, from transgenic organisms and their products, this could potentially lead to the emergence of a new disease, and become a trigger for other diseases. Because the spread of marker genes in GMOs can complicate the treatment of infectious diseases that can threaten life and eventually the disease explodes and then spread throughout the world. The technological failure that still occurs today is the Lapindo hot mud tragedy, a wild burst from oil exploration wells in Sidoarjo, East Java. These hot mudflows contain high pressure, continuously coming out to the surface of the earth and sinking housing, rice fields, and business land. Many of the losses incurred and victims were displaced for several years. On the other hand is the outbreak of epidemics, epidemics. Some of the dangerous viruses that have ever existed in Indonesia have caused people to be infected and have died from the virus so quickly spread.

The national defense system implemented by our government through efforts to build and foster capabilities, the deterrence of the state and nation to overcome all threats through a universal state defense system. The national defense system that faces military threats places the Indonesia National Army (TNI) as the main component with the support of reserve components and supporting components. Whereas to deal with non-military threats, government institutions outside the defense sector are the main element, according to the form and nature of the threats faced with the support of other elements of the nation's strength. Therefore, besides being a major component in facing military threats, the TNI is also another element of the nation's strength in supporting the main elements in dealing with non-military threats. The non-military defense system has implications for national defense through cross-agency roles, namely facing threats with ideological, political, economic, socio-cultural, information and technology-based dimensions, public safety and the task of assisting the TNI. Whereas in facing public safety threats, placing government elements in the field of public safety is the main element. Public safety is multi-agency in nature which consists of handling the impact of natural and man-made disasters, pandemic diseases, transportation safety, and evacuation. Government institutions that make policies within the TNI in overcoming the threat of disaster are the Ministry of Defense of the Republic of Indonesia (Kemhan RI). This is based on the consequences of disaster threats which are challenges and risks that will continue to be faced and need to be anticipated by each country [3]. In carrying out the functions of formulation, stipulation, and implementation of policies in the field of defense, the national defense policy in the military sector was to carry out Military War Operations (OMP) and Military Operations Other than War (OMSP). This disaster management effort is one of the tasks in the CSO. Strategic environmental changes as a result of climate change, natural disasters, or disasters as a result of human actions can cause crises, which have the potential to disrupt national defense. The man-made disaster is one of the threats that can disrupt the non-military defense system. This non-military threat tends to increase from year to year in line with the development and increasingly complex problems faced by the Indonesian state.

On the one hand, the threat can disrupt the national defense system, while on the other hand, the role of the Indonesian Ministry of Defense has not been optimal in overcoming all forms of threats, especially the man-made disaster. For the Republic of Indonesia Ministry of Defense to be more effective and optimal in helping government and other relevant institutions in man-made disaster management in Indonesia, Role Optimization is needed. Based on these problems, the question arises how the real role of the Indonesian Ministry of Defense and its optimization in man-made disaster management. Then it is hoped that the Ministry of Defense of the Republic of Indonesia can maximize its functions and duties as an institution that has a mandate in the implementation of affairs in the defense sector. The research aimed to analyze the real role of the Indonesian Ministry of Defense and its optimization in man-made disaster management.

2. Research Methods

The methodology used in this research is qualitative. Cresswell (2014) explains that qualitative research is a method for exploring and understanding the meaning that by several individuals or groups of people are ascribed to social or humanitarian problems [4].

In this study, using data collection techniques, namely observation, in-depth interviews and documentation. In-depth interviews were conducted with informants from the Ministry of Defense to obtain primary data. The research informants in this study were officials from the Indonesian Ministry of Defense, such as from Directorate of Defense Potential (Ditjen Pothan) namely Director of Support Component of Directorate General of Defense, Directorate General of Defense Strategy (DG Strahan), namely Director of Anstra Directorate General of Strahan and The Director of the Tour Per Law of the Directorate General of Strahan and the Center for Data and Information (Pusdatin), namely the Head of Bangsisinfohan. Documentation techniques for collecting secondary data to support data obtained from in-depth interview techniques. Documentation technique according to Sugiyono (2007) is a record of past events, a method of collecting data obtained from existing documents or records stored, both in the form of notes, transcripts, books, newspapers, etc. [5] The documents in this study can be in the form of writing and drawing, in the form of books, policy regulations and photographs relating to research.

Data analysis in this research uses the Miles and Huberman models as explained by Sugiyono (2016). Data analysis techniques according to Miles and Huberman are data reduction (data reduction), data display (data presentation), and conclusion drawing & verification (conclusions and verification) [5].

3. Data Analysis

3.1 The Real Role of the Indonesia Ministry of Defense

Faced with role theory, Bruce. J. Cohen (1992) states that there are enacted roles and prescribed roles [6]. In this writing, the real role is the role that has been carried out by the Indonesian Ministry of Defense in man-made disaster management, while the recommended role is the optimization of the real role of the Indonesian Ministry of Defense. The real role carried out by the Indonesian Ministry of Defense in man-made disaster management is still limited to formulating the principles of non-military defense policy, namely Non-military state defense policy, Policy for empowering national defense, Policy for mobilizing national defense forces, Legislation policies, Budget policy, and Supervision policy.

Kemhan currently has a work unit, The National Strategic Installation Agency (Bainstranas) with the sub-unit Puspamhar in the Sentul area which deals with strategic areas, in which there is a National Disaster Management Agency (BNPB), the National Counter Terrorism Agency (BNPT), and Defense University. Bainstranas only coordinates matters relating to the headquarters with institutions in the Sentul Strategic region, although in the strategic area there are institutions such as National Disaster Management Agency and National Counter Terrorism Agency, Bainstranas does not have a working relationship about disaster engineering with the two institutions.

Kemhan has a Defense University (Unhan) whose faculty is the National Security Faculty and one of the study programs of this faculty is the Disaster Management Study Program. In the process of learning and teaching, Unhan has collaborated with BNPB, for example, Officials from BNPB have become resource persons and teaching staff at Unhan. In addition, students from the Disaster Management Study Program were included in the Managerial Level of Basic Disaster Management and received the Brevet Response, Agile, Tough, which is usually given to Regional Disaster Management Agency (BPBD) staff.

DG Defense Potency (Pothan) has not formulated policies that regulate man-made disaster management in the Ministry of Defense and the TNI. In accordance with the main tasks and functions work unit which became the leading sector in making this regulation explicitly does not yet exist, but the closest is the Directorate General of Defense. DG Pothan itself does not yet have a data and information center about the disaster as a collector of data and information related to disasters, so if you need data and information, you must actively look for it. If you need data about the disaster, the Directorate General of Hospitality can coordinate with BNPB and BPBD.

Ditanstra Directorate General of Strahan has not carried out a strategic analysis of the threats caused by disasters, especially man-made disasters because the Directorate General of Strahan has not received data and information on disasters routinely from units under the TNI, both as disaster special reports and standby reports. This strategic analysis can be used to make estimates and considerations in disaster management efforts, especially man-made disasters. Dit Tur Per Strahan Law has not yet compiled regulations related to man-made disasters, because this regulation does not yet exist. This directorate has not proposed policy-making in man-made disaster management to be prioritized because there is no policy draft and proposal from the relevant work unit according to their duties so that they can enter the National Legislation Program to be followed up in Proleghan.

Pusdatin Ministry of Defense does not have and collect data and information about the disaster, because there is no Ministry of Defense that has sent data about this disaster and there is no confirmation in the main tasks and functions to send it, while other Ministries / Institutions do not have the relationship/obligation to provide disaster data regularly. But there is already thinking in this direction while waiting for regulations that regulate relations between related Ministries / Agencies. If Pusdatin requires data and information about the disaster, Pusdatin can take it online.

In planning activities, the making of regulations related to disaster management efforts, especially man-made disasters for the 2017 budget year does not yet exist. This can be seen in the Prolegnas and Proleghan. In Proleghan 2017, the one approval agreement that is related to disaster management efforts is only one and that is still general in nature, not related to man-made disasters, namely the RPP on the Assistance of the Indonesian Armed Forces in Facing the Result of Natural Disasters, Evacuation and Providing Humanitarian Aid If a man-made disaster is seen as a threat to national security and is a priority, it can be submitted in the National Legislation Program and the National Office to be immediately followed up in the Work Plans And Budgets for working groups making regulations. The Ministry of Defense of the Republic of Indonesia can propose a larger regulation, a Law or Presidential Regulation as legal protection for man-made disaster management efforts, which can then be followed up / elaborated by Ministries / Institutions according to their respective main tasks and functions. Ministries / Institutions that can follow up include the Ministry of Defense, Ministry of Home Affairs, Ministry of Social Affairs, Ministry of Health, BNPB, BNPT, National Police and others. Specifically for the Indonesian Ministry of Defense, the Act will be followed up with the making of Permenhan regulating artificial disaster management in the Ministry of Defense and the TNI.

Existing regulations related to man-made disasters are general policies, policies on the use of the strength of personnel and TNI defense equipment and the MoU between the Legal Secretariat of the Ministry of Defense and BNPB. General policies relating to man-made disaster management are state policies that regulate military defense in which there are main points of national resource management policies for non-military defense. There are no policies or regulations governing the use of the strength of personnel and TNI defense equipment in the context of disaster management, especially for artificial disasters, but there is only general mobilization, namely Regulation of the Minister of Defense of the Republic of Indonesia Number 46 of 2016 concerning the Use of Weapons in the Implementation of Internal Assistance Tasks Military Operations Apart from War. The policy that regulates disaster management in the form of an MoU between the Secretariat General of the Ministry of Defense and BNPB only regulates coordination/support only if there is a disaster (by case).

3.2 Optimizing the Role of the Indonesian Ministry of Defense

The Indonesian Ministry of Defense has increased its role by formulating policies that regulate man-made disaster management in Indonesia. So based on the theory of optimization, if you want to optimize the role of the Indonesian Ministry of Defense in disaster management, then the role of the Indonesian Ministry of Defense is currently being changed to a better role or the highest role. In other words, optimizing the role of the Indonesian Ministry of Defense in man-made disaster management is a process to get a role that provides maximum value in man-made disaster management. To achieve the role of the Republic of Indonesia Ministry of Defense which is better in man-made disaster management, appropriate policies need to be formulated. Before formulating this policy, it is necessary to do this:

a. Determine the goals to be achieved, the subject and object, the facilities and infrastructure needed and the right method. The targets to be achieved are:
   1) The realization of the situation and condition of the Republic of Indonesia that is safe and controlled from all threats, especially threats originating from man-made disasters.
   2) The realization of the most minimal human and material victims, as a result of man-made disasters.

   The subject of optimizing this role is the Director General of Defense Potential of the Ministry of Defense of the Republic of Indonesia. The Indonesian Ministry of Defense is a ministry that is the leading sector in the field of defense and viewed from the point of view of the country's threat. The Minister of Defense, through the Director General of Defense, formulates policy on mitigating the impact of disasters caused by man-made disasters. With the issuance of policies from the Minister of Defense, of course, the institutions under their supervision, such as the TNI Headquarters and the Force, will follow up the policy by making relevant regulations.

The objects in optimizing this role are software and human resources. The software that will be created at the Ministry of Defense level is the Minister of Defense Regulation (Permenhan), this Permenhan will later be followed up to become a Perpang in TNI Headquarters and Lawsuit, Judicial and Mighty in the Forces. Human resources include TNI soldiers and civil servants of the Ministry of Defense and the TNI starting from work unit personnel related to policy making, disaster expert personnel to TNI soldiers and civil servants who are deployed/assisted in technical disaster management

Facilities and infrastructure such as defense equipment; other aid tools; health equipment; friction / building as an assembly point, post, evacuation site, which is no less important to be prepared from the time before the disaster and prevention, at the time of the disaster until the response to the impact of the disaster. The method used in this strategy can be in the form of assignments to the soldiers of Kemhan and the TNI and their civil servants; empowering disaster experts, owned SAR and defense equipment; counseling/socialization about disasters; job training to Kemhan and TNI personnel and their civil servants; education/courses related to disaster.

b. Implementing efforts in line with the determined goals to be achieved, the subject and object, the infrastructure needed and the right method, then the efforts that need to be done by the Ministry of Defense of the Republic of Indonesia are:

1) Collect regulations related to disaster management, both Laws, Ministerial Regulations (Permen), Head Regulations (Perka) and other rules and regulations that can be used as references.
2) Inventory all possible security threats from man-made disasters.
3) Collect as much information as possible about regions, regions, regions, objects that might be affected by man-made disasters.
4) Submitting the production of this regulation to the relevant Work Plans And Budgets work unit, in this case, the Directorate General of Hospital Affairs.

5) DG Pothan forms a Working Group Team (Pokja) in his internal to draft a draft of Manpower Disaster Management.
6) The internal Working Group Team from the Directorate General of Hospital created a draft regulation that regulates man-made disaster management.
7) DG Pothan submitted a draft Regulation on Managing Disaster Management into Proleghan.
8) Form a Working Group Team at the Ministry of Defense and the TNI tasked with drafting the Manpower Disaster Management Report.
9) The Pokja Kemhan and TNI teams formulated a draft Ministerial Regulation on Man-made Disaster Management in the Ministry of Defense and the TNI.
10) Assign Dir Tour Per UU Strahan General to harmonize the policies made.
11) Proposing the making of a Presidential Regulation (Perpres), if it is deemed necessary to have even greater policies that can regulate coordination and involvement of several ministries and institutions in the prevention of integrated man-made disasters, such as the Ministry of Home Affairs, Ministry of Social Affairs, National Police, BNPT, Sar And Rescue Agency and BNPB.
12) Assign Dir Tour to the Act of the Directorate General of Strahan to coordinate and propose it to the Legislative Agency (Baleg) so that it can enter into the National Legislation Program and become a priority to be put into a Presidential Regulation or Law.
13) Invite all relevant agencies from the Ministry / Institution and the work unit in the internal Ministry of Defense and the TNI to get advice/input, data/information, sharing and determine who does what according to their respective duties and functions.
14) The Perpres Working Group Team makes a draft Presidential Regulation concerning Man-made Disaster Management.
15) Coordinate as best as possible with all relevant agencies, so that policy making that can regulate man-made disaster management can be completed on time.
16) Determine which work unit is responsible according to their respective functions, both those who formulate policies, which collect and analyze as well as those that store disaster data and information
17) Assign Pusdatin to collect data and information about disasters that can be validated and make it in one post or supervise Subdivision of the Directorate General of Pothan if the Directorate General of Pothan does it.

18) Propose / design regulations/articles governing the involvement of relevant ministries/institutions if a more accurate collection of data and information requires cooperation/coordination with ministries/agencies outside the Ministry of Defense.
19) Increasing the role of the State Defense through activities carried out by the Directorate General of Defense Potential (Ditjen Pothan) Ministry of Defense.
20) Increase the study activities on Disaster Management by the Unhan Disaster Management Study Program in collaboration with BNPB, Central / Regional Governments, and other Related Institutions.
21) Increase budget and disaster management activities through TNI activities, both in preventing disasters, assisting the Search and Rescue Team (SAR) when dealing with natural and non-natural disasters and human-caused disasters and Regional Damage Control after the war is over.

4. Discussion

4.1 The Real Role of the Indonesia Ministry of Defense

Man-made disasters are essentially a threat to national security and need to be addressed if they occur and need to be studied to be anticipated and prevented. Faced with the theory of disaster, which says that disasters are caused by natural, non-natural and human factors, the Ministry of Defense's non-military defense system also recognizes man-made disasters, but policies specifically regulating man-made disaster management that do not yet exist and still need to be formulated. Likewise, the involvement of the TNI technically in the phase/phase according to the concept of disaster management, namely pre-disaster, emergency response and post-disaster has not been clearly regulated, because no policy regulates it, especially for man-made disaster management. The making of a Memorandum of Understanding (MoU) between the Secretariat General of the Ministry of Defense and the BNPB had once been made but was still limited to coordination/requests for TNI support if needed and by case. As one of the military threats, matters related to disaster must be coordinated by the Directorate General of Defense with BNPB and BPBD, the Ministry of Social Affairs, and the Ministry of Health, Ministry of Home Affairs, local government, and other Ministries and Institutions.

As one of the military threats, which is related to man-made disaster management efforts, it must be clearly stated in main tasks and functions work unit/sub work unit within the Ministry of Defense, even though it is only as a policymaker that will be technically implemented by the TNI in the region.

4.2 Optimizing the Role of the Indonesia Ministry of Defense

In facing the threat of Nir Military the Ministry of Defense Republic of Indonesia formulated policies relating to all forms of mobilization and the use of TNI forces to counter military threats which were not aggression and for the task of assisting the TNI consisting of humanitarian relief, civic mission, duties assistance to the National Police of the Republic of Indonesia in the context of public security and order, as well as the duty to maintain world peace. This policy includes disaster management efforts, especially man-made disaster management.

The Indonesian Ministry of Defense is not an institution that does technically disaster relief efforts, both natural and non-natural, especially man-made disasters. But as an institution that becomes a supervision and policy formulator from the TNI should make policies or regulations that regulate disaster management, especially man-made disasters in the Ministry of Defense and the TNI. The Ministry of Defense Work unit which organizes policy formulation in the field of non-military potential in accordance with the Organization and Work Procedure of the Ministry of Defense (based on Minister of Defense Decree No. 58 of 2014) is the Directorate General of Defense. But in reality, there is no policy formulated by Pothan that regulates man-made disaster management. In the future, this policy will be important given the changes and advances of the times and the increasing threat of the state, including the threat of disasters, especially the threat of man-made disasters.

As an institution that examines threats to national security, the Indonesian Ministry of Defense in its main tasks and functions must clearly state which work unit/sub-work unit is the leading sector in formulating policies on disaster management, especially man-made disasters. Although the work unit that is closest to matters related to disasters is the Directorate General of Defense, but in the formulation of policies the mitigation efforts are less clear whether it is under the Directorate General of Pothan or Directorate General of Strahan.

Data and information about disasters both natural and man-made disasters have not been received regularly by the Directorate General of Veterinary Medicine, but these data must be actively searched for themselves in the event of a disaster in Indonesia. As a threat to national security, disaster data and information must be obtained routinely so that it can be collected and studied to be anticipated and addressed if it occurs so that the resulting harm can be minimized. Disaster data can be reported in stages through a standby report and then collected and reviewed at the Directorate General of Strahan. Disaster data can also be collected and coordinated by the Directorate General of Drug and Drug Administration with BNPB or BPBD. If needed, the Pusdatin Kemhan can assist/supervise the sub-section of data and information (subbagdatin) from the Directorate General of Pothan or Directorate General of Strahan in collecting disaster data. There needs to be an affirmation of the duties and responsibilities of collectors/collectors of data and information about disasters, to be used as material for strategic study/analysis, whether this activity is carried out by the Directorate General of Defense as a work unit responsible for non-military defense, or Directorate General Strahan responsible for conducting strategic analysis, or Pusdatin as a work unit responsible for data collection and processing.

In the activity of disaster management efforts, both natural and man-made, legal protection is needed in the form of laws, Presidential Regulations (Perpres), Ministerial Regulation (Permen) and Commander's Regulation (Perpang) and the Regulations of the Chief of Staff (Perkasad , Perkasal, and Perkasau). In order to increase the role of the Ministry of Defense of the Republic of Indonesia from not being optimal to be optimal, in a man-made disaster management effort a Minister of Defense Regulation is required. This regulation is made whether it underlies the Presidential Regulation that is related and made before or as a policy formulation that can be used as a legal protection for the TNI in assistance activities or disaster mitigation efforts in the region. This regulation will certainly be elaborated downward in the TNI and Force in the form of Perpang, Perkasad, Perkasal, and Perkasau. With the Perpres, the roles of each Ministry and Institution can be regulated (Ministry of Defense and TNI, Police, Ministry of Home Affairs / Regional Government, Ministry of Social Affairs, and BNPB/ BPBD and other agencies), who does what in man-made disaster management efforts.

5. Conclusions

From the analysis and discussion of the data obtained, conclusions can be given as follows:

a. The real role of the Ministry of Defense in man-made disaster management.
   1)The Indonesian Ministry of Defense does not yet have a policy that regulates man-made disaster management efforts in the Ministry of Defense and the TNI, which will be elaborated under the agency in disaster management.
   2)There has been no confirmation in the main tasks and functions of work unit/subwork unit in the Ministry of Defense of the Republic of Indonesia which is responsible

in formulating policies and collecting data on disaster management, especially man-made as study material in order to anticipate and mitigate it.

b. Optimizing the role of the Indonesian Ministry of Defense.

1)Policies in the form of Permenhan that regulate man-made disaster management in the future will be important in line with the progress of the times and the increasing number of state threats to Military Defense.

2)If even greater policies are needed that can regulate the coordination and involvement of several ministries and agencies such as the Ministry of Home Affairs, Ministry of Social Affairs, Ministry of Health, National Police, BNPT, Sar And Rescue Agency and BNPB in mitigating integrated man-made impacts, it can be proposed the formulation of the Presidential Regulation on Man-made Disaster Management.

Based on the conclusions drawn, the following recommendations are given:

a. In responding to the importance of man-made disaster management at present and in the future, it is suggested that the Ministry of Defense of Republic of Indonesia be advised in this case the Directorate General of Defense to carry out more in-depth research and inventory of the main threats to Nir Military Defense, make matriculation that can map who does what for each of the ministries and institutions, which can integrate all relevant ministries and institutions outside of Defense according to their duties, so that synergy is established when the threat arises.

b. As a recommendation to the Ministry of Defense of the Republic of Indonesia so that they can optimize their role by establishing a policy in the form of Ministerial Regulation on Man-made Disaster Management in the Ministry of Defense and the TNI so that the threat of man-made disasters can be overcome.

References

[1] Anwar, Herryzal Z & Harjono, Hery. 2013. *Menggapai Cita-cita Masyarakat Tangguh Bencana Alam di Indonesia*. Bandung: Lipi.

[2] Wiarto, Giri. 2017. *Tanggap Darurat Bencana Alam*. Jatirejo: Gosyen. Publishing.

[3] Kementerian Pertahanan Republik Indonesia. 2015. *Buku Putih Pertahanan Indonesia*. Jakarta

[4] Creswell, John.W. 2014. *Research Design Pendekatan Kualitatif, Kuantitatif, dan Mixed*. Yogyakarta: Pustaka Pelajar.

[5] Sugiyono. 2007. *Memahami Penelitian Kualitatif*. Bandung: CV. Alfabeta.

[6] Cohen, Bruce.J. 1992. *Sosiologi : Suatu Pengantar*. Jakarta: Rineka Cipta.

COMMUNITY ADMINISTRATION IMPROVEMENT FACING THE ERUPTION OF MERAPI VOLCANO THROUGH SISTER VILLAGE

Nur Intan Sari[1], Arlen Intani[2], Sugimin Pranoto[3], and Christine S.M.[4]

Department of Disaster Management, Defense University, IPSC Area, Bogor, West Java 16810, Indonesia

*Corresponding author: nurintansari44@gmail.com

Abstract

Magelang district has a new program in disaster risk reduction through Sister Village, villages that are in the KRB III disaster-prone areas, and villages that safer as a buffer village. This study uses a descriptive method with a qualitative approach that aims to analyze the sister village as an effort to improve community preparedness in the face of the eruption of Merapi volcano. The research locations were located in Ngargomulyo, Kalibening, Kaliurang and Ngelumut villages as KRB III villages, as well as Tamanagung, Adikarto, sucen and Bligo villages as buffer villages. Participants were selected through techniques purposive and snowball sampling. Data collection techniques used observation, in-depth interviews, documentation and material audio-visual which were then analyzed by qualitative techniques. The results of the study show that Sister Village can improve community preparedness, by applying 12 preparedness values in disaster risk reduction with supporting factors for local wisdom, feeling the same impact from the eruption of Merapi volcano, and adequate resources. This program emphasizes the community independence to utilize the resources they have in disaster risk reduction, and needs the role of the government as supervisor evaluation, so as to increase community preparedness in the face of the eruption of Merapi volcano.

1. Introduction

Indonesia geologically located at the confluence of three tectonic plates of the world who are active, namely Indo-Australian plate, the Eurasian plate and the Pacific plate are respectively located in the south, north and east. The three plates move and collide with each other, so that the Indo-Australian plate goes down the Eurasian plate and causes earthquakes, volcanic pathways, and faults or faults. The occurrence of subduction of the Indo-Australian plate which moves north and the Eurasian plate which moves to the south forms the earthquake pathway as well as a series of active volcanoes along the islands of Sumatra, Java, Bali and Nusa Tenggara. Indonesia is part of two large mountain ranges in the world, namely the Mediterranean mountain range and the Pacific Circum mountain range. In addition, Indonesia is also located in three shallow areas, namely the Sunda Shelf, Sahul and the Australian Mid Sea region of Asia. The geological location is what causes Indonesia to have many volcanoes. Indonesia is the country that has the most volcanoes in the world with a percentage of 13 percent of the total volcanoes in the world. One of the volcanoes that is still active in Indonesia is Merapi volcano.

Based on data from the Regional Disaster Management Agency (BPBD) of Magelang Regency (2014), the number of deaths due to the Merapi volcano eruption and cold lava floods since the 20th century has been recorded at 1,987 people, with the highest number of casualties occurring at 1,369 people in the eruption of Mount Merapi in 1930. It was recorded that Merapi volcano had erupted more than 68 times since 1548. Merapi volcano has released a lot of hot clouds on the surface of the earth, as many as 32 of the 68 eruption events. In addition, Merapi volcano has also experienced major eruptions that occurred in 1786, 1822, 1872 and 1930 [1]. In the past 100 years, small eruptions have occurred between 2 and 4 years and larger eruptions occur between 10 and 15 years. When viewed from the history of the eruption of Merapi volcano, that the biggest eruption in the 21st century occurred in 2010, the eruption resulted in the death toll as many as 338 people, 453 people were injured, and 2,856 destroyed houses spread in Sleman regency, Klaten, Boyolali, and Magelang. Based on data from the Center for Operational Control (Pusdalops) of the National Disaster Management Agency (BNPB) as of November 27, 2010, that the disaster of the eruption of Merapi volcano in November 2010 caused 339 deaths in the Central Java region. Based on data compiled by BNPB as of December 31, 2010, the eruption of Merapi volcano has caused damage and losses of Rp. 3.5 trillion.

Various efforts have been made to reduce the risk of the Merapi volcano eruption, one of which is in Magelang district. The Magelang regency government through BPBD is the facilitator of the establishment of the MOU for the creation of a Disaster Risk Reduction (DRR) program, namely the *sister village*. *Sister Village* is a DRR program that emerged from the initiative of Merapi volcano disaster-prone areas. Through this program, it is expected that during the Merapi volcano eruption, the community in the Merapi volcano KRB III will not experience panic because they already know the clear direction and purpose of where they have to flee.

Based on the experience of the eruption of Merapi volcano in 2010, that displacement carried out by affected communities evacuated more than once, according to the status of Merapi volcano. If the status of Merapi from normal becomes vigilant, then the people have evacuated to places that they think are safe, but if Merapi's status returns to increase, then the people will return to flee to a point farther from the initial evacuation to make it safer. The evacuation carried out became irregular, where there were several people who were displaced by utilizing public facilities, such as mosques, urban village offices, school buildings and the homes of relatives who owned them. Even there are still people who do not want to take refuge because they are worried about livestock and their property.

In the program *Sister Village, the* placement of refugees in sister villages (buffer villages) varies greatly, some are placed in public facility buildings, residents' houses or a combination of public facility buildings and houses, all depending on the conditions of the buffer village. So that after the program *Sister Village, it is* expected that the community can carry out a far better pattern of refuge, namely the community can only carry out evacuation once and with the guarantee that livestock can participate in the evacuation.

Sister village as a Disaster Risk Reduction program, not only focuses on disaster-affected villages KRB III to be active in Disaster Risk Reduction, but buffer villages also play a role as subjects and objects in Disaster Risk Reduction. One of the things that must be considered in this program is the facilities and infrastructure for supporting refugees in the buffer village. With the program *sister village*, it is expected that community preparedness will be far better and a pattern of refugees be formed, clear distribution of logistical assistance during the disaster of the Merapi volcanic eruption.

The establishment of the MoU *sister village was* conducted in 2014 and continues to the present. In implementing or implementing the program *sister village, it* still has many short comings both from the preparedness of buffer villages and from affected villages. This is in accordance with the results of the study stating that, community involvement in the program is *Sister Village* still very minimal because it does not have clear basic tasks and functions (TUPOKSI) from the community itself, both from the buffer and affected villages [2]. Community involvement is the key to implementing theprogram *sister village*. The community is the main subject and is directly involved, because this program starts from the local wisdom of the community in establishing brotherly relations among the villages. In addition, community involvement can also optimize the protection of the community itself from the threat of risks and impacts of disasters [3].

2. Methodology

The method used in this study is a descriptive method with a qualitative approach. Qualitative research is a method of research carried out to explore and understand meaning that is ascribed to social or humanitarian issues involving various efforts, such as asking questions and procedures, collecting specific data from participants, analyzing data inductively from specific themes to general themes, interpreting the complex meaning of data from a problem, and compiling a final report that has a flexible structure or framework [4]. Qualitative descriptive research is a research procedure that produces descriptive data in the form of written and oral words from the people observed [5]. The research subjects were the Magelang District Disaster Management Agency, the Village Head in the affected villages and buffer villages, the Community in the KRB III area of Magelang district, the OPRB KRB III village and the buffer village LPBD, and facilitators in the system *Sister Village*. Data collection techniques by observation, in-depth interviews, documentation, and *audio-visual* [6]. Data analysis is done by coding data, and triangulation of data is done as a method of testing the validity of data.

3. Results and Discussions

3.1. Preparedness Improvement Analysis in the Program Sister Village

Research was conducted on 4 pairs of villages, namely Tamanagung and Ngargomulyo, Adikarto and Kalibening, Ngelumut and Sucen, Bligo and kaliurang. Of the 10 indicators of preparedness in each village, almost all of them have applied, although there are still some indicators that need to be improved. The 10 indicators are conducting vulnerability analysis, the first step taken by the Magelang district government in implementing the program *Sister Village* is conducting vulnerability analysis. The Merapi volcano region of Magelang district is divided into 3 Disaster-Prone Areas (KRB) which consist of KRB 1 or areas that are considered the safest and far from the disaster-prone areas; KRB 2 or areas that are still considered safe from the eruption of Merapi volcano, but the distance of the location is not too far from Merapi volcano; and KRB 3 or volcanic eruption-prone areas of Merapi [7]. Vulnerability analysis carried out in the program *sister village* with the aim of affected villages is to look at what resources and vulnerabilities they have, so that they can assist in selecting the buffer village criteria they need. After each of the villages has conducted their vulnerability analysis, the next step in each village is to plan with the resources they have to overcome this vulnerability. As stated by Mr. Mart Widarto (2017) as the facilitator in the making of the *Sister Village*, that "the BPBD of Magelang regency only provides a condition, that the buffer village must be a village outside the KRB III and the buffer village must voluntarily accept and approve the fraternal request from the village affected by disasters. "

The selection of village partners is done by measuring the resources needed by each village, such as the number of residents, number of livestock, vulnerable populations, and any needs that are considered necessary in the evacuation and evacuation process. As has been done by Ngargomulyo village and Tamanagung village. Ngargomulyo Village is a village with more cattle than the population, so Ngargomulyo village chose Tamanagung village as a buffer village with one consideration, that Tamanagung village has a livestock market that can be a place of refuge for livestock during the eruption of Merapi volcano. As stated by Mr. Gunawan (2017), "in the program *Sister Village, resources* are needed from each village, because the *sister village* is actually an independent refugee system, where each village must make the most of the resources they have, if truly unable to eat the local government will help with the value of the disability. ''

After we know the vulnerabilities and resources of each village, anwill be made MoU by the chosen village partners. After submitting a request in theprogram *Sister Village*, each village gave a *draft* request to the village partner to be agreed upon and signed together, so that it became an MoU with the aim of changing the management of the village apparatus, the program *Sister Village* will continue without any obstacles. The MoU was conducted as a result of the Regional Regulation of Magelang Regency Number 7 of 2014 concerning the 2014-2019 Regional Medium-Term Development Plan, which was inaugurated in 2014 as a form of community preparedness in facing the eruption of Merapi volcano. The form of MoU conducted in *Sister Village* was not only carried out by 1 affected village with 1 buffer village, but 1 affected village could have brothers with 2 to more buffer villages, all depending on vulnerability analysis and resources owned by each village.

After the formation of village pairs with an MoU, BPBD Magelang regency as the person in charge of disaster risk reduction in Magelang district carried out education and training in stages. The first education and training was carried out with the aim of all village partner apparatus to find out the concept from the *sister village*, because the village apparatus would be responsible for implementing the program *Sister Village* to disseminate information to the community regarding the implementation of the *sister village* program. As explained by Mr. Mart Winarto as the facilitator of the *sister village* (2017) training, "this training was not carried out simultaneously by all villages within the KRB 3 scope, but this training was conducted per period. As in 2014 only 2 pairs of villages were trained in *sister villages*, because all depends on the BPBD of Magelang regency. "Meanwhile, according to Mr. Gunawan as Head of Preparedness (2017)," training is carried out gradually every year because it adapts to the budget provided by Magelang regency, so that if there is sufficient budget, there will be many couples *sister village* conducted training. If the budget is a little, then there will be a little pair *sister village* that will be trained. "

In the program *Sister Village*, the Magelang district government in this case BPBD suggested that the Disaster Risk Reduction Organization be formed (OPRB) at the village level for the KRB 3 area and the Regional Disaster Management Agency (LPBD) at the buffer village level as a forum for coordination and communication between the villages. These two organizations were formed with members from government and village communities, with the aim of creating a good coordination system within one organization, as well as existing organizations within the community, also involved in the management of the organization, either OPRB or LPBD. As has been done by Mr. Yatin as the Ngargomulyo Village Head, who has had many local organizations such as Pagar Merapi, Pasak Merapi KARINA (Catholic community organizations that care about disasters), and Santri Peduli Bencana and outside organizations. Combining these organizations into the village OPRB with the aim that if there is an eruption of the Merapi volcano OPRB which basically represents all groups of people can be directly coordinated to notify the community to carry out evacuation at a safe point. Not much different from the LPBD in the buffer villages, such as Tamanagung village which has the only LPBD that actively applies the merger of LPBD management by the community and village officials [8].

New organizations under the auspices of the BPBD on the program *Sister Village*, such as the OPRB and LPBD found in KRB 3 disaster affected villages and buffer villages, are not all capable of being active due to various things. Village of Adikarto is one of the villages that has an inactive LPBD, such as the explanation of Mr. Muhammad Mansur as the Village Secretary (2017), that Merapi volcano does not have a specific or special early warning device, because the eruption of Merapi volcano occurs with several stages of the Merapi volcano condition, as delivered directly by BPPTKG (Institute for Investigation and Development of Geological Disaster Technology) which was then submitted to all local governments to village governments. BPBD Magelang Regency still facilitates the community and the schools and their environment with the Merapi eruption warning system, a form of warning system facilitated by BPBD is an agreed early warning system and must be accessible to all communities, both in the village environment and communities in the fields where they work. The agreed early warning system is in the form of a *siren* or notification directly through the mosque toa and using *kentongan* if the electricity goes out [9].

The information system carried out in the eruption of Merapi volcano is centered on BPPTKG. Information related to the status of Merapi volcano activities was officially issued by BPPTKG which will then be reported to the BPBD of Magelang regency on a regular basis, as stated by Mr. Gunawan as the Head of BPBD Preparedness for Magelang regency. The information is then disseminated through existing media, namely radio and website or distributed through groups *Whatsapp* consisting of all Village Heads of Magelang Regency. In addition to information directly from BPPTKG, BPBD also received reports from local communities around Merapi volcano. The information system delivered was in accordance with the activity conditions of Merapi volcano, where when Merapi volcano was alert the people had prepared valuables to prepare for evacuation, had been carried out by vulnerable people, children and pregnant women, so that when Merapi volcano was alert the community had can do total evacuation.

Mr. Ahmad Husen Rifai as Chair of the SIBAT in Kaliurang Village (2017) explained that, "The response mechanism established in the community remains based on the information system of BPPTKG, where the public will be prepared and begin to collect valuable items for evacuation preparation and carry out initial evacuations to vulnerable communities when they are on alert. On the alert status of Merapi, the Kaliurang people are still allowed to carry out activities as usual, such as raising livestock and farming, but all activities are only allowed until noon. After noon, all residents are not allowed to do activities far from settlements " [10].

Residents stand guard when the condition of Merapi volcano rises to alert, there will be notifications through *Kelentong*, mosque ToA, and direct notification by officers to carry out evacuation or evacuation processes, so that the community will gather at the gathering point that they have agreed on, so that evacuation can be carried out together towards the buffer village. However, the response mechanism in each village is different, as is done by the Kalibening village, Kalibening village conducts a response mechanism based on each hamlet [11].

The evacuation routes that are made will be different in each village, and the paths made will not be on the main route to avoid congestion, so the chosen evacuation route is jalaur-jalaur which is outside the main line even though the route is slightly rotating from each village to the village buffer. Making this evacuation route has been agreed by each village, according to the explanation of Mr. Gunawan as the Head of BPBD Preparedness in Magelang regency. Although there are still refuge points that are used together, such as Ngargomulyo and Kalibening villages which only have 1 evacuation route to the buffer village, one route is only passed until the sub-district or KRB III location is out, while on the main line of each village. have their own path to get to their respective buffer villages. After all the steps have been taken, the final stage that is very important is simulation. Simulation is the initial training phase scheduled by BPBD Magelang district in theprogram *Sister Village*, where the first training is training all village officials or those represented by the OPRB or LPBD, where the simulation takes place after training on the form of *Sister Village*, assignments and functions from each village, planning, response mechanisms and evacuation routes, postal rehearsals, training, and simulations [12]. Simulations were carried out to test contingency plans that had been made by BPBD in Magelang district. In addition, simulations are the right way to improve community preparedness, where in the simulation process the community gets direct training on what they have to do, knows the meeting points they have to go to, and the evacuation sites they will temporarily occupy if the eruption of Mount Merapi . The purpose of this simulation is to train the community about the procedure for evacuation and the response that must be made by the community. So that the obstacles that arise during the simulation will be used as material for evaluation, because even though the OPRB or LPBD has been formed, it is feared that the public will forget if they do not practice it. Therefore, the simulation is very important for every village, so that aformed *Sister Village* program can bethat can run well.

3.2. *Supporting Factors and Inhibiting Factors in the Implementation of Sister Village*

One of the supporting factors is local wisdom. This policy was born based on inner closeness between communities, the experience of displacement and the local wisdom of the people on the slopes of Merapi volcano. So that in its formulation, the community is fully involved. This shows that *sister village* is a manifestation of the concept of *Living in Harmony with Risk* [13] and is a form of resilience that is born of community care. Based on the results of interviews with Mr. Yatin as the Head of the Ngargomulyo village, that the term *sister village* which was first carried out by the village community is often referred to as "ngedol deso". In addition, the growth of local wisdom which is a supporting factor for the implementation of the program *sister village* is a sense of encouragement, please help. From this local wisdom is formed aprogram *sister village* that focuses on disaster risk reduction. In addition, the similarity of cultures, the similarity of tribes, livelihoods, and language also make it easier for people to establish communication, so that communication and adaptation can work well. Another supporting factor is the same impact. Eruption of Merapi volcano has many stages, starting from the appearance of hot clouds, thick fog, hot lava, cold lava and other impacts. Almost all the people in Magelang district felt the impact of the eruption of Merapi volcano, even though they did not feel the harmful effects directly, as felt by the community in KRB III, while other villages still felt the rain of leftover ash from Merapi volcano, dead economy, environment it became dark because it was covered by a cloud of mountains. "Villages that are far away can feel the impact like that, what else is the village that is in the KRB III", according to sir Nunung as Chair of LPBD Tamanagung village. So that the people in Magelang regency would voluntarily accept the community from the KRB III when they fled from the eruption of Merapi volcano even though without going through the program *sister village*, because the KRB III community had often sought refuge in the village of Tamanagung, and the community always welcomed, gave make shift housing and logistics assistance.

The inhibiting factor in the implementation of this program is communication, because *Sister Village* is a disaster risk reduction program based on community independence, where the main key in this system is communication between the two villages. The purpose of communication is to establish a good communication so that when the displacement occurs due to the eruption of Merapi volcano the buffer village continues to carry out its duties as a buffer village and is able to accept the affected villages well. The impact of poor communication as experienced by the village of Adikarto as a buffer village from the village of Kalibening, according to Mr. Muhammad Mansur as the Secretary of the Village of Adikarto, that after the signing of the MoU between the two villages and training, the village of Adikarto as a buffer village felt objections related to village requests Kalibening in the MoU that they agreed to before, there are points that they cannot fulfill as buffer villages. The role of the organization should be very important in communication, because it is an alternative pattern of communication between village partners if village officials are not able to communicate. The form of organization formed in the *sister village* program recommended by BPBD Magelang regency to be formed in the program *sister village* is the OPRB for Disaster affected villages (KRB III) and LPBD for buffer villages.

Making an organization in the midst of existing organizations makes the newly backward organization inactive if the village government is not good at managing to make the organization stay active, because members of each organization are people from their respective villages, and every individual from the community have a different job and not all people have an interest in social life, because even active in the organization will not get a salary. As was done by Mr. Yatin as the Head of Ngargomulyo village who already had 5 Care for Merapi organizations from various elements before the OPRB was made, so that when the OPRB was made he merged the 5 existing organizations into one within the OPRB, so that the OPRB in Ngargomulyo village remained active with 5 existing organizations, and the inhibiting factor that plays an important role is supervision. The *sister village* program is a-based self-reliance disaster risk reduction program, which focuses on the ability of each village to utilize the resources they have in advance. When the resources they have have not been able to meet their needs, then the government plays an active role to help meet the shortcomings of the village's needs. The government which is currently represented by the BPBD in Magelang regency should carry out a supervisory function to check the condition of each village, both from resources, communication, and organization that occurs between the two villages, so that when the Merapi volcano erupts the program *sister village* planned can be carried out good, according to the explanation from Mr. Mart Widarto as the facilitator of the program *sister village*.

New indicators in implementing the program *Sister Village* to increase community capacity and preparedness, namely communication and supervision. Where communication in the program *sister village* is an important indicator of the success of the village to maintain harmonious relations and mutual openness about the needs of each village. *Sister village* will run well and be able to improve community preparedness if it has 12 indicators of preparedness. The function of 12 indicators is to improve the performance of the program *sister village, the* need for supervision in seeing the development of communication that occurs between villages, helping village couples to re-collect resources and needs, make contingency plans or plans, and resolve problems. Each village in the program in the *Sister village* Magelang regencyhas implemented 12 indicators of preparedness, although not all villages have implemented 12 indicators that are able to improve community preparedness in the implementation of *Sister Village*.

4. Conclusions

The application of the 12 preparedness indicators in the program *sister village* is a way that can improve community preparedness, but still needs the important role of the government in the process of monitoring the implementation of the program. Each village, both buffer villages and affected villages must be active in conducting communication and discussion between villages, so they can resolve existing problems and get a way out. *Sister Village* can improve community preparedness by applying the values of preparedness, such as conducting a vulnerability analysis to identify and record resources as a basis for planning, making an MOU based on the needs of each village. The process of training and outreach was carried out to improve community capacity, the existence of organizations that focused on disaster risk reduction that made the community participate in all activities. There is a response mechanism agreed upon by the community in the form of early warning, information systems, evacuation routes that can be easily accessed by the public. Not only training and socialization, simulation is also carried out as a direct practice for the community to implement what has been learned. The simulation starts from postal simulation to thorough simulation in testing the planning and mechanism of community response in the face of increasing the status of Mount Merapi, simulations carried out until the community evacuation process to the evacuation site in the buffer village involving 30% of the number of disaster-affected villages III. So that people act as subjects and objects in disaster risk reduction.

Supporting factors in the program *Sister Village* are local wisdom, where the *sister village* is local wisdom that stems from the habits of the community in the eruption of the Merapi volcano eruption which later became an official program of local government in disaster risk reduction. In addition to local wisdom which is a contributing factor, it is felt the same impact from the disaster of Merapi volcano eruption, making other villages feel safe by helping and willing to become a buffer village. The availability of adequate resources from both the KRB III disaster affected villages to carry out displacement independently and the buffer village as a place of refuge is one of the supporting factors for the implementation of *Sister Village*. The inhibiting factor in implementing *Sister Village* is the lack of supervision from the local government in this case is the BPBD Magelang regency in monitoring the implementation of *Sister Village*, such as increasing the data of their resources to evacuate, forms of communication between the two villages, activeness of the organization village disaster risk reduction, both KRB III disaster affected villages or buffer villages. *Sister Village* is a program that emphasizes the independence of the community to utilize the resources they have for disaster risk reduction, but the role of the government as responsible for implementing the program *Sister Village* must also be an important role that not only provides logistical assistance during a disaster or post disaster, but remain active in the pre-disaster process to improve community preparedness by conducting evaluations.

Acknowledgements

The Authors wish to thanks the management of the BPBD Magelang and the Disaster Management Study Programme, Faculty of National Security of the Indonesia Defense University for their full support and facilitating this research.

References

[1] Matsuda, Y., and Okada, N. (2006). *Commonity Diagnosis for Sustainable Disaster Preparedness. Journal of Natural Disaster Science*. Kyoto University.

[2] Ardianingrum, A.G. 2014. Dampak Erupsi Merapi 2010 terhadap Pemanfaatan Lahan dan Daya Pulih Masyarakat di Kecamatan Cangkringan. Tesis: MPPPDAS, Fakultas Geografi, UGM.

[3] Pratomo, I. (2006). Klasifikasi Gunung Api Aktif Indonesia, Studi Kasus dari beberapa Letusan Gunung Api dalam Sejarah. *Jurnal*

Geologi Indonesia, 220.

[4] Creswell, John. W. 2016. *Research Design Pendekatan Metode Kualitatif, Kuantitatif dan Campuran.*Yogyakarta: Pustaka Pelajar.

[5] Meleong, Lexy J. 2012. *Metodologi Penelitian Kualitatif*. Bandung: PT. Offset Remaja Rosdakarya.

[6] Creswell, John. W. 2016. *Research Design Pendekatan Metode Kualitatif, Kuantitatif dan Campuran.*Yogyakarta: Pustaka Pelajar.

[7] Gunawan. 2017. Hasil Wawancara dan Observasi di Lapangan. Kepala Kesiapsiagaan BPBD Kabupaten Magelang. Jawa Tengah.

[8] Yatin. 2017. Hasil Wawancara dan Observasi di Lapangan. Kepala Desa Ngargomulyo. Magelang.

[9] Yatin. 2017. Hasil Wawancara dan Observasi di Lapangan. Kepala Desa Ngargomulyo. Magelang.

[10] Rifai, Ahmad Husen. 2017. Hasil Wawancara dan Observasi di Lapangan. Ketua SIBAT Desa Kaliurang. Magelang.

[11] Eni. 2017. Hasil Wawancara dan Observasi di Lapangan. Sekertaris OPRB Desa Kalibening. Magelang.

[12] Widarto, Mart. 2017. Hasil Wawancara dan Observasi di Lapangan. Fasilitator dalam Pembuatan *Sister Village*. Yogyakarta.

[13] Maarif, Syamsul. (2012). *Pikiran & Gagasan Penanggulangan Bencana di Indonesia*. Badan Nasional Penanggulangan Bencana. Jakarta.

[14] European Committee for Standardization (CEN) 2003 Actions on Structures; Traffic loads on bridges *Eurocode 1, Part 2 (EN 1991-2)* – this is an example of a reference to a standard

PEOPLE EMPOWERMENT THROUGH RIVER SCHOOL PROGRAM FOR DISASTER MITIGATION IN PUJIHARJO VILLAGE, TIRTOYUDO SUB-DISTRICT, SOUTH MALANG DISTRICT

Yohanes Ari Setyaji[1], Rahaninda Putri Assanti[2], Fani Aprilia Perdani[3], Sutopo Purwo Nugroho[4], Fauzi Bahar[5]

[1] Disaster Management Study Program, Faculty of National Security, Indonesia Defense University, Bogor 16810, Indonesia
[2] Disaster Management Study Program, Faculty of National Security, Indonesia Defense University, Bogor 16810, Indonesia
[3] Disaster Management Study Program, Faculty of National Security, Indonesia Defense University, Bogor 16810, Indonesia
[4]Permanent Lecturer, Faculty of National Security, Indonesia Defense University, Bogor 16810, Indonesia
[5]Permanent Lecturer, Faculty of National Security, Indonesia Defense University, Bogor 16810, Indonesia
*Corresponding author: arijjo@gmail.com ; rahanindaputri@gmail.com

Abstract

Community Empowerment is a process that comes from society to society. Community Empowerment has contained four aspects according to Deepa Narayan, which is access to information, involvement and participation, accountability, and organizing capacity of local communities. This concept is the process from below or bottom up because the solution comes from the community, rather than accommodate the desire or demand from the upper level. The purpose of the research is to analyse community empowerment through the River School Program for the mitigation of flood flooding in Pujiharjo village, Tirtoyudo sub district, South Malang district. Data obtained from the specified informant, hereinafter analyzed by qualitative analysis technique. The River School Program in Pujiharjo village is does not continous, as a result Pujiharjo village is still has a prone of flash flood threats because disaster mitigation for river normalization is not maximized. The absence of sustainability of the River School Program is due to the program not being put in the Rencana Pembangunan Jangka Menengah Daerah (RPJMD). Badan Penanggulangan Bencana Daerah (BPBD) Malang district need to prepare the possibility of flash flood in Pujiharjo Village with disaster risk reduction activities.

1. Introduction

Malang district includes high disaster risk areas based on threat indicators, indicators of regional vulnerability to disasters and public capacity indicators and government responses in resolving disasters [1]. The disaster that most often struck Malang district is flooding, followed by landslides and drought [2]. The cause of flooding is closely related to the condition of the ecosystem, the greater the flood intensity the worse the ecosystem quality of a region. Data dan Informasi Bencana Indonesia (DIBI) Badan Nasional Penanggulangan Bencana (BNPB) records the number of catastrophic events up to June 2017 as many as 1,368 occurrences. The victim died and lost 227 inhabitants, injured victims and suffered 434 inhabitants, refugees 1,710,539 inhabitants, damage to the settlement as much as 18,983 units [3].

The trend of flood disaster and landslide continues to increase from year to year as the land function over [4]. From the forest area in Malang district about 127 thousand hectares, only remaining 47 thousand hectares. The critical forest transforms into cassava, sugarcane, and banana farming fields. Illegal logging or forest reforestation in the Daerah Aliran Sungai (DAS) system is associated with flooding during the rainy season in Pujiharjo village. Forest construction, soil compaction, decay and narrowing of the river cause rainwater to be unable to soak into the soil and largely become a surface flow with the expellers [5].

In this research, researchers emphasize the community's ability to protect its livelihoods and life from catastrophic threats. Empowerment is one aspect of state defense policy [6]. State defense policies are needed to build strong defensive forces that have the ability to handle various types of threats, including catastrophic threats. Empowerment as the process of developing, establishing, remixing, strengthening the bargain position of the community both layer down and over to the suppressor forces in all areas and sectors of life [7]. The Community empowerment approach is a disaster relief effort that helps create a more proactive attitude among the community [8].

The impact of damage and loss [9] due to flash flood in Pujiharjo Village becomes the forerunner of BPBD Malang district to conduct community empowerment program for the management of Tundo river and Purwo river with normalization and restoring function hydrological DAS [5]. Strengthening non-structural mitigation through the empowerment of the River School Program aims to ensure that people value rivers, maintain and maintain rivers. This activity is an empowerment process commonly associated with participation [11]. In the context of empowerment, participation is prevalent in the conceptualisation of community involvement in various forms of activities to make changes.

2. Theory

The concept of the River School Progam is learning about the in and out of the river with all its aspects that are community-based for river activists, students, local governments and the needy and organized to answer the needs of the river activists that requires adequate knowledge of community-based Sustainable river management/community participation [12]. The background of the program was the large number of damage to the rivers in Indonesia that reached 73% in 2014 and the management of the river that has been far from ideal. The school of rivers in Pujiharjo village, Tirtoyudo, Malang district is an idea of BNPB and BPBD that have been implemented on Tuesday, 25 October 2016 after a flash flood incident in Pujiharjo village. Based on regulation of Peraturan Menteri Desa, Pembangunan Daerah Tertinggal, dan Transmigrasi number 22 year 2016 on the establishment of priorities of village funds in 2017 article 5 points D said that procurement, development, development, and maintenance of facilities and environmental infrastructures for the fulfillment of needs, among others, 1) the preparedness of natural disasters; 2) natural disaster management; 3) other extraordinary event handling, and 4) environmental preservation.

Flash flood concept is flooding caused by high rainfall in mountainous or hilly areas, especially if the environment is already damaged. The flow of water on the surface will flow downward or to the lower place quickly or into a tributary that has been filled by rocks or trees and branches so that it will stem the river water naturally. When the accumulated volume of water grows and has not been restrained by the trees that stem, this natural dam will be broken, and water will slide downward with a very high speed and pressure while carrying rocks and grinding land On the river body so it becomes mud [2].

Community empowerment research through this River School Program authors using disaster management theory with community empowerment indicators, disaster mitigation paradigm, and effectiveness. Disaster management is a science that studies disasters along with all aspects related to disasters, especially disaster risk and how to avoid the disaster risk. The disaster management works through the activities that exist in each cycle, that are prevention, mitigation and preparedness, emergency response and recovery. The goal is to protect the community and its goods from catastrophic threats [13].

In the theory of Community Empowerment, society is an important aspect of a country or region. It is not only the primary actor in the life of the process, but the community is also a potential for social life sustainability. The paradigm of empowerment is the paradigm of human development, which is a people-centered development in this community of Pujiharjo Village incorporated into the River School Program, which is a development process that encourages initiatives Communities rooted from under [14]. Flay et al [15] stated that the study of effectiveness focuses on important factors such as the quality of implementation that will affect the outcome of a program, in this study is the school of Rivers Program. Meanwhile, Drucker [16] formulates effectiveness as a corresponding level between empirically output in a system with the expected output. Effectiveness is closely related to an activity to work properly in order to achieve a better outcome in accordance with its original purpose. Effectiveness of two aspects is assessed, that are problem solving skills and achievement of objectives.

In the implementation of this research also refers to the four elements according to Deepa Narayan [17] that are: access to information, involvement and participation, accountability, the organizing capacity of the local community. In addition to these theories, the discussion will be supported with some concepts being advocates in the research discussion.

3. Result and Discussion

The concept of disaster management has developed from a conventional view to a holistic view [5]. The conventional view considers the disaster an inevitable event or incident and the victim should immediately get help, so the focus of disaster management is relief and emergency. The aim of disaster management based on this view is to suppress the level of loss, damage and quickly restore the state of the paradigm on the subsequent disasters evolved into a mitigation paradigm. In this paradigm, the objectives are more aimed at hazard studies, including identification of disaster prone areas, recognizing patterns that could lead to insecurity and conducting mitigation activities. Its purpose as historical and empirical data can be used to determine the level of insecurity and the anticipated flood effort.

Village Hazard study [18] among others: a) the presence of recordings or records of catastrophic events that have occurred in the village Pujiharjo stored in archives or documents of the village, such as special daily reports by the head of the village of Pujiharjo to Camat Tirtoyudo, Data The Bandang flood disaster assessment, and the Bandang flood victim data which indicates an initial indication of the coming flood called the periodic flood (annual, five years, ten years, fifty years or one hundred years); b) Topographical mapping that shows the contour of the altitude surrounding the river basin which is equipped with the ability of the capacity of hydrological system and wide area of rainfall (catchment area) and "plotting" a wide range of puddles ever Happen. In this process, the rainfall data in the village of Pujiharjo is still use traditionally counting, as the community has the belief that when the rain drops at high intensity for a day, the early warning is ready to be activated.

Apart from the structural mitigation that has been done, disaster mitigation in Pujiharjo village has been quite effective because it has three main elements, which are assessment of hazards, warnings, and preparations [5]. First, a hazard assessment is needed to identify endangered populations and assets, as well as threat levels. This assessment requires knowledge of the characteristics of a flash flood, a possible occurrence of flash floods, and catastrophic event data in the past. This stage results in a potential map of the village disaster threat Pujiharjo. Secondly, a warning that aims to warn the public about a flash flood that will threaten or happen. The warning system of Pujiharjo village is based on disaster data that occurs as early warning and uses traditional and modern communication channels to give message to the community. Traditional communication channels in the form of kentongan/titir that will be sounded to the residents who are tasked to keep the picket in the post of the ronda when the signs of disaster occurs. While the modern communication channels used by Pujiharjo people are Handy Talky (HT), sosmed, etc. Thirdly, preparatory activities require knowledge of areas that are likely to be affected by disasters and knowledge of warning systems to know when to evacuate and when to come back when the situation is safe. The understanding, caring, and simulation carried out by the community and the village government has resulted in a reduction in the impact of the flash flood of the absence of casualties.

In this study, non-structural mitigation efforts were conducted through the River School Program. The River School Program is a disaster education activity that contains education about rivers and flash floods. This program is included in the community awareness program to modify the behavior of people to be more concerned about the environment. From the results of the research is known that the idea of the River School Program was held after the disaster. River School Program has a working group (Pokja) that consists of the community of Pujiharjo village and related agencies to perform the division of roles and work on the non-physical efforts of the flash flood mitigation efforts. These activities include inspections, observations and traceability of flood control infrastructure and facilities, recommending improvements to infrastructure and the means of flood control so that it can function as planned, monitor and evaluate rainfall data, floods, puddle areas and other information necessary for flood prone areas, preparing maps of flood prone areas with "plotting" evacuation routes, temporary evacuation locations, location of posts, and postal locations observer discharge flood/altitude flood water in flood cause river, check and test the existing facility early warning system and take steps to preserve it and shape it if it is not yet available with the simplest means implement logistics planning and the provision of funds, tools and materials required for emergency response, including emergency response supplies, food supplies and drinking water, countermeasures equipment (e.g.: movable pump, dump truck), countermeasures (example: sand bags, wood/bamboo shoots), and rescue equipment (e.g., inflatable boat and life buoy), planning and preparation of SOP (Standard Operation Procedure) for response activities involving all members of BPBD Malang district, conducting evacuation training for the community, holding coordination meetings, forming cross-sector networks and NGOS engaged in disaster awareness and with the media both print and electronic, conducting community education on the mapping of flood threats and associated risks and the use of waterproof/flood-resistant building materials [18].

Structural mitigation efforts undertaken by the people of Pujiharjo village according to Putuhuru [18] there are construction of retaining walls and embankment along the Tundo river and the setting of water flow and discharge speeds from upstream areas so as to help reduce the occurrence of flooding. Some efforts that need to be done to regulate water speed and the discharge of water flow into the streaming system include the reforestation and development of the system and DAM/reservoir construction. Forest replanting or reforestation is carried out by the people of Pujiharjo village and Perhutani. The installation of prohibition boards around the river was carried out by the village government Pujiharjo and Perhutani, both restrictions on the forest of sengon land and prohibition of throwing garbage in rivers.

Community Empowerment Through the River School Program

BPBD Malang district has been implementing the River school Program as an effort to empower the people of Pujiharjo village in accordance with the definition of empowerment from Narayan [17] "Empowerment is the expansion of assets and capabilities of poor people to participate in, negotiate with, influence, control, and hold accountable institutions that affect their lives". Community empowerment is widely used in disaster risk reduction approaches, identifying disaster prone areas, recognizing patterns that can lead to insecurity, and conducting mitigation activities. One form of community empowerment is the Program of the River School. The River School Program serves to stimulate or give stimulation to the important community to reduce the risk of flash flood impacts. There are three important definitions of the empowerment that Deepa Narayan expressed. Firstly, the empowerment of asset expansion and poor people capability. The poor people not only interpreted a group that is always weak and helpless, but they actually have assets and capabilities. With the empowerment activities will expand or expansion of assets and capabilities. As the people of Pujiharjo village who previously had the understanding that their residence is a disaster risk area, but this understanding should be balanced with the ability of society in the case of self-rescue when disaster event, such as disaster simulation training organized by BPBD Malang district.

Second, the expansion of assets and capabilities is moved and facilitated by promoting participation, negotiation, accountability and risk-sharing. In other words, the process of asset expansion and capability is done through a constructive mechanism or delivery system. In this case, the local government is BPBD Malang district, Dinas Pengairan, Dinas Cipta Karya, Bina Marga, PMI, Dinas Kesehatan has facilitated the community Pujiharjo village through the River School Program and provide an excavators help to help rapid dredging and normalization of streams. Although the idea of the River School is derived from BNPB, but according to Narayan [17] BPBD Malang district has the power of organizing the River School Program according to the needs of the people of Pujiharjo village.

Third, the focus of group empowerment affected by flash flood. The group has limited access to economic and political resources, after occurement of a flash flood in Pujiharjo village they will lose access to basic needs. River School Program is a community-based program, hence community empowerment is done with the participation of community related planning and implementation of the River School Program. The objective of empowering the community that Deepa Narayan delivered is the effort to move participation with the community in social sectors, economic and environmental outcomes that can be increase the Community's continued participation, welfare socio-economic independence, individual community groups and can preserve the environment as a life supports system.

The pattern of empowerment is carried out through various activities, such as the socialization of awareness and community involvement actively, either the community individually or collectively, colleges, Media, NGOS, civic organizations, and the parties including volunteers [13]. Community empowerment is associated with changes in behavioral patterns, it takes consistent and constant effort to make individual patterns of behavior change. The pattern of community empowerment in Pujiharjo Village is packed with River School Program. Through empowerment can be revived and developed social capital that has been rooted in the community Pujiharjo village that is mutual cooperation/togetherness, social solidarity, entrepreneurship, and family. Local wisdom that is characteristic of the community can be utilized to cope with disasters.

Access to information is as a means that the intervention of the Government in accordance with what is required by the community and what the community has so that it does not harm the community. In this study, the Government provided the assistance of the River School Program to the people of Pujiharjo village to normalize the Tundo river and Purwo river to avoid harm to the community. Assistance should be noted so that the helpless communities become dependent on the government.

In providing community assistance affected by the disaster, the government needs to implement the concept of empowerment because the community affected by the disaster actually has the power, but because it is affected by the disaster then as if the society is not empowered

Access this information including information about threats that exist around the community and further threats in the event of a disaster, such as a flash flood disaster, the continuation of the threat is a landslide. In this study, the flood of Pujiharjo village was accompanied by a further threat of landslides accompanied by mud and rocks derived from forests. Therefore, the organizing of the River school Program provided a vacuum cleaner by the government to clean the mud-mud that was in the home and school. People need access to information about where people should report, convey their needs, and know where to evacuate. The village chief of Pujiharjo informs the affected community to evacuate to a disastrous home or to evacuate to Pujiharjo village hall, so that people affected by the disaster feel safe. At the post-disaster stage, the village chief informs the River School Program to be followed by all the people both affected and unaffected.

Empowerment is a process based on the bottom up concept, where groups, communities, or individuals participate actively and are involved fully in the empowerment programs to create sustainable independence. The empowerment program in this study is the Sungai school Program, where the program involves the people of Pujiharjo village, Pujiharjo village device, BPBD Malang district, and related offices such as the Dinas Perhubungan, Dinas Pengairan, Dinas Cipta Karya, Pekerjaan Umum, TNI/Polri, and the business world. All elements of both society and government are actively involved and cooperate in the implementation of the River school Program.

The River School Program also has a bottom up concept where the community plays an active role in voicing necessary needs, such as bronjong, excavators or heavy equipment, mud-suction machines or diesel engines, and other basic necessities. The community is also involved in the planning meeting of the River School Program by representing 5 people per RT so that the results achieved are representatives of each RT can socialize the purpose of this river school Program to other citizens. This encourages the independence of citizens to be more creative when inviting other citizens to engage in the River School Program. The involvement and participation of the community shows that the community awareness of Pujiharjo village about its existence as individuals or members of the community and its environmental conditions (physical, social, cultural, economic, political) already exists. Involvement and participation of the community also conducted an alternative analysis of problem solving and chose the best alternative in the River School Program, namely involving people

Pujiharjo village not only youth and adults but children since participate in the River School Program.

Community involvement and participation can be categorized in two aspects, namely the cause and participatory aspects. The factors for the cause of the flood are: a) not throwing garbage into rivers; b) not construct buildings that obstruct or narrow the flow of rivers; c) not reside in the riverbank and make it a settlement; d) stopping deforestation in water catchment areas; e) cease agricultural and land use practices contrary to water and soil conservation, and f) to control the pace of urbanization and population growth. while participatory or contributing aspects of the community can reduce the impact of flash floods, include: a) participating and active in simulations or exercises (gladi) of the flash flood mitigation efforts through the River School Program; b) participate and active in the design and construction of flood-resistant houses, among others, home of the level, the use of water-resistant materials and water scours; c) participate in public education related to flash flood mitigation efforts; d) participate in every stage of public consultation related to the construction of flood control infrastructure such as plengsengan and bronjong; e) implement patterns and planting time that adapt the patterns and local flood conditions to reduce the loss of business and agricultural land from flooding through reforestation, and f) hold the mutual assistance of clearing the river from trash in the environment respectively.

Accountability further leads to agencies related to the implementation of the River School Program in terms of funding accountability, program implementation, and regulations in the Empowerment program. The River School Program is based on the MOU between BPBD Malang district and director of PRB in 2016, Technical Instruction of Disaster Risk Reduction Movement (Sekolah Sungai Indonesia), and DIPA Penguatan Kelembagaan for BPBD Malang in 2016. This River School Program fund comes from BNPB, which is included in ready-made funds. This is in accordance with the Law number 24 of the year 2007 on Disaster Management [19] on responsibility and authority in article 6e that allocating disaster management budget in the country's adequate income and expenditure budget and article 6f That allocating disaster management budgets in the form of ready-made funds.

Accountability is included in the evaluation of the River School Program which includes reviewing developments or changes occurring as a result of the River School Program, reviewing what objectives have been achieved and which have not been reached and identify why it happens and provide the information required in order to accountability to various stakeholders. This evaluation will be used for consideration, input, and advice for the next River School Program.

Organizing Capacity of Local Communities and Effectiveness of River School Programs

Community organizing according to Deepa Narayan [17] is a process when a particular community identifies its her needs and develops its belief to strive to meet that need, including the prioritization of These needs are adjusted to the available resources and with the effort of mutual assistance. The purpose of organizing the community is to build community power, strengthen the power of the base community, build a network and foster the confidence that they have the ability in disaster management.

Aspects of community organizing consist of the process, the community and the functioning of society. The process of organizing the community in the early stages is conducted by holding an internal preparatory meeting with BPBD Malang district as well as representatives of related offices of about 20 people. The internal preparatory meeting resulted in the location of the River School Program. The next stage is the socialization of the related SKPD, the village, sub-district, TNI/Polri and volunteers. Finally, the construction of the group is the establishment of the river in Pujiharjo Village by organizing the community. The purpose of this river Group is able to transfer knowledge about the river to the community as a whole in Pujiharjo village. The organizing of local communities has identified the needs of developing the school of rivers, including the committee of BPBD Malang district and tools and supporting facilities of the River School Program, as well as logistics to the participants and volunteers involved.

Flay [15] states that effectiveness focuses on the quality of implementation that will affect the outcome of a program. The quality of implementation of this river school Program can be determined by the achievement of programs. The effectiveness of the River School Program can be seen from two aspects [16] i.e. the first, the ability to solve problems. Based on the interview and observation of research, the River school Program has not been maximized in solving the problem of flash flood in Pujiharjo village. This is because the River School Program in Pujiharjo village is only done a day and does not reach the whole river so that only some parts of the river are normalised and there is a dispute about the citizens who do not want to be relocated.

Second, achievement of objectives. Based on a proposed proposal regarding the River School Program, the purpose of the River School Program is to change the behavior of people to care about the river. The results of observations in the field that the community without government assistance has a work agenda to install Netlon around the river independently and mutual cooperation. Although there are still some residents who throw garbage in the river, but the rivers in Pujiharjo village began to be cared for well, one of them with bamboo planting around the river banks.

The River School Program must continue as learning for people living around the river. The rivers in Pujiharjo village are small rivers but have very large damaged power. The River School Program will be effective in trying to reduce the flood riisko when done consistently and continuously in one village, both downstream (river) and upstream (forest) repairs. Efforts are made by the safety of a hard crop, such as a coffee tree. Although the community grows bananas but there must be a tree-lined plant. The River school Program can not be done once but continuing to the river and the forest Pujiharjo village is good condition. The River School Program will not be maximized if the environment in the upstream area is not repaired, namely forest in Pujiharjo village. Therefore, there must be continuity between upstream and downstream.

Recommendations

Mitigation requires socialization and training on changes in community mindsets regarding the pattern of the development of rivers with normalization, the manufacture of side dikes, wall-casting, and wall-hardening that turns damage to the river ecosystem. Artificial beater and a small pond to accommodate the rainwater in the settlements and the manufacture of natural catchment wells to avoid the flow of rainwater runoff immediately downstream. The River School Program for the people of Pujiharjo village is not only implemented after a flash flood occurred but in the cycle of disaster management. The River School Program can be held before the disaster occurs as a mitigation effort for both structural mitigation and non-structural mitigation.

Community empowerment with the River School Program needs a social understanding of the problems relating to its liquidity and its conservation, namely the linkage between the upstream and downstream areas, waste-and flooding, the logging of trees/forest and flood. It is necessary to mass awareness of the people of Pujiharjo village to the importance of DAS through an intensive and continuous social learning process. In principle, by expanding the chance of rain water can be absorbed naturally into the soil before entering the river or flowing downstream.

The effectiveness of the River School Program has several obstacles, supposedly of the River School Program focus is implemented in one location namely Pujiharjo village with a short-term and long-term River School concept, so that the results can be felt In the environment condition of Pujiharjo village. The focus of public assistance is no longer food and clothing needs when the flash floods are crashing back, but the repairs of the Tundo River and Purwo rivers as well as damaged forest conditions.

For BPBD Malang district, the handling of flash flood in Pujiharjo village can not be done partially but must be overall because the environment of rivers and forests are damaged, it is necessary to reforestation and the prohibition of mass logging in upstream areas. The River School Program in Pujiharjo village is only carried out around the river.

For Pujiharjo village government, the implementation of the River School Program in order to be included in Rencana Pembangunan Jangka Menengah Daerah (RPJMD), the sustainability of the River School Program in Pujiharjo village continues to be done until the return of hydrological function Tundo river ecosystem and Purwo river and forest in Pujiharjo village.

For the government of Malang district, it is necessary to develop a contingency plan of village, especially located far from the district capital, the inventory of countermeasures necessary in the case of emergency, such as an excavators or heavy equipment, boats evacuation routes or signs to give warnings to the public. Need to be increased synergity between the institution and the related service namely Dinas Pekerjaan Umum, Perhutani, Dinas Perhubungan, and Dinas Pertanian to deal seriously the condition of forests and rivers are damaged.

4. Conclusion

Disaster mitigation that has been performed both structural mitigation and non-structural mitigation is able to reduce the impact caused by flash floods. Although the goal of mitigation has not been fully achieved is to avoid risk but the people of Pujiharjo village can reduce the chances and consequences of risk, accept the risk by making efforts anticipate the impact of disasters. Structural mitigation that has been done is strengthening the building by raising the house up to 2 meters to avoid water inside the house, build a flood retaining construction that is installing netlon and plengsengan around the river so that water the river is not crashing into settlements. While the non-structural mitigation is avoiding disaster areas by means of development that is away from the location of disaster, namely Pujiharjo village people who live in the river, many of which move their house away from the river, empowerment efforts local government through the River School Program.

Community empowerment both as individuals and society as a whole can play a significant role in the flood disaster management which in the study aims to mitigate the impact of the flood disaster and able to Increase disaster mitigation capacity for Pujiharjo village community. The River School Program held in Pujiharjo village has not been effective in reducing the risk of flash flooding. This is due to the limited implementation of the River school Program and time. Heavy equipment limitations in the implementation of the River School Program because of the location of Pujiharjo village away from the district capital. The operation time of the River School Program which is only a day makes installation of netlon is not maximal and not thorough. The handling of the River school Program only focuses on the handling of rivers, but the handling of upstream forests is also important improvement. Some obstacles that affect the quality of implementation of the River School Program, namely the distribution of volunteers on the net point of the river is uneven, not all volunteers understand what will be done in the river, some point of shortage of netlon and planting trees can not be done synchronously.

References

[1] Delia, Miftode Iona. 2015. Hazards, Vulnerability and Associated Hydrological Risks in the Hydrographical Basin of The River UZ, Tributary of the River Trotus. Romania: Cluj University Press

[2] Anwar, Herryzal Z & Harjono, Hery. 2013. Menggapai Cita-cita Masyarakat Tangguh Bencana Alam di Indonesia. Bandung: Lipi

[3] Data Indeks Bencana Indonesia. Online Available at http://dibi.bnpb.go.id/data-bencana/lihat-data/per-halaman=10;halaman=1

[4] Borga, et al. 2011. Flash Flood Forecasting, Warning and Risk Management" the Hydrate Project. India: Journal: Environmental Science a Policy. Vol.14. B34-B44

[5] Suprayogi, Slamet, dkk. 2013. Pengelolaan Daerah Aliran Sungai. Yogyakarta: Gajah Mada University Press

[6] Darmono, Bambang. 2010. Keamanan Nasional: Sebuah Konsep dan Sistem Keamanan bagi Bangsa Indonesia. Jakarta: Sekjen Wantanas

[7] Eko, Sutoro. 2002. Pemberdayaan Masyarakat Desa, Materi Diklat Pemberdayaan Masyarakat Desa, yang diselenggarakan Badan Diklat Provinsi Kaltim, Samarinda, Desember, 2002

[8] Asian Disaster Preparedness Center.2008. Cpmmunity Empowerment and Disaster Risk Reduction in Chittagong City. Online Available at www.adpc.net/igo/contents/Publications/?tagDoctype=19...Technical%20Papers *diakses pada 6 Oktober 2017 Pukul 20.00 WIB*

[9] Lamond, Jessica, dkk (2013). Cities and Flooding: Lessons in resilience from case studies of integrated urban flood risk management. Australia: Queesland University

[10] Widati.2016. Menggerakkan Partisipasi Masyarakat Kawasan Sungai Menuju Pemberdayaan Berkelanjutan: Yogyakarta: Universitas Negeri Yogya

[11] Usman, Sunyoto. 2015. Esai-esai Sosiologi Perubahan Sosial. Yogyakarta: Pustaka Pelajar

[12] Hidayat, Arif Fuad. 2016. Menggerakan Relawan dan Stakeholder Untuk Gerakan Sungai dan Gerakan Restorasi Sungai

Yang Berkelanjutan di Klaten untuk Indonesia. Klaten: Modul Sekolah Sungai

[13] Kusumasari, B. 2014. Manajemen Bencana dan Kapabilitas Pemerintah Lokal. Yogyakarta: Gava Media

[14] Alfitri. 2011. Community Development. Teori dan Aplikasi. Yogyakarta: Pustaka Pelajar

[15] Flay, Brian R. Gottfredson, Denise, Valentine, Jeffrey C, Biglan, Anthony, Boruch, Robert F. Kellam, Sheppard, & Ji, Peter. 2005. Standards of evidence: criteria for efficacy, effectiveness and dissemation. Journal of prevention science, 6 (3). 151-175

[16] Sukmaniar. 2007. Efektivitas Pemberdayaan Masyarakat dalam Pengelolaan Program Pengembangan kecamatan (PPK) pasca tsunami di Kecamatan Lhoknga Kabupaten Aceh Besar. Tesis. Program Pasca Sarjana Universitas Diponegoro, Semarang

[17] Narayan, Deepa. 2002. Empowerment and Proverty Reduction: a Source Book: Washington DC: World Bank

[18] Putuhuru, Ferad. 2015. Mitigasi Bencana dan Penginderaan Jauh. Yogyakarta: Graha Ilmu

[19] Undang-Undang Nomor 24 Tahun 2007 tentang Penanggulangan Bencana

KENTONGAN AND WHISTLE: COMPLEMENTARY SIMPLE TECHNOLOGY FOR MODERN TECHNOLOGY IN THE PERIOD OF DISASTER EMERGENCY RESPONSE

Sunu Tri Yuana[1] and Dian Andi Nur Aziz[1,2]

[1]Indonesia Defence University, Indonesia Peace and Security Center, Bogor, 16811, Indonesia
[2] National Human Rights Commission of Indonesia, Jalan Latuharhary No. 4B, Menteng, Jakarta, 10310, Indonesia

*Corresponding author: sunutriyuana47@gmail.com

Abstract

Effective communication is key in the emergency response period. Standards for managing countermeasures in the emergency response phase are carried out by disseminating disaster warning information to reduce disaster risk. In general, in a disaster emergency response modern technology cannot function due to cessation of electricity supply, loss of internet signals and the stuttering of society towards modern technology. Information and disaster emergency communication cannot be disseminated properly. This article describes the use of bells and whistles during the emergency response period. This study uses a qualitative descriptive method with secondary data. This article concludes that kentongan and whistle qualify as technologies that can be used to complement modern technology in the emergency response period. Kentongan has become a tradition in the culture of Indonesian society. Kentongan is a means to disseminate information through the beat of a punch with the meaning of each that has been agreed upon by the community. A whistle is a device that produces high frequency sounds so that it can be heard in a wide radius. Whistle can be a personal item in the emergency response period.

1. Background

Indonesia is a disaster-prone area. Indonesia's National Disaster Management Agency (BNPB) noted that in 2018 there were 1,999 disaster events in Indonesia. The number of dead and missing victims reached 3,548, the injured number reached 13,112. As many as 3.06 million people were displaced and affected by the disaster 339,969 houses were severely damaged, 7,810 moderate damaged houses, 20,608 lightly damaged houses, and thousands of damaged public facilities [1].

Disasters can be grouped into natural disasters, non-natural disasters, and social disasters. Disasters cause suffering for humans and other living beings. Disasters also cause natural damage, among others, earthquakes, tsunamis, volcanic eruptions, floods, droughts, hurricanes, and landslides. Non-natural disasters, including, include technological failures, failed modernization, epidemics, epidemics. Social disasters, including, include social conflict between groups or between community communities, and terror. There are six most frequent disasters in Indonesia, namely earthquakes, forest fires and buildings, tsunamis, floods, landslides and volcanic eruptions (Article 1 of Indonesia Law No. 24 of 2007 concerning Disaster Management).

Preparedness actions, early warning and disaster mitigation are carried out to prevent and reduce fatalities and material losses due to disasters. Preparedness is an action taken to ensure a fast and appropriate effort in dealing with disasters. Early warning is taking quick and appropriate actions to reduce disaster risk and preparing emergency response actions. Mitigation is a pre-disaster activity carried out to reduce disaster risk for communities in disaster-prone areas[2].

An early warning system using modern technology has been developed. For example, the initial sensor device is very sensitive to environmental changes and the initial symptoms of natural disasters. Information from the sensor is forwarded to an alarm in the form of sirens and the like. Emergency response information is captured by people around him. Furthermore, steps are taken that are quick and swift to save themselves to reduce the risk of being hit by a disaster.

Modern disaster detection devices and early warnings usually require electricity as an energy source, and internet signals to control them automatically. These tools also require sufficient levels of competence and skills to operate them.

The territory of Indonesia is very wide, spread from Sabang to Merauke. Not all regions have emergency response tools such as sirens. Likewise, remote areas and remote areas that are prone to natural disasters. A large budget is needed for the regular purchase and maintenance of these tools.

The internet network in remote areas prone to disasters is very limited. Internet network devices rely on very limited electricity supply. Internet network constraints have caused modern disaster technology to not reach all disaster-prone areas in Indonesia. Other technologies are needed to complement modern emergency response technology.

2. Theoretical framework

2.1. Disaster

Disasters are natural events or events resulting from unusual human hands. Disasters can also be due to technological system failures that weaken responses from human communities, individual groups or the natural environment. Disasters cause major damage, economic loss, destruction, injury and or death [3].

2.2. Preparedness

Preparedness includes the following activities [4]:

- Formulation, testing, and training in planning to deal with disasters;
- Training for disaster-affected communities and the general public;
- Development of communication with the public and others about the vulnerability of disasters and actions that must be taken to reduce them;

In disaster management there are several reasons that cause preparedness to be considered a very important component [4], namely:

- Effective response and preparedness activities can help save lives, reduce injuries, limit property damage, and minimize all kinds of disturbances that can be caused by disasters;
- Preparedness helps protect community values and reduces unwanted conditions during disasters;
- Preparedness improves coordination and communication between organizations and establishes responsibilities for key players, such as community officials, state officials, regional and hospital officials;
- Preparedness helps identify resources (personnel, time, finance, equipment, equipment or facilities) that may be needed by the community for the steps of response and recovery activities;
- Preparedness identifies several important functions that need to be carried out during a disaster, such as resource management, evaluation, and damage assessment.

2.3. Local Wisdom

Local wisdom and culture according to I Ketut Gobyah are truths that have been tradition or steady in an area. Local wisdom is a combination of the sacred values of God's word and various values. Local wisdom is formed as a cultural superiority of the local community as well as geographical conditions in a broad sense. Local wisdom is a product of the past culture that should be continuously taken into account in life. Although it is of local value, the values contained in it are considered to be very universal.

Local wisdom is a system of values and norms that are compiled, adhered to, understood and applied by local communities based on their understanding and experience in interacting with their environment [5].

2.4. Mitigation

Mitigation is actions aimed at reducing the impact of disasters on the community, namely the soul, property, and infrastructure. In terms of time, mitigation actions are almost similar to preventive actions [6].

3. Discussion

3.1. Kentongan.

Kentongan is a sound instrument that comes from bamboo or hollow wood which can produce sounds by being hit using repeated wooden sticks to declare a time mark or danger sign or a way to gather mass (Indonesian Dictionary). *Kentongan* or the connection with the sound of "*thung, thung*" (Javanese), made of wood or bamboo with different lengths in the middle there are grooves / elongated cavities [7]. Each pattern of *kentongan* punch frequency means. People who hear know what events are happening and what needs to be done.

Kentongan is very well known by the people in Java. *Kentongan* is a local wisdom product, especially the Javanese people. *Kentongan* will be beaten if there are emergency events involving the safety of the inhabitants' lives in their environment.

Lately, *kentongan* as a traditional communication tool has rarely been found. *Kentongan* is a part of local wisdom is an effective instrument in delivering messages immediately to the general public. Realizing this, the Special Region of Yogyakarta Government issued the Instruction of the Governor of Yogyakarta Number: 5 / INST / 1980 dated May 26, 1980 concerning the sound of the *kentongan*.

Table 1. The sound of the *kentongan* based on Instruction of the Governor of Yogyakarta Number 5/INST/1980

Situation	Sound	Meaning
Safe situation	-----V----- (one-time grandiose doro)	The situation is safe or the situation is safe again
Ready/alert state	00.00.00, etc. (two two)	The possibility of natural/crime occurring; vague/suspicious situation; be prepared
Special crimes	000.000.000, and so on (three-three)	There is theft of buffalo, cow, horse, etc.; there is a theft of communication devices; there is ordinary/light theft
Great crime	0000000.0-0000000.0-0000000 (seven *beats plus one)*	There is a raid (robbery); theft with resistance; there is clipping/mugging; there is murder; there is a mugging by motorcycle/motor vehicle

Natural disasters	00000000 (*gobyok* / *titir*)	There is an ordinary flood/cold lava; there is a hurricane/noise; there is a fire; there are landslides; there is a volcano erupting; there are wild animals
Dead	-----V-----,-----V-----(grandiose doro 2 times)	there are people who die

3.2. Whistle

A whistle is a small wind instrument in which sound is produced by the forcible passage of breath through a slit in a short tube, that makes a loud noise when blown. The purpose of whistle is to send, bring, signal or call by or as if by whistling [8]. Whistles are generally oval shaped with small holes at the top for air circulation. The whistle is also termed a simple air aero phone, because it produces sound from forced air flow. In the past twhe whistle was made of wood, plastic, metal, aluminium and silver. Now more whistles are made of plastic.

The benefits of the whistle are very many. Whistles are often seen being used by referees in soccer matches or police traffic control vehicles to break down traffic. The whistle is used as an emergency blow on the ship to find the position of victims of ship accidents at sea. Survival victims at sea use whistles available in emergency lifeboats and life craft to ask for help. When the victim had been floating in the sea for a long time, the energy was drained due to logistical limitations, so the victim used a whistle to tell his position.

Whistle is also used in youth activities such as scouts for various purposes. In scouting, whistle signs follow the following pattern:

Table 2. The sound of whistle signs in scouting

Situation	Sound	Meaning
A sign of concern	____________________ (long blow is not interrupted)	A sign of attention, a sign of silence, a sign of being prepared
Gathering signs	- - - - - - - - - - - - - - - and so on (continuous short bursts)	Sign to gather

Signs scatter	— — — — — — — and so on (broken long bursts)	When you hear these sounds all people move apart
Danger sign	— – — – — – — – — and so on (long puffs then short alternately continuously)	Community members who hear the sound in order to increase alertness because of the danger in the area that is heard blowing
Call sign from team leader	— – —— – – – —— – – – —— – – – – – – – – (for three short puffs, one time three lengths)	Those who listen please convey to the team leader to approach the whistle blower

Kentongan and whistles can be said to meet emergency response technology standards. *Kentongan* and whistle are simple technologies that are important to complement modern equipment for early warning and disaster response. Disasters cannot be predicted when they will occur. Disasters can come suddenly. When disasters come, the potential damage to early warning equipment and emergencies can occur in various infrastructures including modern early warning and emergency equipment. Disasters can damage need to prepare backup equipment as a supplement.

Aftershocks often occur. Repairing and restoring public infrastructure such as electricity and roads requires time including early warning instruments. In this situation, anticipation will continue as long as the early warning infrastructure cannot be used. For example, electricity recovery in the earthquake and tsunami disaster in Central Sulawesi in 2018 took months [9].

Kentongan and whistle are simple technology that is effective to complement modern technology. Several ways can be done so that the kentongan and whistle can be part of the emergency response and disaster emergency. *Kentongan* and whistle need to be preserved in civil society as part of disaster mitigation. Training on the use of kentongans and whistles in disaster management in Indonesia needs to be done periodically. Disaster awareness and emergency response measures must be grown in the community. It is necessary to socialize the benefits of *kentongan* and whistle as important information and communication tools in disaster emergencies to the people of Indonesia. The main target is the younger generation and residents in disaster-prone areas.

To complete the disaster warning siren, bamboo sticks (mini kentongan) are a warning tool in people's homes. Kentongan in strategic offices and public spaces such as police stations, residential observation posts, and public offices. The whistle itself is used as a complement to each individual who is personal.

Kentongan has warned residents ahead of the tsunami. At the end of October 2010, a large earthquake occurred in the Mentawai Islands. The houses in one of the villages in South Pagai Subdistrict were destroyed on the ground, but the residents survived the tsunami hit. They saved themselves in the direction of the hills after the tribal chief sounded *kentongan*. The sound of kentongan signals all citizens about the arrival of the tsunami and gives orders to save themselves [10].

One of the principles of response to disasters is communication. Communication in emergency response situations must be accurate and effective. But in an emergency situation there are generally obstacles. To overcome these difficulties, it is necessary to prioritize the use of tools and findings from local initiatives. Of course, as long as it meets the standards of effective communication (Moore, 2008: 118) [11].

The experience of surviving one of the residents from the tsunami in the Mentawai Islands is proof that the *kentongan* is culturally acceptable. They use this simple tool for various purposes. One of them is a warning about the arrival of a tsunami. *Kentongan* has become part of emergency response technology in disaster.

4. Conclusion

Kentongan is a simple technology that has become part of local traditions in several regions in Indonesia. This technology can be culturally acceptable. *Kentongan* fulfils the requirements to be used to give a warning sign of culture. The use of *kentongan* can complement modern technology in the emergency response period.

Whistle is a simple tool that has been received in several community activities. Whistle is a tool that can complement modern technology in the emergency response period. Whistle can be a personal equipment in saving yourself in the event of a disaster.

Kentongan and whistle need to be socialized to the community. Continuous training in order to foster awareness of disaster response. Warning from danger signs from *kentongan* and whistle can be a deterrent to the casualties caused by the disaster.

Acknowledgements

Authors wishing to acknowledge assistance or encouragement from the Indonesian Defense University's Peace Study and Conflict Resolution Program and the Indonesian Defense University Disaster Management Study Program.

References

[15] "BNPB: Selama 2018 Ada 1999 Kejadian Bencana", *www.kompas.com*¸ accessed by Mei 31, 2019

[16] Badan Nasional Penanggulangan Bencana Indonesia 2017. Buku Panduan Kesiapsiagaan Bencana

[17] Parker, D 1992 *The Mismanagement of Hazards – Hazard Management and Emergency Planning; Perspective on Britain* (London: James & James)

[18] Mileti, D S 1991 *Disaster by Design: A Reassessment of Natural Hazards in the United States* ((Washington.D.C: Joseph Henry Press)

[19] Tjahjono. 2000 *Pola* Pelestarian Keanekaragaman Hayati Berdasarkan Kearifan Lokal Masyarakat Sekitar Kawasan TNKS di Propinsi Bengkulu dalam Prosiding Hasil Penelitian SRG TNKS . Kehati. Jakarta

[20] Kodoatie, Robert J., dan Sjarief Roestam 2006. *Pengelolaan Sumber Bencana Terpadu – Banjir, Longsor, Kekeringan dan Tsunami*. Jakarta

[21] Sumiyati, F 2007 *Makna Lambang dan Simbol Kentongan Dalam Masyarakat Idonesia,* Jurnal Lembaga Penelitian dan Pengabdian kepada Masyarakat. Vol 21 no 2 Oktober 2007

[22] Webster Merriam. Dictionary (https://www.merriam-webster.com/dictionary/whistle) accessed by Mei 31,2019

[23] Jokowi Sebut Pemulihan Listrik Akibat Gempa Palu Butuh Waktu Lama", *https://nasional.tempo.co/read/1132559/jokowi-sebut-pemulihan-listrik-akibat-gempa-palu-butuh-waktu-lama/full&view=ok*, accessed by Mei 31, 2019

[24] "Bunyi Kentongan Kepala Suku Selamatkan Warga Sekampung dari Tsunami", *https://www.republika.co.id/berita/breaking-news/nusantara/10/11/01/143654-bunyi-kentongan-kepala-suku-selamatkan-warga-sekampung-dari-tsunami*, accessed by Mei 31, 2019)

[25] Moore, Tony 2008 *Disaster and Emergency Management Systems* (London: Bristish Standars Institution)

OPTIMIZING THE ROLE OF TAGANA IN THE MANAGEMENT OF NATURAL DISASTER THREATS IN INDONESIA

Ryaniraffiyadita

Indonesia Defense University

*Corresponding author: ryaniraffiyadita@gmail.com

Abstract

Disasters that occur in Indonesia are one of non-military threat that caused by many factors. In dealing with natural disasters, several problems were found. One of the agencies that responded to this problem was Indonesia Social Ministry through the Disaster Preparedness Cadets (TAGANA) program. This research is descriptive qualitative with data collection techniques are using observation techniques, interviews with the Minister of Social Affairs and literature related to the TAGANA program. This study aims to: (1) Know how the appropriate disaster management process; (2) knowing the role of TAGANA in natural disaster management; (3) Knowing the development of TAGANA in Indonesia. The results of the study found that TAGANA was a social volunteer who came from a community that was caring and active in disaster management in the field of social protection. The member of TAGANA in Indonesia still does not fulfill the needs of volunteer so that it still has to be increased in quantity and quality through the recruitment of Friends of TAGANA and updated training. Consistency and community participation through Tagana must be maintained by including Tagana in various stages of disaster management. With that, natural disaster management efforts will be more responsive.

1. Preface

The development of a dynamic strategic environment and context brings changes to the spectrum of threats that have implications for national defense. The complexity of threats is classified into a multidimensional type of threat in the form of military threats, non-military threats and hybrid threats that can be categorized in the form of actual and potential threats. Thus, future national defense requires integration of military defense and non-military defense through efforts to build strong and respected national defense forces and capabilities with high deterrence power.

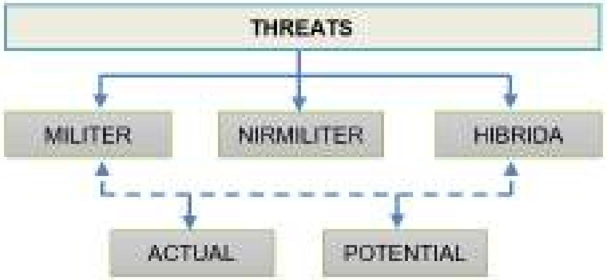


Figure 1. Threats in Indonesia (Indonesian Defense White Paper 2015)

Military threats that threaten the NKRI are in the form of Aggression / Invasion, Regional Violations, Espionage, Sabotage, Armed Terror Action, Threats of Sea or Air Security, Civil War or Communal Conflict. This attention to non-military threats and vulnerabilities is also a special concern in Indonesia. The Indonesian Minister of Defense, Ryamizard Ryacudu, stated that there were eight manifestations of non-military (asymmetric) threats in the context of state defense, including: 1) Terrorism; 2) Natural Disasters; 3) Border Violations; 4) Separatism; 5) Infectious Diseases; 6) Cyber Attack; 7) Narcotics; and 8) Cultural Infiltration. In addition, the Ministry of Defense of the Republic of Indonesia through the 2015 Indonesian Defense White Paper has also suggested that the distribution of threats is currently divided into three: military, non-military and hybrid threats. Sources of threats can come from within and outside the country, and are carried out by state and non-state actors, which are national, regional and international. The impact caused includes all aspects of social conditions such as ideology, politics, economics, socio-culture, defense, and security. [1]

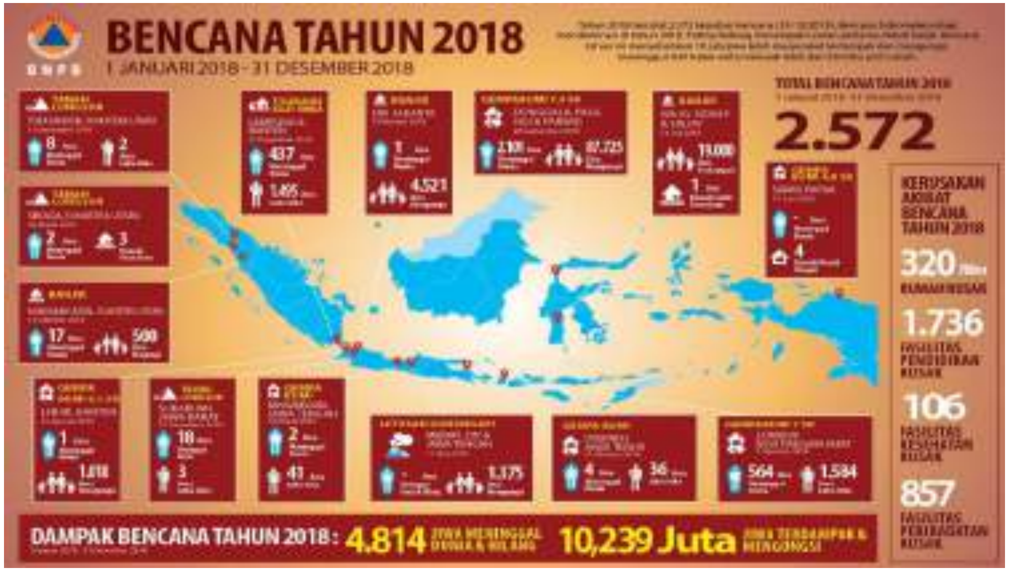

BENCANA TAHUN 2018
1 JANUARI 2018 - 31 DESEMBER 2018
TOTAL BENCANA TAHUN 2018
2.572
KERUSAKAN AKIBAT BENCANA TAHUN 2018
320 ribu
RUMAH RUSAK
1.736
FASILITAS PENDIDIKAN RUSAK
106
FASILITAS KESEHATAN RUSAK
857
FASILITAS PERIBADATAN RUSAK
DAMPAK BENCANA TAHUN 2018:
4.814
JIWA MENINGGAL DUNIA & HILANG
10,239 Juta
JIWA TERDAMPAK & MENGUNGSI

Figure 2. 2018 Indonesia Natural Disaster Data from the Ministry of Social Affairs of Indonesia

Throughout 2018 there were 2,572 disasters recorded. Hydrometeorological disasters dominate in 2018. Tornado winds ranks first followed by floods. Last year's disaster left 10 million more affected and displaced people, claimed 4,814 lives and damaged more than 320 thousand housing units. [2]

Disasters are a series of events that threaten people's lives either caused by natural factors and / or non-natural and human factors which result in human fatalities, environmental damage, property losses, and psychological impacts.[3] While disaster management is one way to reduce the very detrimental impacts of a disaster threat, the activities carried out are disaster prevention (before a disaster occurs), emergency response (when a disaster occurs) and rehabilitation (post-disaster).

The disaster management process regulated in Law Number 24 of 2007 concerning Disaster Management still has weaknesses, namely weak coordination in disaster management. [4] The results of observations made after the tsunami disaster in Palu on September 28, 2018, the tsunami in Banten on December 22, 2018 and the landslide natural disaster that hit the Cisolok area, Sukabumi on January 1, 2019 showed that there was still a lack of natural disaster management in Indonesia. Inadequate disaster management can be caused by a lack of volunteers who assist the emergency response and post-disaster response processes. Disasters that occur suddenly, massive, and must be dealt with quickly require relevant parties to be able to move more agile in the disaster management process so that the number of disaster victims can be minimized.

Pearce (Djalante et al., 2011) suggests that planning and managing sustainable disaster hazards can only be achieved through community participation in disaster management.[5] In disaster management management systems, communities have the same responsibilities as other national components. Therefore the community has an obligation to actively participate in the disaster management process. This participation was demonstrated by the establishment of the Disaster Preparedness Cadets (Tagana) as a manifestation of community participation in the disaster management process.

The explanation above can be concluded that the role of the community is an important factor in overcoming the threat of natural disasters. The Ministry of Social Affairs through the Directorate General of Social Assistance and Security seeks to improve the role of this community by forming the Disaster Preparedness Cadets (Tagana). According to Article 1 paragraph (1) Regulation of the Minister of Social Affairs of the Republic of Indonesia (Permensos RI) No. 29 of 2012 concerning Tagana, stating that Tagana is a trained social volunteer or Social Welfare Worker (TKS) from a community that is concerned and active in disaster management. Tagana was formed on March 23, 2004. In this study will be discussed (1) How is the appropriate disaster management process; (2) Roles and functions of TAGANA in disaster management; and (3) the development of TAGANA in Indonesia in the face of the threat of natural disasters.

2. A section of your paper

This research method uses qualitative methods. The data used was data derived from primary and secondary data. The primary data was the result of an interview with the Minister of Social Affairs of the Republic of Indonesia which issued a regulation on Tagana formation in public lectures to Marine Strategy Study Program Students, Applied Master Program Dikreg Seskoal January 22 2018. While secondary data was collected from literature books, journals, research reports, seminar materials, legislation obtained through printed material or electronic material that examines disaster management, community participation in disaster management and which examines the Disaster Preparedness Organization (Tagana).

3. Result and Discussions

3.1. Disaster Response

Management is all efforts carried out in activities including prevention, taming (mitigation), rescue, rehabilitation and reconstruction activities, both before a disaster, during a disaster and after a disaster and avoiding a disaster. So it can be concluded that disaster management is not only at the time of a disaster (disaster response) or after a disaster (post-disaster), but also before a disaster occurs (pre-disaster) disaster management needs to reduce disaster risk. The importance of the implementation of disaster management has a goal, among which has been stated in Law Number 24 of 2007 Article 4 :

a. Providing protection to the community from the threat of disaster
b. Align existing rules
c. Ensure the implementation of disaster management in a planned, integrated, coordinated and comprehensive manner
d. Respect local culture
e. Building public participation and partnership privately
f. Encouraging the spirit of mutual cooperation, solidarity and generosity

Carter (2008) defines disaster management as an applied science that seeks, with systematic observation and disaster analysis to improve measures related to preventive, mitigation (reduction), preparation, emergency response, recovery and rebuilding. The objectives of disaster management include reducing or avoiding physical, economic and mental losses experienced by individuals, the public, reducing the suffering of victims, accelerating recovery, and providing protection to refugees or communities who have lost their place when their lives are threatened.

There are 3 stages of conducting disaster management, namely the pre-disaster stage, the phase of emergency response and the post-disaster phase. These three stages have different objectives and activities which are included in the following [6]:

a. Pre-Disaster Phase

The purpose of this stage is to reduce property losses and human casualties caused by hazards and ensure that losses can also be minimized when a disaster occurs. Activities in the pre-disaster phase include 3 things:

1) Prevention; efforts to eliminate or reduce the possibility of a threat.

2) Mitigation; efforts that made to reduce the adverse effects of a threat.

3) Preparedness; preparation of a plan to act when a disaster occurs (or is likely to occur). Planning consists of estimates of needs in an emergency and identification of existing resources to meet

those needs. This plan can reduce the adverse effects of a threat.

b. Stage of Emergency Response

The purpose of this phase is to help affected communities immediately to be immediately fulfilled their most minimal basic needs. The main target of this emergency response phase is humanitarian rescue and relief. In this emergency response phase, efforts are also made to settle decent temporary shelters, as well as to regulate and distribute logistics quickly and precisely to all disaster victims.

Operationally, in the emergency response phase it is directed at activities: 1) Handling disaster victims including burying dead victims and handling injured victims 2) Handling refugees 3) Providing emergency assistance 4) Health services, sanitation and clean water 5) Preparation of shelter temporary 6) Construction of social facilities and temporary public facilities and improving basic facilities and infrastructure so as to be able to provide adequate services for victims.

c. Post-Disaster Phase

Post-disaster response includes two main stages, namely, rehabilitation and reconstruction.

1) Rehabilitation

The purpose of this stage is to restore and restore the functions of buildings and infrastructure that are urgently needed to follow up on the emergency response phase, such as rehabilitation of religious buildings, school buildings, basic social infrastructure, and economic infrastructure and facilities that are very necessary. The main objective of this rehabilitation phase is to improve public services to an adequate level. In this rehabilitation phase, efforts are also made to solve various problems related to psychological aspects through handling trauma from disaster victims.

2) Reconstruction

The purpose of this stage is to rebuild the disaster area by involving all communities, representatives of non-governmental organizations, and the business community to be able to build damaged infrastructure and facilities, as well as public facilities with the aim that people's lives will return to normal. The main objectives of the reconstruction phase are the growth of economic, social and cultural activities, the upholding of law and order, and the rise of the role and participation of civil society in all aspects of community life in post-disaster areas. Logistical assistance is carried out by adhering to a variety of institutions / Institutions in the institutional system in various regions that are implemented in an integrated manner include national, provincial and district / city. Each level of institution in carrying out PB logistical assistance uses a logistical assistance mechanism, which at each level has special characteristics in accordance with the level of authority.

3.2 TAGANA.

The Responding to the design of a community-based disaster management system, the Ministry of Social Affairs held a meeting with humanitarian activists in Lembang, March 25, 2004. From this meeting, a Humanitarian Volunteer Organization which was concerned and active in disaster management was named TAGANA (Disaster Preparedness Cadets) To equalize the perception and capabilities of Tagana in Indonesia, PB Cibubur National Jamboree was held. Not only arrived there, the development of Tagana's capacity throughout Indonesia continued to be improved through trainings by the Central Government and the Regional Government in order to obtain strong and quality Tagana.

According to Permensos No.29 of 2012 concerning Disaster Preparedness Article 1 that Disaster Preparedness Cadets, hereinafter abbreviated as TAGANA, are social volunteers or Social Welfare Personnel from communities who are concerned and active in disaster management in the field of social protection. The purpose of the formation of TAGANA is to utilize and empower the younger generation in disaster management.

Tagana collects all the strengths of the component of community-based disaster management, especially from the younger generation who are fostered and developed by the Ministry of Social Affairs of the Republic of Indonesia intended to respond to the challenges of the times and change from the disaster management paradigm from responsive to preparedness. To answer this challenge, the social institutions in each province, district / city to develop the TAGANA membership in stages include the following:

a. TAGANA Muda, is TAGANA members who have taken basic training, are experienced in disaster management;
b. TAGANA Madya, is a member of TAGANA who has participated in training and stabilizing middle level disaster management, experienced, and has special skills in disaster management;
c. TAGANA Utama, is TAGANA members who have participated in training, primary level stabilization, and have special skills and have experience in disaster management both regionally and nationally.

3.2. Roles and Functions of TAGANA in Indonesia.

TAGANA has the task of assisting the Government and regional governments in implementing disaster management both during disaster, during emergency response and post-disaster as well as the tasks of handling other social problems related to disaster management. In carrying out the tasks referred to in Article 5, TAGANA has functions at the time of pre-disaster, emergency response; and post-disaster. [7]

TAGANA candidates are recruited by Regency / City Social Services / Agencies or Provincial Social Services / Agencies. Derived from individuals, both from community groups and sent or delegates from social organizations. The requirements for a TAGANA are male and female Indonesian citizens, aged between 18 (eighteen) years and 45 (forty five) years; and physically and mentally healthy. Prospective TAGANA must follow and be declared to have passed TAGANA basic stabilization.

The function of TAGANA consists of: a) Prevention function, which is to inhibit and or limit the growth and development of problems or needs experienced by victims and their social environment; b) Function of Development or empowerment, namely to develop the ability, motivation, and role of the victim and his social environment; c) Function of Rehabilitation, namely solving problems or meeting needs and restoring and improving the status and social role of victims and their social environment in community life; d) Protection Function, which guarantees every citizen to avoid various catastrophic events that cause it, experience various problems; e) Supporting Functions, namely to support the successful implementation of other sector / sector related disaster management programs.

3.4 The Development of TAGANA

TAGANA is a social volunteer who has concern and is active in disaster management. Tagana comes from a community that has concern and is active in disaster management in the field of social protection. Tagana is a manifestation of disaster management in the field of community-based social assistance.

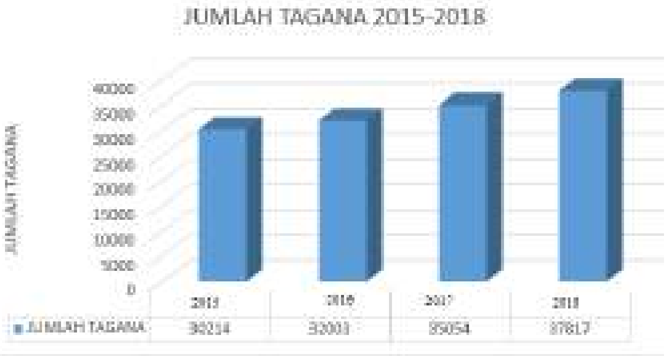


Figure 3. Increasing the Number of Tagana 2015 to 2018

The Ministry of Social Affairs Indonesia noted that the number of cadets in disaster preparedness (Tagana) in Indonesia has increased from year to year in 2015 the number of Tagana reached 30,214 people consisting of 520 Tagana Madya and 29,694 Young Taganas . In 2016 there was an increase to 32,003 people consisting of 720 Tagana Madya and 31,283 Young Tagana. In 2017 the number of Tagana increased to 35,054 people and in 2018 it increased to 37,817 with details of Tagana Madya as many as 660 people and Tagana Muda as many as 37,157 people.

In order for each TAGANA Personnel to have a function in accordance with the specified specialization. These specialties include:

Table 1. Specialization for Alert Disaster (TAGANA)

No.	Specialist	Personnel
1	Rescue	1,183
2	Psychosocial	7,040
3	Shelter	4,121
4	Public Kitchen	3,732
5	Communication	610
6	Logistics	2,263
7	Social Advocacy	296
8	Evacuation	1,369
9	Social Companion	1,269
10	Disaster Victim Investigation	22
	Total	21,905

From the total number of Tagana in Indonesia in 2018, 21,905 have been specialized so that the disaster management process will be more directed, structured and integrated. The remaining 18,980 personnel are General TAGANA in charge of helping TAGANA specialize in the mitigation process, emergency response, and post-disaster recovery stages.

The number of TAGANA in Indonesia currently around 38,000, has not met the number of Indonesian disaster volunteer needs of 120,000 people. In its implementation, the public interest in being part of the TAGANA is quite large, but the allocation of TAGANA formation has a limit every year. In response to this, the Ministry of Social Affairs has developed a component for the last three years, namely TAGANA Volunteers / Friends of TAGANA. TAGANA volunteers and Sahabat TAGANA have differences with the core TAGANA. the difference lies in the training given to TAGANA in the form of disciplinary training and other more comprehensive and technical training on disaster. But Friends of TAGANA also get training related to their profession.

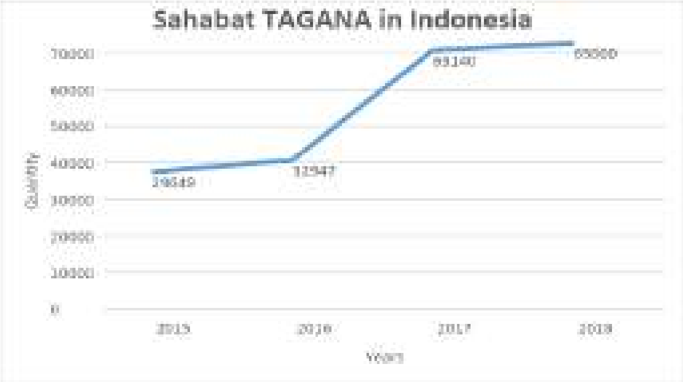


Figure 4. Graph of the increasing number of TAGANA Friends in Indonesia 2015 - 2018

In optimizing the role of the Disaster Preparedness Cadets (TAGANA) in the disaster management process, the Ministry of Social Affairs seeks to increase the number of Friends of TAGANA from year to year. In 2015 Friends of Tagana numbered 29,649 people and in the following year began to increase to 32,947 people. The number of Friends of TAGANA continues to increase in 2017 totaling 63,140 and reaching 65,000 in 2018. This number is expected to be able to meet the number of volunteers targeted by the government in tackling the threat of natural disasters in Indonesia.

The Ministry of Social Affairs cooperates with Sahabat Taruna Siaga Bencana (Tagana) from various elements of the organization in the community to be provided with disaster preparedness training. These organizations include journalists, youth organizations, and community radio as a step to anticipate and increase knowledge on natural disaster management in the field of social protection. Following are Friends of TAGANA in Indonesia in order to optimize the role of TAGANA in disaster management:

a. JUGANA (Jurnalis Sahabat Taruna Siaga Bencana). Journalist Disaster Preparedness Friends.
   The Ministry of Social Affairs also held training for journalists who aimed to improve the knowledge of journalists about the maagement of the disaster. The training participants were taught how to set up tents, public kitchens, and clean water, as well as water rescue. The training was attended by dozens of print, electronic and online journalists. Those who are trained will later be confirmed as Journalists of Disaster Preparedness Friends (JUGANA).

b. BANSER ANSOR SAHABAT TAGANA.
The Ansor youth movement is a youth organization in Indonesia affiliated with Nadhlatul Ulama (NU) that manages the Multipurpose Ansor Line (Banser). Banser is in charge of security, carrying out humanitarian missions in various regions of Indonesia. As one of the strategic elements in Indonesia, Banser will greatly help in handling disasters considering there are 274 disaster-prone areas.

c. PRAGANA (Pramuka Sahabat Tagana) Scout Friends of Tagana
Working together with scouts who are all over Indonesia to become Friends of TAGANA at the Kwarnas level (National Quartir). The National Quartier is in charge of leading the scout movement during his tenure (5 years), establishing budget policies, fostering and assisting the regional quarters, fostering cooperation and assisting the government in implementing government programs in an effort to achieve national goals.

d. RAPI SAHABAT TAGANA. (Radio Antar Penduduk Indonesia Sahabat Tagana) Inter-Population Radio Indonesia Friends of Tagana. As a Community Organization that is engaged in Inter-Population Radio Communication and is ready to participate in helping the Government and the community build up-to-date communication systems in disseminating information on natural disaster and social disaster management.

e. DIFAGANA (Difabel Tanggap Bencana). Disabled Disaster Response.
The Minister of Social Affairs inaugurated a group of diffable volunteers named DIFAGANA. The establishment of Difagana is based on the spirit of volunteerism and disaster. Then from that awareness gathered several people with disabilities who shared the same vision and mission, namely Difabel was not a weak citizen, but diffables had the potential, had a spirit of volunteerism and enthusiasm to help others. Synergy of persons with disabilities in Disabled Disability Preparedness. As many as 50 Difagana people have been given training on how to mitigate disasters, trained first aid questions and trained in evacuation in the event of a disaster. The trainings were also held in collaboration with TAGANA, NGOs and PMI.

f. MAPAGANA (Mahasiswa Siaga Bencana) Disaster Preparedness Student
Aimed at students to be able to become agents of TAGANA's reinforcing inspiration and synergize with other elements in disaster management.

4. Conclusion

The disaster management process is a collective effort that must involve various layers of government and society. Strategically implemented businesses by the National Disaster Management Agency (BNPB) at the national level, and the Regional Disaster Management Agency (BPBD) at the regional level, it is still not enough to overcome the threat of natural disasters that occur in Indonesia.

The Ministry of Social Affairs through the Permensos policy No.29 of 2012 triggered the TAGANA (Disaster Preparedness Cadets) program which aims to activate the disaster management system in social protection, mobilizing Tagana HR and social volunteers, providing assistance to fulfill basic needs and other social services, psychosocial support and advocacy services. This program was formed to utilize and empower young people in integrated disaster management. Midshipmen involved are prioritized by cadets who come from disaster-prone areas and areas that have been mitigated.

One form of efforts to increase the number of TAGANA in Indonesia is through integration with other community organizations. In standard operating procedures (SOP), all TAGANA must be ready to attend one hour after the disaster occurs. Must be responsive, swift to carry out social protection against disaster victims. The joining of journalists in Sahabat Tagana makes the natural disaster management efforts more responsive.

Consistency and community participation through Tagana must be maintained by including Tagana in various stages of disaster management. This is important, because Tagana is one of the elements of society that plays a role in disaster management officially recognized by the government. Therefore, the central and regional governments must be able to prepare programs to be able to increase the role of Tagana in the stages of disaster management so that it becomes an important point in maintaining national defense, especially in managing disaster response.

References

[1] Kemeterian Pertahanan Republik Indonesia 2015 Buku Putih Pertahanan Indonesia

[2] Menteri Sosial RI 2019 *Peran Kementerian Sosial RI Dalam Penanganan Masyarakat Pesisir Pasca Bencana Alam* Disampaikan pada kuliah umum kepada Perwira Siswa Prodi Strategi Laut, Program Magister Terapan Dikreg Seskoal

[3] Undang-Undang no 24 tahun 2007 Tentang Penanggulangan Bencana

[4] Carolina, Martha 2018 *Kelemahan-Kelemahan Penanggulangan Bencana Alam di Indonesia* Vol. III, Edisi 18 Analis APBN, Pusat Kajian Anggaran, Badan Keahlian Dewan DPR RI

[5] Djalante, et all 2011 *Adaptive Governanceand Managing Resilience to Natural Hazard* International Journal Disaster Risk Science

2011, 2 (4)

[6] Peraturan Kepala Badan Nasional Penanggulangan Bencana Nomor 4 Tahun 2009 tentang Pedoman Bantuan Logistik (Perka BNPB No. 4/2009) oleh Kepala Badan Nasional Penanggulangan Bencana (BNPB)

[7] Peraturan Menteri Sosial (Permensos) No. 28 Tahun 2012 tentang tugas dan fungsi TAGANA

INSURANCE DESIGN AND BUILDING PUBLIC RESILIENCE IN FACING NATURAL DISASTERS IN INDONESIA

Tedy Ardiansyah

Universitas Indraprasta PGRI, Jakarta 12530, Indonesia

*Corresponding author: teddyappi@gmail.com

Abstract

Indonesia is a disaster-prone country as evidenced by the epicenter of the earthquake in Indonesia as well as the Indonesian seismicity map when viewed from the number of incidents and the number of victims of disasters from year to year always increasing, further aggravated by economic losses resulting from the disaster. This is what underlies how to build community resilience to disasters and disaster insurance in Indonesia where with state disaster insurance can reduce the cost of building infrastructure, but until now disaster insurance has not been made even though there are plans. For now, it is more directed at insurable state assets. This research is using qualitative research methods. The above problems will be analyzed through several data sets, both observations, interviews and data references. Data and information are analyzed by data reduction techniques, data presentation, and verification retrieval through triangulation to conclude. Where specifically, the analysis of disaster insurance designs uses Nvivo tools to simplify and assist in the data processing. The results of future research can help provide alternative answers in dealing with risks and insurance guarantees in the community.

1. Introduction

Based on BNPB data, the total number of disasters occurring in various parts of Indonesia as of December 30, 2018, reached 2,564 disasters and is still likely to increase. Thousands of disasters left 3,349 people dead, 1,432 people missing, 21,064 people injured, 10.2 million people displaced and affected, and 319,527 houses damaged. BNPB noted that floods, landslides, and nipples still dominated the disasters that occurred in various regions. Only later geological disasters such as earthquakes and tsunamis. The geological disaster that occurred in 2018 recorded 83 incidents. However, this disaster has the greatest impact compared to other disasters. BNPB estimates that the total economic loss from the thousands of disasters that have occurred in Indonesia so far this year can exceed the figure of Rp 100 trillion, both material losses and others.[1]

In 2018 the death toll rose 984 percent, victims lost up 1,972 percent. "Injured victims rose 1,996 percent and victims were displaced and affected as well, up 178 percent and the number of damaged houses rose 1.341 percent, and this 2018 disaster was the largest since 2007 until 2018," he said. Central Java, West Java, East Java, Aceh, and South Kalimantan Sutopo said that the most affected area was Java Island, the number of occurrences, the highest was always Java, both Central Java, West Java, and East Java because the population was the most there. They live in disaster-prone areas, with the five largest districts in Central Java, namely Cilacap, Wonogiri, and Tangerang, one in West Java, one in Bogor Regency, one in Banten Province, namely in Serang District.[2]

The impact of the disaster was reported to be very large. 3,548 people died and lost, 13,112 people were injured, 3.06 million people were displaced and affected by the disaster, 339,969 houses were severely damaged, 7,810 houses were moderately damaged, 20,608 houses were slightly damaged, and thousands of public facilities were damaged. "Disaster trends also tend to increase from year to year. The high danger of disasters, such as earthquakes, tsunamis, volcanic eruptions, floods, landslides, droughts, forest and land fires, tornadoes and extreme weather, are also still high in vulnerability and low capacity cause a high risk of disaster.[3]

Table 1. Natrual Disaster in Indonesia Period 2018 s/d 2019

Type of Disaster	Total	Wounded			Broken house (unit)			
		Death	Victim	Evacuate	Heavy	Moderate	Light	flooded
Flood	904	119	302	1,453,803	1,538	430	4,794	290,893
Landslide	715	167	180	38,198	663	573	1,321	0
Flood & Landslide	4	0	1	0	6	1	21	0
Tidal wave	37	0	5	114,829	69	44	52	26,580
Tornado	1,187	24	248	16,019	2,343	3,816	15,238	0
Dryness of water	129	0	0	7,798,693	0	0	0	0
Forest fires	400	4	4	586	1	0	1	0
Earthquake (EQ)	33	572	2,063	483,399	77,055	35,988	114,026	0
Tsunami	2	453	14,059	41,132	1,583	70	1,099	0
EQ & Tsnunami	2	3,475	4,438	221,450	68,451	0	0	0
Volcano eruption	53	0	56	71,424	0	0	0	0
Total Number	3,466	4,814	21,356	10,239,533	151,709	40,922	136,552	317,473

The Purpose of this study are as follows: finding out the Disaster Insurance Perspective in Indonesia, helping accelerate the implementation of Disaster Insurance in Indonesia in the form of input information or policies from the Insurance Industry Experts in Indonesia, and To identify disasters that occur are the best experience so that it transforms into a formidable Indonesia to rebuild after being forged by natural disasters. That is what inspires Indonesia to build community resilience to disasters

2. Research Method

The method used is qualitative is to find a deep understanding of a phenomenon, fact or reality.

Facts, reality, concepts, symptoms, and events can only be understood if the researcher tracks them in a manner that is not limited to just a view on the surface. This depth highlights the qualitative method, as well as its superior factor. Like the phenomenon of the iceberg in the area that appears on the surface is only small, but the one beneath it is the big and strong one. Conventional understanding will not be possible without observation, interviews and direct experience. That means that there is a logical relationship between relationships, interviews, observations, phenomenological theories, and inductive processes. Thus methodologies and methods are very difficult to separate in the context of qualitative research.[4]

Another theoretical study of the methodology used in the form of qualitative research methods, is a research method based on post positivism or interpretive philosophy, used to examine the natural condition of objects in the researcher as a key instrument, the technique of data collection is triangulation (collection of observations, interviews, documentation), the data obtained tends to be qualitative data, data analysis is inductive/qualitative, and the results of qualitative research are to understand meaning, understand uniqueness, construct phenomena and determine hypotheses.[5]

Data analysis in qualitative research is carried out at the time of data collection, and after completion of data collection in a certain period. At the time of the interview, the researcher had analyzed the answers of the interviewees. If the answers interviewed after being analyzed have not been satisfactory, the researcher will continue the question again, to a certain extent, obtained data that is considered credible. Miles and Huberman (1984), suggest that the activities in qualitative data analysis are carried out interactively and run continuously until complete, suggesting that the activities in qualitative data analysis are carried out interactively and take place continuously until complete so that the data is saturated. Activities in data analysis, namely data reduction, data display, and conclusion drawing/ verification. [6]

Data Collection Techniques are carried out using Trianggulasi where the combination of several data, Primary Data using Interview from Informants, specifically Informants related to Insurance Design are Insurance Experts, generally these Insurance experts still serve as top brass in leading insurance companies in Indonesia[7], While the others are using secondary data in the form of references from books, Internet and national and international journals that have been indexed.

3. Results And Discussion

There are two parts in the discussion of the problem, First on Community Resilience in the face of Natural disasters and the second Natural Disaster Insurance

Design in Indonesia were at this stage using the Nvivo Tools.

3.1. *Building community resilience in the face of natural disasters*

The results of several studies have formulated how to build community resilience in the face of disasters[8]:

a. Towards Total Disaster Risk Management Promotion (TDRM)

In promoting total disaster risk management (TDRM) it is very important to build, develop and strengthen building blocks as listed below:

Steps were taken by Indonesia administratively to reduce disasters: Seismic Earthquake Resistant Houses and Buildings, Improvements are needed regarding building codes in Indonesia, Directions for improving future building standards in Indonesia, The importance of seismic earthquake-resistant buildings.

Establishment of Early Warning Systems for Tsunamis and other Disasters: Current problems and future direction of the tsunami early warning system in Indonesia, Current network status of Indonesian seismological observations, Improvements needed from the Indonesian seismology observation network, Important Media Roles Including Sirene and Communication.

Measures to overcome floods, debris flows, landslides, slope failures and, volcanic eruptions: The importance of continuous observation, Use of earth observation satellites for disaster information collection, Map of the importance of risk, To ensure the effectiveness of risk maps, Planning, and Investment in land use help hazard maps

b. Promotion of Disaster Prevention Culture, among others: Culture of disaster prevention is rooted in everyday life for disaster information, The culture of disaster prevention has its roots in everyday life for housing seismic resilience in Japan, Interdisciplinary approach to disaster risk reduction, Reconstruction of disasters, learning, and education for disaster prevention.

3.2. *Natural Disaster Insurance Design in Indonesia*

Characteristics of Informants and Use of NVivo Tools According to Cresswell in Kuswarno, the criteria for good informants are: "all individuals (Creswell, 1998: 118), researchers chose informants who were a Managing Director who, because of his experience, was able to articulate his experiences and views about something being asked.[9]

The researcher decides the informant who can provide relevant information and can help answer his research question. In this study the research subject or informants have the following general characteristics: (1) Men aged 40 - 70 years; (2) Men who are married and have children; (3) The final education is at least a Bachelor(S1). (4) Having a permanent job outside the home either as a civil servant or employee private sector with opportunities for improvement in their work (having a career path or track record in their careers); (5) Having a high position in the job. (6) Work outside the home for more than eight hours; (7) Income above the minimum work wage in Jakarta (8) Residing in Jakarta.

In this study, researchers used NVivo 10 tools, where these tools have been recognized internationally for conducting qualitative research. Nvivo 10 have research data source (internals), external research data sources (Externals), researcher records during data collection (memos), and matrix framework (framework matrices). Internal Sources in this context is all qualitative research data sources that can be included in NVivo, for example, interview records, interview transcripts, notes during conducting research, photographs, survey data tables, certain website contents, bases, and even videos.[10]

External sources are research materials that cannot be entered directly into NVivo, such as reference books from printed libraries or printed journals. Memos is a research data source in the form of researchers' records during the process of collecting data or reflections carried out by researchers during their conduct research. Matrices framework is a summary of the results of observations of certain participants and project themes that have been made in the matrix table.
Classify Nodes

Nodes are 'Containers' where researchers store themes, participants, settings research and research organizations. Therefore, as researchers can arrange themes into sub-themes (sub-topics) into specific topics that are more specific (child nodes)[11]. Enclosed below regarding the nodes from the research title of the Disaster Insurance Perspective in Indonesia:

3.2.1 Data analysis through Text Search Queries.
Text search queries, researchers can explore words contained in text or research data sources. NVivo will display these words in the form of diagrams to form the meaning of the word in the context of its use.

Table 3 Analisis Data Text Search Query

Name	In Folder	References	Coverage
Informant 1	Files\\interview	40	011%
Informant 2	Files\\interview	47	005%
Informant 3	Files\\interview	33	009%
Informant 4	Files\\interview	36	009%
Informant 5	Files\\interview	25	007%

It is very clear from all the informant data displayed, the word disaster insurance is the most dominant in all informants, the minimum that appears is 25 references and the maximum is 40 references, meaning that disaster insurance is the main thing in anticipating disaster risk.

3.2.2. Data analysis through Frequency Queries word. Word Frequency Queries in NVivo can help researchers to explore the most frequently occurring words (freq) in the research data. With this analysis tool also, words that have the same meaning can be categorized in the same group. Word Frequency Queries is effective for text content analysis or thematic analysis (content/thematic text analysis). The details of word frequency queries from this study are attached below as below:

Table 4 Analisis Data Word Frequency Queries

Word	Length	Count	Weighted Percentage (%)
Insurance	8	97	004
Disaster	7	84	003
Which is being	4	83	003
This	3	58	002
That	3	46	002
For	5	46	002
Earthquake	5	42	002
And	3	39	002
Government	10	34	001
Therefore	5	1	000

The NVivo output above shows a table of 741 words that appear most frequently in Interviews / Interviews. 10 The top word is filled by "Insurance" 87 times, "Disaster" 84 times, "Earthquake" 42 times and "Government" up to 34 times while the last word is "that is" which only appears once. All data comes from informants who have conducted interviews or interviews. In the NVivo output above, the most mentioned words are displayed in the largest letters with very clear colors. It appears that the words "Insurance", "Disaster", "Government" and "Earthquake" are the most dominant ones appearing in their entirety. A Word frequency Query Result analysis produces the word Disaster Insurance which is a very important or urgent matter, which is part of the information that has been submitted.

3.2.3. Associative Relations (Associative Relationship) Cluster Analysis. In the type of associative relationship, the researcher needs to determine the two-unit analysis items (two types of nodes) that are connected. For this purpose, the researcher needs to provide the name of the relationship (for example associated to / associated with, in line with/in line with, in the same direction).

The perspective of Disaster Insurance for 26 parent nodes has a good picture of the Association of Cluster Analysis aka "High" Interpretation, which is between

Informant Harsanto S.M Widodo and Julian Noor. While the others fall into the category of "Rather Low" and "Enough" Interpretations. As for the association summary of the Cluster Analysis of the Disaster Insurance Perspective in Indonesia indicated by the significant Pearson Correlation in the form of a Cluster Analysis Associative Summary table as follows:

Table 5. Summary Asosiatif Cluster Analysis

File A	File B	Pearson correlation
Files\\interview\\Informant 4	Files\\interview\\Informant3	0,721769
Files\\interview\\Informant 5	Files\\interview\\Informant 1	0,69043

If you look at the table above, it is clear that the number 0.7 shows a high interpretation of the correlation between informant 4 and 3, which means that there is a strong relationship or similarity from the results of interviews regarding the Disaster Insurance Perspective in Indonesia.

3.2.4. Comparison Analysis. A Comparison Analysis(Project Map) is a way of exploring visually or presenting data in a project that will or is being worked on. Comparisons analysis are made of shapes that represent various items in the project and connectors that show links between items. To do this you need some project data before you create a project map. The usefulness of the project map is as follows: Exploration and arrangement of data, Developing ideas, constructing theories and making decisions, Identifying patterns, theories, and explanations that arise, Visually describing links between project items and providing record stages in a project.[12].

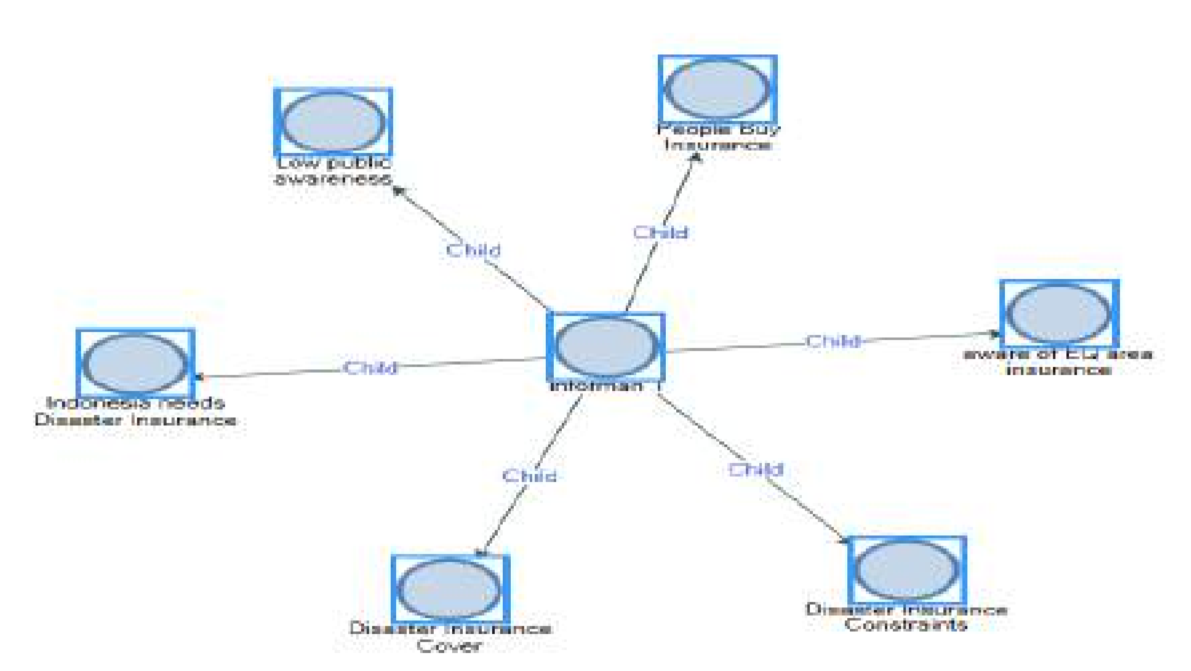


Figure 1. Comparison Analysis informan 1

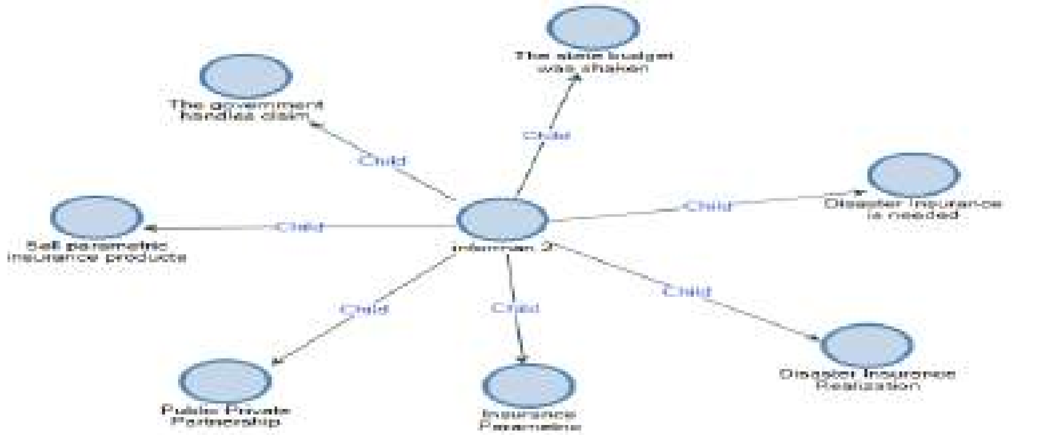

The state budget was shaken
The government handles claim
Child
Child
Disaster Insurance is needed
Child
Sell parametric insurance products
Child
informan 2
Child
Child
Child
Public Private Partnership
Insurance Parametric
Disaster Insurance Realization

Figure 2. *Comparison Analysis informant 2*

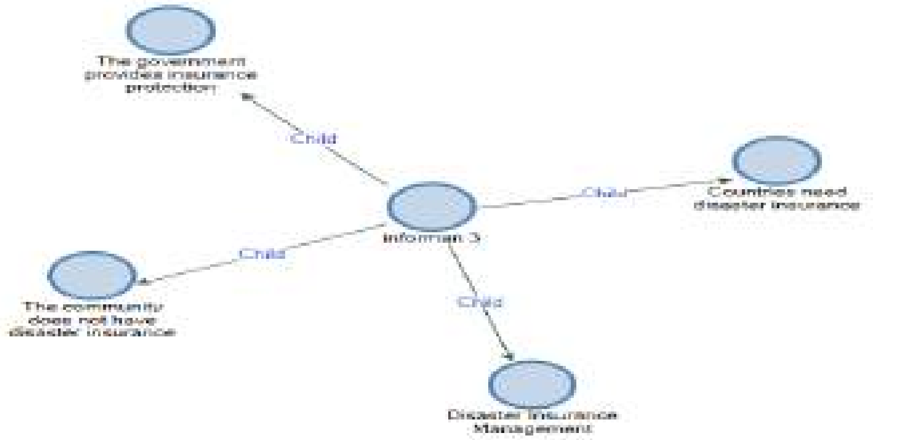

The government provides insurance protection
Child
Countries need disaster insurance
Child
informan 3
Child
The community does not have disaster insurance
Child
Disaster Insurance Management

Figure 3. Comparison Analysis informan 3

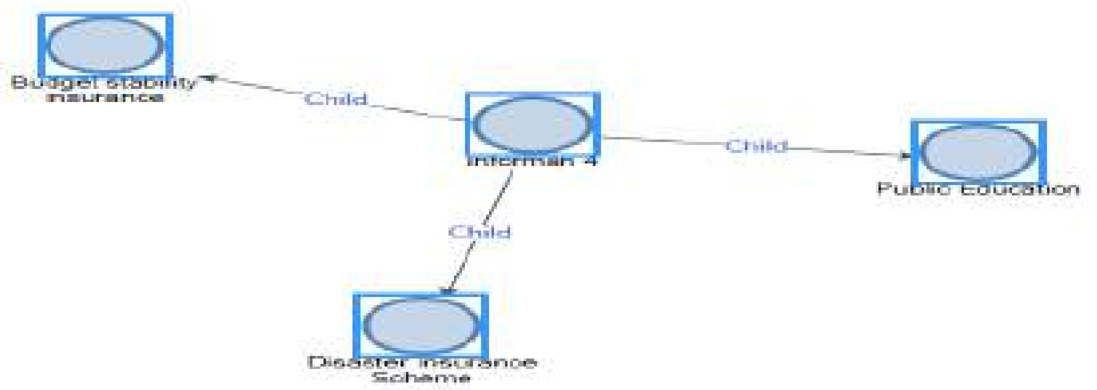


Figure 4. Comparison Analysis informan 4

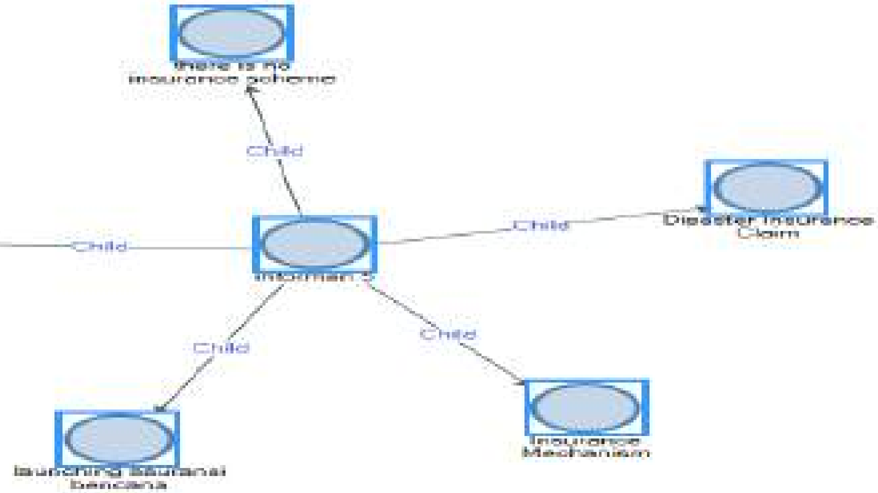

there is no insurance scheme
Child
The government pays premium
Child
Informan 5
Child
Disaster Insurance Claim
Child
Child
launching asuransi bencana
Insurance Mechanism

Figure 5. Comparison Analysis informan 5

4. Conclusion and Recommendation

Based on the results of the study it can be concluded, Disasters that occur are the best experience so that it transforms into a formidable Indonesia to rebuild after being forged by natural disasters. That is what inspires Indonesia to build community resilience to disasters, And Insurance Design results (Text Search Query, Word Frequency Query, Associative Relationship Cluster and Comparison Analysis) With Nvivo tools are very clear that the state is the one who has the highest responsibility to protect the public from disaster risk and plays a major role in accelerating the formation of disaster insurance both protection for state, industrial and community assets.

5. Acknowlegements

This paper is dedicated to Indraprasta University Jakarta and Universitas Pertahanan in Indonesia.

References

[1] C. G. Asmara, "BNPB: RI Ditimpa 2564 Bencana dan Merugi Rp 100 T di 2018," *CNBC Indonesia*, pp. 2018–2019, 2018.

[2] E. Safitri, "BNPB : Tahun 2018 Paling Banyak Korban Meninggal Dunia Akibat Bencana," *news.detik.com*, pp. 2018–2019, 2019.

[3] Fitria Chusna Farisa, "BNPB: Selama 2018, Ada 1.999 Kejadian Bencana - Kompas.com," *Kompas.com*, p. 1, 2018.

[4] M. S. Dr. J. R. Raco, ME., *METODE PENELITIAN KUALITATIF*, Pertama. jakarta: Grasindo, 2010.

[5] P. D. Sugiyono, *Metode Penelitian Kualitatif*. bandung: alfabeta, 2017.

[6] P. D. Sugiyono, *Memahami penelitian kualitatif*. bandung: alfabeta, 2014.

[7] M. Asuransi, "Asuransi Bencana," *Media Asuransi*, jakarta, Jan-2018.

[8] D. Sarkawi, A. Oktaviani, and A. Priadi, "Membangun Ketahanan Masyarakat Indonesia terhadap Bencana. In Peranan Perguruan tinggi dalam membangun budaya risiko masyarakat menghadapi bencanan," 2019.

[9] engkus Kuswarno, *Metode Penelitian Komunikasi Fenomenologi: Konsep, Pedoman, dan Contoh Penelitian*. bandung: Widya Padjadjaran, 2009.

[10] Bandur Agustinus, *Penelitian kualitatif metodologi, desain dan teknik analisis data dengan Nvivo 11 plus*. jakarta: Mitra Wacana Media, 2016.

[11] Jackson & Bazeley, *Qualitative Data Analysis with NVivo*. Losa Angeles, CA, USA: Sage Publication, 2013.

[12] qs international, "Nvivo 11 for windows help-about project map," *qsinternational.com*, 2019. [Online]. Available: www.qsinternasional.com.

Defense Strategy

Defense Management

National Security

Defense Technology

Cyber-Physical Systems Threats, Risks, and Vulnerabilities: A Challenge to Indonesia Defense Sector – IIDSS 2019

Arwin Datumaya Wahyudi Sumari[1], Sarwono Sutikno[2]

[1]Department of Electrical Engineering, State Polytechnic of Malang, Malang 65141, East Java, Indonesia

[2]School of Electrical Engineering and Informatics, Instittut Teknologi Bandung, Bandung 40132, Jawa Barat, Indonesia

E-mail: arwin.sumari@yahoo.tni-au.mil.id, arwin.sumari@yahoo.com

Abstract. We present a simple introduction regarding the awareness of the threats, the risks, and the vulnerabilities of Cyber-Physical Systems (CPS) with the emphasis on hardware attack. It will be discussed the risks and vulnerabilities of CPS as well as their components in systematic manner. CPS simply is any software-controlled hardware, any physical system which is controlled by software in order that it can be operated or used through internet-like connection. Various institutions, government, and private sectors, have installed and used CPS infrastructures such as defense, transportation, communications, finance, electrical, nuclear, health, and energy which are called as critical infrastructures. In defense sector, various weapon systems have used this kind of system. Network-Centric Operation (NCO) cannot be applied and implemented if it is not supported by CPS weapon system. The perilous threat to CPS is hardware attack which has not been thought before that it is now becoming a very dangerous threat to defense system. In this paper we show how vulnerable is CPS from cyberattack, namely hardware trojan attacks which in turn bringing risks to the defense and military sectors which have procured modern CPS weapon system.

1. Introduction

Cyber-Physical System (CPS) actually is not a new thing. In its simple definition, it is any software-controlled hardware or any physical system which is controlled by software in order that it can be operated or used whereas the control information is delivered through cyberspace by means of internet or any data link which employs internet-like network. CPS became attracting attention along with the coined of Industry Revolution 4.0 (IR4,0) with the supporting technologies to be mastered that is, Artificial Intelligence (AI), Internet of Things (IoT) and Big Data. IoT is where anything software-based electronic equipment that can communicate one to another, whether it is human-controlled one or autonomous one. Meanwhile AI is the technology to create and develop not only autonomous systems but also intelligent systems. The intelligence of the systems may mimic one or combinations of various intelligences already provided in the Earth. Those technologies not only need but also produce a huge volume of whether structured or non-structured data. Hence it is called as Big Data.

CPS is also not a new technology and it is a generalization of embedded system [1], a place where the hardware and the software works together to carry out a certain function. Embedded systems have around for years and they are already installed in various equipment used in many applications fields. Transportation modas in the early of 2000s already had embedded system installed in their systems. Warfighter aircrafts are the ones which are equipped with such system, such as Flight Control System (FCS), electrical system, weapon delivery system, navigation system, and many others. The information obtained from such systems are only kept within the aircraft. With the introduction of the internet and the needs of knowing the information of the aircraft systems while in operation, the gathered information can be transmitted to the ground system and vice versa where the ground station sends messages to the aircraft. The embedded system plus the internet as the means of informaton exchange is called as CPS. Modern airborne vehicles, ground vehicles and sea vehicles are CPS. Most of their systems are controlled by software. Even some vehicles' instruments are software-defined equipment. As an example, the F-4 Phantom warfighter built in 1970s has only 8% software in its systems. On the other hand, the F-22 warfighter built in 2000s has 80% software in its systems [2]. Meaning that there is a significant increase in putting more software to the aircraft systems.

Such systems bring risks and vulnerabilities to threats whether from the software or the hardware, especially from cyber realm. The threats become perilous the era of networked systems. Defense and military sector have used such system of systems because of the motivation pushed by new warfare paradigm called Network-Centric Warfare (NCW) more than 20 years ago [3]. Networked system has also been accomodated by a framework called Command, Control, Communications, Computers, Intelligence, Surveillance, and Reconnaissance (C4ISR) [4]. Those paradigm and framework were born almost in the same time. In NCW paradigm, all weapon systems are assumed as a computational node which has capability to process the information, to exchange such information with its parties in the network, and to make decision based on the gathered information. Meanwhile the C4SIR framework gives a guidance how to develop a networked system in terms of architectural, operational, and technical aspects. The framework also gives a guidance how to synchronice any kind of data received from various data sources to become a single information which represents the processed data. The ultimate aim of the two is to accelerate the command and control from sensor-to-shooter and vice versa.

Networked system especially the dedicated one such as used my defense and military sector has to be protected from any means to make it down knowing that threats are also evolving. There are various cyber threats starting from software, hardware, environment, and people. One of the perilous threat is hardware attack such as trojan. Software trojan has been known since the invention of computer viruses long time ago and there have been various antidotes for them. Hardware trojan which has not been thought before, it is now becoming a very dangerous threat to CPS. Trojan is a hibernated attack. It will wake up when triggered by something such as system's clock. Understanding the importance to protect the CPS since the beginning it is created, in this paper deliver a survei on the threats, the risks, and the vulnerabilities of CPS against hardware attack. This paper is arranged as follows. Our intention regarding the need of CPS protection is already given in Section 1. In Section 2, shorts theories on relevant materials will be given in Section 2. Meanwhile, the elaboration of the risks and the vulnerabilities of CPS will be given in Section 3 as well as the challenges that are now faced by the defense and military sectors. We conclude our paper in Section 4.

2. Relevant Theories

2.1. Cyberspace and Its Impact to Defense and Military Sector

There are some definitions on cyberspace. One of this definition come from United States Department of Defense (US DoD) which defines cyberspace as a global domain within the information environment consisting of the interdependent network of information technology infrastructures, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers [5]. Cyberspace is a man made space with the help of the internet and its infrastructures. It is a space that cannot be seen, be tasted, be smelled, and be touched, but it is there. It is the means for digital information to be transmitted, processed, and exchanged among parties. Cyberspace can be in form of wire and wireless, depended on the method in developing the networked system, or it can the combination of wire and wireless. Referring to the definition above, cyberspace is global domain where any actor can use it to do something good or bad. The information environment means a place where the information and communication infrastructures as well as the information itself reside. These infrastructures are systems of networked systems which are interdependent one to another. Only digital information which resides in cyberspace because only this type of data format that is understood by the computers as well as the embedded processors and controllers. The internet is the essential thing of the cyberspace, and it is the must mandatory thing in the cyberspace. One essential thing for its sustainable operation is the electrical supply received from the electrical grid. Embedded processor and controller are processor and controller which are equipped with hardware and software wihtin them. With those resources they can be programmed to control other equipment, such the ones used in aerospace and manufacture applications. The combination of embbeded processors and controllers triggered a new consept what is now called as CPS.

Defense and military viewed that the cyberspace is the opportunity and also the challenge. As an untouchable space, it can be used by the enemies to obtain advantages over own critical and strategic assets. Therefore, some of military operations concept whether for war or for other than war are then adopted to be done in the cyberspace. Long before the cyberspace taken as consideration as a domain for warfare, a military operation called Information Operations was formed with the aim to achieve information superiority which is the basis for achieving decision superiority. The successfulnes of achieving it is as a guarantee to win in all spectrum of warfare. Information Operations is a joint or combined operations or multiple operations which all operate in information realm. Some of the operations are Computer Network Operation (CNO), Electronic Warfare (EW), Military Deception (MILDEC), Psychological Operation (PSYOP), and Public Affairs (PA) [6]. As the warfare technology and military strategy as well as the threats evolve along with the massive use of the cyberspace for conducting warfare with many actors involve in it, CNO was then taken out from Information Operations and formed as an autonomous military operation called Cyberspace Operations (CO). It has three operations within it, namely Offensive CO (OCO), Defensive CO (DCO), and DoD Information Network Operation [7][8].

2.2. Network-Centric Warfare

Network-Centric Warfare (NCW) is just another warfare paradigm after observing the benefits of using the Internet to accelerate the decision making cycle. The concept of NCW actually was adopted from business environment then was taken to the military one. Network-centric or net-centric has been there since the invention of the Internet by Advanced Research Project Agency (ARPA), which then taken over by DoD and became Defense ARPA (DARPA), called ARPANet in the end of 1960s [9]. The network connected several universities in the United States of America (USA) and they can exchange information one to another in a quick manner. This network then became the Internet what we know now after it is used by many universities, institutions, agencies, and communities all over the world. This make the world borderless and timeless. The evolving technology has also contributed in delivering more modern computing devices and equipment which make the information exchanging can be done anytime, anywhere, using any device. This paradigm has successfully leverage the economics of the people, shorten the time, and lower the overhead. This reality attracted the military and thought how develop such mechanism which can be applied in military operations. The primary aim for the military is to shorten the time between the sensor and the shooter, because information gathered by the sensors will become the information for the shooter to carry out its mission. The faster the information received by the sensor, the faster the war can be won.

Net-centric is not a new thing but in reality this jargon was needed to raise the awareness of the military of the importance and the critical of the Internet as a means to support the military operations to achieve much better results. In essential, net-centric is a networked system of systems with the center is the network itself, meaning that the network is everything. A formation of warfighter aircrafts or warfare ships or warfare land vehicles can be said a networked system. The warfighter aircrafts can talk to each other in their formation and the ground stations but the information displayed on the instruments can only be seen by each member of the formation and cannot be extended to other members. Meaning that such information can only be broadcasted manually to all members and this takes time. The time is very crucial for warfighter aircraft especially when the situation in the air needs a quick decision. The same thing happens to their parties, the warfare ships and the warfare land vehicles. The emergence of net-centric concept brought a new blood to military sector to upgrade their systems to be have capablities for Net-Centric Operation (NCO) or NCW. By making use of net-centric, What You See Is What Your Team Sees (WYSIWYTS) can be achieved. The information displayed on a member of a team's instruments will be automatically displayed on other members of the team, and also it is automatically displayed on other members which are connected to the network such as the warfare ships team, the warfare land vehicles team, and the ground station as well as the command and control posts. A simple illustration of NCO is depicted in Figure 1.

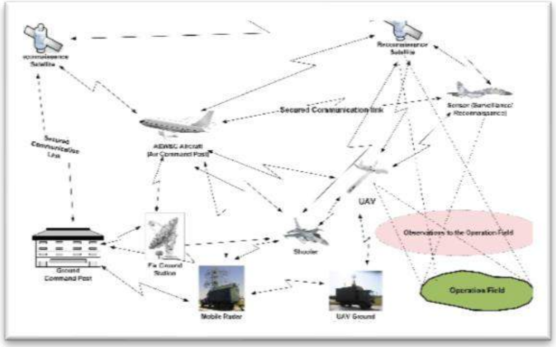

Reconnaissance Satellite
Reconnaissance Satellite
Secured Communication link
Sensor (Surveillance/ Reconnaissance)
Secured Communication Link
AEW&C Aircraft (Air Command Post)
UAV
Observations to the Operation Field
Ground Command Post
Fix Ground Station
Shooter
Operation Field
Mobile Radar
UAV Ground

Figure 1. An illustration of a Net-Centric Operation (NCO) based on C4ISR framework [10].

The components of NCO include warfighter aircrafts, ships, land vehicles, and ground stations while command posts can be in one of ground stations or in one of warfighter vehicle (air, sea, or land), the satellites, data communication links which can be internet-like wired and wireless tactical data link. Warfighter vehicles will include manned and unmanned vehicles such as Unmanned Aerial Vehicle (UAV), Unmanned Sea Vehicle (USV), and Unmanned Ground Vehicle (UGV) where they may be equipped with combat capabilities or not. Any warfighter vehicle has opportunity to carry out observation and surveillance operation to objects in operation area. Based on WYSIWYTS, the intelligence gathered from such operation will be broadcasted directly to all parties in the network and it is called as information sharing. Hence, the shared information can increase the level of situational awareness of all parties participating in the operation which then also increases self-synhcronization among parties. By knowing and understanding the real military area's dynamic, the higher command can not only make a decision what action should be carried out by his lower commands in a quick manner, but also he can manage the tempo of operation to ensure higher survivability of his men in order to bring higher lethality to the enemies [11]. As we can see that most of the components of NCO/NCW are CPS. To have capabilities to connect to the network, they have to have internet-like system within their systems.

2.3. Cyber-Physical System

History shows that software and hardware were separated one to another because in that time our predecessors thought that software is in informatics domain and hardware is in electronic domain. Informatics people just do programming to make softwares, that is writing codes, compiling them, and debugging them to ensure the softwares work as they are designed. On the other hand, electronic people just do developing electronic components such as Integrated Circuit (IC) which can be in form of microprocessors and memories, or electronic tubes such the one used to built computers in the past. The need of small devices that have capabilities similar to the big ones, pushed the people from those two worlds to work together which then ended up with embedded system, a system which combines software and hardware within it. Big computers were then resized to smaller ones such as personel computers and laptops. This also happened to communication equipment such telephones and the related ones. The most important thing is those devices and equipment are already internet-ready, meaning they have already equipped with internet connection capability which make them can connect to the internet easily wherever they have access to communication networks whether wired or wireless. This thing that makes such devices as CPS. The most dangerous thing is by using these CPS devices, any actor can do command and control to other devices or equipment to do something bad.

In general, CPS has four components as follows.

- Cyber component. The component which is related to computer systems or the component which does computational mechanisms where it controls the physical activities of the physical component.

- Physical component. The component which does physical activities and sends the results of its activities to the cyber component through the network. The information regarding the physical activities will be inputs to the cyber component whether to be recorded for future used or to be used to refine the physical component's activities in order to get better results.

- Cyber-Physical interface. This component is rarely mentioned but it plays important role to bridge the cyber component anf the physical one, such as monitor and take information regarding the physical phenomenon being observe, and perform the action based on the command delivered from the cyber component. As mentioned in [12], interface is the central of the imtegration of systems.

Cyber-physical system have two kinds of inerface, namely physical interface and cyber interface which they are very vulnerable of threats.

- Network. This component is a mandatory one which responsible to the unblocked information delivery from the cyber component to the physical one and vice versa. It can wired or wireless but most of the cases it is a combination of the two means.

As elaborated in Section 2.2, most of weaponry systems are CPS which are made up from a combined hardware and software with an internet-like-connection capability. Threats to CPS can be divided into four categories, namely threats to hardware, threats to software, threat to the network, and threat to the information. Threats can be viewed from various perspectives. In his research, [13] views the threat to CPS from five factors, namely source of the threat, the target of the threat, the motive behind the threat, the attack vector, and the potential consequences of the threat. In another research, the threats to CPS are related much to parameters in Information Security (INFOSEC), namely Confidentiality, Integrity, Authenticity, and Availability [14]. Threats to CPS is not only comes from the software side but also from the hardware side. The cyber component and its counter part, the physical one certainly have electronic systems installed within them, and theya are very vulnerable to hardware attack. A comprehensive elaboration on CPS was done by [15] and they have made classification of CPS viewed from the design, the aspect/issues, the applications, and challenges and roadmap.

2.4. Malacious Hardware and Software

Malicious software (Malware) has been a thing talked about for decades after the introduction of computer viruses. Malware is designed to harm, impair, ruin, violate, or destroy the computer and the computer-based system or machine as well as the network which runs or executes it. Malware can gain remote access to an information system, record and send data from that system to a third party without the user's permission or knowledge, conceal that the information system has been compromised, disable security measures, damage the information system, or otherwise affect the data and system integrity [17]. The worst thing that can happen is malware can take over the operation of a system which may cause severe damages not only to the system itself but also causalty to the personnel around it. On the other hand, malicious hardware also started getting an attention after a report mentioned that a high-tech country in the East used tiny chips to steal secret information from a high-tech country in the West [17]. Malicious hardware is (1) A virus or other malicious software that is attached to a program preloaded on a computer or external hard drive, (2) A Central Processing Unit (CPU) chip in a computer or handheld device that has a built-in back door, enabling an attacker to gain illegal entrance [18]. Far more difficult than a software virus, it requires access to an assembly line or semiconductor fab in order to replace good parts with infected ones. Malicious hardware installed as backdoor in a system is generally called as hardware trojan. It is also said as hardware-based cyber threats [19].

As mentioned above, malacious hardware like its counter part, Malware, can be designed to act as a backdoor which can be activated in various ways and used for performing many things. Research done by [20] shows that malicious hardware can be designed to steal passwords or break privilege protections, extract secret keys, add communication channels using Universal Serial Bus (USB) peripheral trojans, and add communication channels using a network card trojan. This also shows that what mentioned by the report above is true. For computer systems and machines which are computer-based, hardware is the house of software, the enviroment where software works. Each hardware is designed to accomodate certain sotwares. Meaning that the software has a trust to the hardware that it can work in a maximal way. In some cases, software may able to check hardware problems but cannot perform a check if something went wrong. If there is an attack to hardware, it will be a big problem if such attack affects all layers of the system [21]. As example, an attack to computer processor will affect all mechanisme which are relied on that Integrated Circuit (IC).

3. Hardware Attack: Risks and Vulnerabilities

Before the introduction of IC technology, the electronic devices had a big size such the ones which were used to build old computers. Electronic Numerical Integrator and Computer (ENIAC) built in 1945 was driven by vacuum tubes to perform computational mechanism. The invention of transistor in 1948 by John Bardeen, William Shockley and Walter Brattain, had changed the paradigm of computing system and it made the size of computers smaller. In 1958, Jack Kilby of Texas Instrument succeeded to build an oscillator IC with five electronic components in single IC [22]. This development has proved the prediction of Gordon Moore that the number of components on an integrated circuit had been doubling every year on average [23]. This trend will continue as there is a continued progress in terms of (1) new devices, (2) new architectures (with or without new devices), and (3) new paradigms of computation [24]. In 2017, Intel announced that it had succeeded packing 100 million transistors in each ne milimeter using 10 nm technology [25]. Meaning that the recent technology has been able to exceed to highest IC integration scale, that is Ultra Large-Scale Integration (ULSI) where more than 1 million electronic components can be accommodated in a single chip. It is clear that the higher the number of transistor in one IC the higher the potential vulnerability, hence the higher the potential of the occurence of hardware attack.

3.1. Hardware Trojan

Unlike Malware trojan, hardware trojan needs special attention in order to be able to detect its existence. Malware trojan is a malicious code which is designed to operate once it is downloaded to a compting system. It will active after a trigger such as time or being executed by the user. Some Malwares may target the computing system hardware by screwing up the mechanism of the hardware works or target a specific machine once a computing system is delivered to the market. A hardware trojan is any malicious and deliberate change to an integrated circuit (IC) design that may cause unwanted effects [27] or a malicious modification of circuitry and can occur at the system level, at the printed circuit board level, or internal to an integrated circuit [28] or malicious modification of an integrated circuit in order to offer advantage to an adversary [29], or a malicious and deliberately stealthy modification made to an electronic device such as the circuitry of an IC or chip. It can change the chips functionality and thereby undermine trust in the systems using that chip. Hardware trojan can be classified from its attributes [30], its trigger and payload mechanisms [31], three types of characteristics [32], and its scale level of attack impact [20].

Hardware trojan can infect the computing system's components or devices at the insertion phase and the abstraction phase at the components such as processor, memory, input/output device, power supply, and clock grid. If we follow the software engineering mechanism correctly and thoroughy starting from such as Specification Design Document (SDD), we can ensure that the components will be developed will be free from hardware trojan infection. The abstraction level plays very important role before the designed component is translated into real hardware. In this level, engineer will use Hardware Description Language (HDL) to make sure that the designed component is feasible to be transfered into real hardware, that is IC. The effects of hardware trojan infection can be one of or the combination of such effects. Cybersecurity threats to CPS can be information leakage and Denial of Service (DoS) attack. These are the vulnerabilities of the electronic device which are the door to infect the hardware trojan.

Hardware trojan can occur because of the addition or deletion of transistors or gates within a chip which causes malfunction or function but not as it was designed to, and can occur by modifying the wires and the logic how the chip works. The number of components which are added, deleted, or compromised also an important thing. This can happen during the system design especially when the chip designer has been compromised. This can also happen when the enginer does coding the logic of the hardware using HDL before it is simulated to ensure its clock feasibility. Inline with other researchers' classification, one of action characteristics is Transmit-info. This is a cyber theat to CPS caused by infectious hardware. The impact of hardware trojan attacks can escalate to affect the whole organization either military or non-military one. Insertion can be considered as bringing in infectious computing system to the organization. The larger the number of the system taking in, the higher the risk of the attacks. When the hardware trojan is activated from a large number of computing systems, then it will deliver a systemic effect to the organization performance. The last scale is when the attacks succeed, the hardware trojan has succeeded compromising organizational processes in a wider scale. This is the escalation of hardware trojan attack effect to an organization. Therefore cautiousness in procuring computing systems and having knowlege of their technical specifications are mandatory.

3.2. Threats and Risks to Defense System and Military Operation

We have did observation regarding C4ISR NCW/NCO and found that [33]:

- Defense sector uses CPS in almost its weapon system equipment especially in NCW era where size is matter.

- CPSes are highly needed for various applications especially in the Internet-of-Things (IoT) era.

- Small size CPSes can only be achieved via IC technology.

- Vulnerabilities of CPSes hardware which effect to cyberattack emerge from any level of IC manufacturing and various types of IC.

e number of components on an integrated

circuit had been doubling every year on average

Refer to NCO and C4ISR framework as depicted in Figure 3, the working flow of CPS is as follows.

- Intelligence, Surveillance, and Reconnaissance (ISR). This activities involve various sensors which can be manned and unmanned vehicles, human intelligence, network intelligence, signal intelligence, and measurement and signature intelligence. The information gathered in these activities is then stored in a secured Big Data to be processed directly or later depending the urgency of the situation. Surveillance and Reconnaissance on the military operation area are done to physical activities where the information collected is then delivered to command and control post or other parties through cyberspace.

- Computing. The collected information is then processed, analyzed, and inferred to become knowledge as the basis for making decisions. In net-centric paradigm, each vehicle is a computational node which has capability to carry out internal computation to the collected information to enhance its performance when performing ISR activities. Computing is an important aspect of CPS.

- Communicating. Information collected by all ISR vehicles can only be transmitted to command and control post or broadcasted to all parties if there is a secured communication network. Communication plays an important role as a means to deliver information from one node to another or to broadcast information to other nodes connected to the network.

- Commanding and Controlling. The knowledge obtained from computing phase is used as the basis for making decisions to make actions, that is commands to be performed. The commands are used to control the actors under command and also to ensure that the instructed commands have been performed correctly. Actions by actors are physical activities and these activities will be observed and monitored by nodes to gather new infomation regarding the impacts of the given commands.

3.3. CPS Weapon System

As mentioned briefly 2.2, most of NCO/NCW components which are distributively located at various strategic and critical areas are CPS such as the satellites (communication, intelligence, weather, positioning, combat), manned vehicles (air, land, sea, space), unmanned vehicles (air, land, sea, space), command posts (air, land, sea), and ground stations as well as surveillance systems such Radar (air, ground, sea).

Modern weapon systems are equipped with many advanced technology systems which include control system, navigation system, communications system, weapon targetting and delivery system, Radar system etc. A report mentions that multiple factors contribute to the current state of weapon systems cybersecurity such as the increasingly computerized and networked

nature of such weapons with more software and Information Technology (IT) dependent. Meaning that weapon systems' components can be easily attacked using cyber capabilities through the network as the pathways [34] and through systems' hardware such as processor and memory.

3.4. CPS Weapon System Cybersecurity

Cybersecurity to CPS should be done from four perspectives. The first one is cybersecurity for the cyber component, the second one is from the physical component, the third one is from the interface component, and the last one is from the network. If we take a look at deeper, all of those components have chips or ICs within their own systems which are potential to get infected by hardware trojan. By refering to Figure 2, here are some problems which may occur if the systems' hardware have hardware trojan activated, as follows [33]:

- Satellite

□ Intelligence satellites may send mislead information to other nodes, that is manned vehicle such as F-16, Airborne Early Warning/Control (AEW/C) command post, and Surveillance/Reconnaissance Sukhoi, and unmanned vehicle, that is the UAV. The same thing occurs to other nodes.

□ Communications satellite may malfunction and cannot bridge the communications among nodes. This will cause failure in command and control which can cause mission not accomplished.

- Manned and unmmaned air vehicle's avionics systems may not work properly and give risks to the aircrafts and the person who operate them on site. The failure of the avionics systems while the vehicle is being operated may cause fatal accidents such as friendly fire, uncontrollable, or taken over by the enemy.

- Degrading the capabilities of the reconnaissance systems of the manned and unmmaned air vehicles.

- Radar system can be directed to detect own vehicles as targets that have to be shot down.

- Information exchange may be delayed or transmitted to the designated enemy actor unknowingly. On the other, information leakage can also occur through communications channel which is opened by infectious hardware.

- Mislead information caused by the change in database stored in the memory can cause wrongly mapping of the operation field. This can cause incorrect military operation strategy.

- Loss communication because of communications systems malfunction or stop working causes shared situational awareness will not be achieved. In other word, WYSIWYTS is never achieved. The result is each node will know nothing what its parties see.

- Without having comprehensive information regarding the operation field causes the decision made can be incorrect and risk the units under command. Therefore decision superiority is not achieved and the victory is far to achieve or may already be defeated before the operation is even carried out.

We can see that hardware trojan attacks to CPS weapon system can escalate from penetrating the weapon system's hardware which then spreading to certain systems to achieve a systemic effect. This is in turn will give high impact to the accomplishment of the military operation in a whole. Table 1 and Table 2 show example of CPSes used NCO/NCW weapon system, the location of vulnerabilities, and some risks of their vulnerabilities.

Table 1. CPSes Weapon System Vulnerabilities

	NCO/NCW Weapon System				
CPS Component	**Navigation**	**Communica-tions**	**Sensors**	**Mission System**	**Diplays and Controls**
Cyber	▪ Processor ▪ Memory ▪ Input/Output	▪ Processor ▪ Memory ▪ Input/Output	▪ Memory ▪ Input/Output ▪ Power Supply	▪ Processor ▪ Memory ▪ Clock Grid	▪ Processor ▪ Memory
Physical	▪ Input/Output ▪ Power Supply	▪ Input/Output ▪ Power Supply	▪ Input/Output ▪ Power Supply	▪ Input/Output ▪ Power Supply	▪ Input/Output ▪ Power Supply
Interface	▪ Input/Output	▪ Input/Output	▪ Input/Output	▪ Input/Output	▪ Input/Output
Network	▪ Processor ▪ Memory	▪ Processor ▪ Memory	▪ Processor ▪ Memory	▪ Processor ▪ Memory	▪ Processor ▪ Memory

Table 2. CPSes Weapon System Types of Attack and Risks

	NCO/NCW Weapon System				
CPS Component	**Navigation**	**Communica-tions**	**Sensors**	**Mission System**	**Diplays and Controls**
Cyber	▪ Information leakage	▪ DoS ▪ Malfunction	▪ Information leakage	▪ DoS ▪ Information leakage	▪ Information leakage
Physical	▪ Degraded performance	▪ Malfunction	▪ Degraded performance	▪ Malfunction	▪ Malfunction
Interface	▪ Malfunction	▪ Malfunction	▪ Malfunction	▪ Malfunction	▪ Malfunction
Network	▪ Malfunction ▪ Information leakage	▪ DoS ▪ Degraded performance ▪ Information leakage	▪ Malfunction ▪ Degraded performance ▪ Information leakage	▪ DoS ▪ Malfunction ▪ Information leakage	▪ DoS ▪ Malfunction

3.5. Challenge to Indonesia Defense and Military Sector

Indonesia is a non-block country and it is one of reasons that Indonesia procured weapon system from two block countries, East Block and West Block. Some new modern weapon systems are NCO/NCW ready. The real challenge is how confident the defense sector that the existing weapon system or the future one are free from hardware trojan. On the other side, local industries have not had yet capabilities to produce high-grade military standard systems especially the systems' hardware. Hardware trojan can be infected from the scratch, that is the first time a chip or IC is designed. It can also be infected at gate level when the designed IC is converted into electronic circuit, or in fabrication phase. The insertion of hardware trojan can be done by compromised engineers or by a machine which is programmed to compromise the chip fabrication. In the era of IoT, externally control of a remote machine can be done from anywhere and anytime by using any device.

Hardware trojan is a real threat for defense and military sectors in the Industry Revolution 4.0, more over if a country still depends on other countries for weapon systems. Indonesia already has components to cope with this hard-to-detect threat which resides within CPS weapon system, such as defense industries, the regulator of defense industry (government), leading universities which already have facilities for IC design and fabrication, and abundance electronic and electrical engineers who are very competence in this field. The main key is how to find the most proper mechanism to make them do collaboration in such field.

4. Concluding Remarks

CPSes have been used in weapon systems long before the introduction of IR4.0 which is shown by the deployment of networked weapon systems using tactical data link as the data communication means. CPS is the generalization of embedded systems with addition that the cyber and the physical components are connected by the internet, which is different from the tactical data link even though they have the same function that is, to make sure the information among nodes flows securely. Modern weapon systems are equipped with CPS in form of advanced electronics systems such as avionics system for modern warfighter aircraft. Any advanced electronics systems consist of many ICs or chips with various function from processing data to inputting or outputting data and displaying information extracted from the data, where these components are very vulnerable to hardware attacks. All CPSes's components can become the target of infected hardware by hardware trojan with the effects that escalates from the infected hardware's systems themselves to systemic attack which can cause system performance degradation or malfunction, to the whole process of an organization.

Hardware trojan attacks to weapon systems certainly not only degrade or malfunction the weapon systems' components but also thwart the military operation and paralyze the defense system. Hardware trojan is hard to detect because it can be brought in during the IC design, IC translation from scratch to gate level, or IC fabrication.

Hardware trojan can do attacks in form of DoS to degrade of malfunction the systems, and leak the secret information by activating certain communication lines to transmit such information to the designated actor. Indonesia's defense and military sectors should be aware with this hard-to-detect threat and optimize their existing resources, as up to this moment the dependent of modern weapon systems from other countries is still high.

References

[1] Alur R 2015 Principles of Cyber-Physical Systems (London: MIT Press)

[2] Alford L D 2010 Cyber warfare: the threat to weapon systems The WSTIAC Quarterly 9 No. 4

[3] Cebrowski A K and Gartska J J 1998 Network-centric warfare: its origin and future, Proceedings of the Naval Institute, January.

[4] US Department of Defense 1997, C4ISR Architecture Framework version 2.0 December 18

[5] US Joint Chief of Staffs 2008 Department of Defense Dictionary of Military and Associated Terms Joint Publication 1-02 Amended May3 0

[6] US Joint Chief of Staffs 2012 Information Operations Joint Publication 3-13 November 27

[7] USAF 2011 Cyberspace Operations Air Force Doctrine Document 3-12 Incorporating change November 30

[8] US Joint Chief of Staffs 2013 Cyberspace Operations Joint Publication 3-12(R) February 5

[9] Denning P J 1989 The ARPANET after twenty years American Scientist 77 pp 530-535

[10] Sumari A D W 2019 Defense applications of blockchain technology Blockchain Jakarta Conference May 2 https://www.researchgate.net/publication/332924862_DEFENSE_APPLICATIONS_OF_BLOCKCHAIN_TECHNOLOGY

[11] Sumari A D W 2007 Network-centric warfare: doktrin tempur era informasi Satria 3 No. 4 pp 90-103

[12] Fromel B 2016 Interface design in cyber-physical system-of-systems Proc. of 2016 11th System of Systems Engineering Conference (SoSE) August 15

[13] Humayed A, Lin J, Li F, and Luo B 2017 Cyber-physical systems security – a survey https://arxiv.org/pdf/1701.04525.pdf

[14] Wang E K, Ye Y, Xu X, Yiu S M, Hui L C K, and Chow K P 2010 Security issues and challenges for cyber physical system Proc. of 2010 IEEE/ACM International Conference on Green Computing and Communications & 2010 IEEE/ACM International Conference on Cyber, Physical and Social Computing pp 733-738

[15] Khaitan S K and McCalley J D 2015 Design Techniques and applications of cyberphysical systems: a survey IEEE Systems Journal 9 , 2 , June

[16] Korea Communications Commission 2008 Malicious software (malware): a security threat to internet economy OECD Ministerial Meeting on the Future of the Internet Economy June 17-18 http://www.oecd.org/sti/40724457.pdf

[17] AFP 2018 China used tiny chips on US computers to steal secrets: report October 4 https://techxplore.com/pdf457866474.pdf

[18] Malicious hardware https://www.pcmag.com/encyclopedia/term/59521/malicious-hardware

[19] Alves T and Morris T 2018 Hardware-based cyber threats Proc. of the 4th International Conference on Information Systems Security and Privacy (ICISSP 2018), pp 259-266

[20] Shield J, Hopkins B, Beaumont M, and North C 2015 Hardware trojans – a systemic threat Proc of the 13th Australasian Information Security Conference (AISC 2015) pp 45-51

[21] Yang K, Hicks M, Dong Q, Austin T, and Sylvester D 2016 A2: analog malicious hardware Proc. of 2016 IEEE Symposium on Security and Privacy (SP) pp 18-37

[22] Wadho L H 2016 Integrated circuits (IC) April 15 https://www.slideshare.net/ LATIFHYDERWadho/integreted-citcuits-ic

[23] Moore G E 1965 Cramming more components onto integrated circuits Electronics 38, Number 8, April 19

[24] Shalf J and Leland R 2015 Computing beyond the end of Moore's law: is it really the end, and what are the alternatives? June 9 https://www.researchgate.net/publication/288855758_ Computing_beyond_Moore's_Law

[25] Courtland R 2017 Intel now packs 100 million transistors in each square millimeter March 30 https://spectrum.ieee.org/nanoclast/semiconductors/processors/intel-now-packs-100-million-transistors-in-each-square-millimeter

[26] Bryant R E. and O'Hallaron D R. 2015 Future of computing: Moore's law & its implications 15-213: Introduction to Computer Systems December 3 https://www.cs.cmu.edu/afs/cs/ academic/class/15213-f15/www/lectures/27-future.pdf

[27] Rajendran J, Gavas E, Jimenez J, Padman V and Karri R 2010 Towards a comprehensive and systematic classification of hardware Trojans Proc. of 2010 IEEE International Symposium on Circuits and Systems pp 1871-1874

[28] Cao X 2015 Hardware Trojan vulnerability Graduate Theses and Dissertations. 14647 https://lib.dr.iastate.edu/etd/14647

[29] Hely D 2012 Hardware Trojans in processor based circuit: from design to countermeasures GDR SoC-SiP – Journée «Sécurité des systems embarqués» Contrefaçons, PUF et Trojans November 12

[30] Karri R, Rajendran J, Rosenfeld K, and Tehranipoor M 2010 Identifying and classifying hardware trojans Computer 43 Issue: 10 October pp 39-46

[31] Bhunia S, Hsiao M, Banga M, and Narasimhan S 2014 Hardware trojan attacks:

threat analysis and countermeasures Proceedings of the IEEE 102 No. 8 August

[32] Wang X, Tehranipoor M and Plusquellic J 2008 Detecting malicious inclusions in secure hardware: challenges and solutions Proc. of 2008 IEEE International Workshop on Hardware-Oriented Security and Trust June 9

[33] Sarwono S and Sumari ADW 2017 Introduction to hardware trojan and cyber-physical systems risks and vulnerabilities: a case in defense sector July 21 https://www.slideshare.net/ ambil/iidss-2017-sarwono-sutikno-arwin-sumari-cps-in-defense

[34] United States Government Accountability Office 2018 Weapon systems cybersecurity: DOD just beginning to grapple with scale of vulnerabilities Report to the Committee on Armed Services, U.S. Senate GAO-19-128 October

Utilization of Smartphone Technology in Military Operations Attack on armed Terrorists in Poso

Mahturai Rian Fitra1 and Arman Sobary2

1University of Indonesia, Jl.Salemba Raya rw 5, Jakarta Pusat and 10430, Indonesia

2University of Indonesia, Jl.Salemba Raya rw 5, Jakarta Pusat and 10430, Indonesia

E-mail: mahturairian@gmail.com

Abstract. The presence of armed terrorist groups in Poso can threaten security conditions in the country, because their activities are considered quite dangerous for the surrounding community. This terrorist group did not hesitate to kill civilians who tried to deny its existence. Therefore, various joint military operations have been launched to crush this armed terrorist group, such as: Camar Maleo and Tinombala. However, until now this terrorist group is difficult to completely destroy, due to the condition of the operating area in the form of dense tropical rainforest and steep slopes. This makes it difficult for troops to carry out chases and hunting. Through smartphone technology, troops are able to read operating field conditions much more easily and can predict far-field conditions in front of them more quickly. The concept used is the incorporation of raster data, vectors and DEM which are processed using GIS (Geographic Information System) software with smartphone devices based on Android. The result is a smartphone device that has been inserted geospatial-based data used by troops in the operating field in the hunt for terrorists.

1. Preface

The hunt for the Santoso terrorist group has not been fully resolved, because it still leaves one of the leaders of a terrorist group named Ali Kalora and several members of his group. Although it has no influence as big as Santoso, who was killed in the Tinombala operation. However, Ali Kalora also has advantages in terms of affiliations with terrorist groups in Mindanao (Philippines) and Bima (West Nusa Tenggara).

The TNI-POLRI Joint Force continues to look for the presence of Ali Kalora and his followers, but the traces of this terrorist group are difficult to detect. This terrorist group deliberately moved and was able to hide in the dense jungle. In addition, the heavy terrain that must be passed also makes the search process more difficult to do. Moreover, the joint forces serving in Poso often experience exchanges with the new troops on duty. As a result, the ability to read the terrain conditions in the operating area is very limited.

Beginning The digital age created the latest innovations in helping carry out the task of joint forces in the operating field. Initially the troops on duty were equipped with GPS Navigation such as: Garmin GPS 62s, Garmin 63s, Garmin eTrex Touch 35, and Montana 680. Navigation in closed terrain can utilize an Android-based smartphone device. All terrain data in raster, vector and DEM (Digital Elevation Model) operating areas can be combined with these smartphone devices. The use of smartphone devices can certainly be more effective and efficient, because most soldiers are used to using them and are easily operated.

2. Research Methodology

2.1. Literature Review

The researcher tried to find references related to the research topic, so that reference sources were found that were considered capable of helping researchers to carry out research. There are main points that are of particular concern to researchers, including: Security Patrols Constrained by Terrain Conditions of the Extreme Earth Surface, Spatial Data Models, and Android Offline GPS Application Integration. The following will be briefly described.

2.1.1. Security Patrol Constrained by Extreme Terrain Conditions. Terrain forms on the surface of the Poso region are dominated by steep hills and mountains, in addition there is also very thick vegetation cover of tropical rain forests. So that patrol can only be carried out within a limited radius. Soldiers carrying out security patrols in border areas are hampered by landscape barriers in the form of steep and steep slopes. Based on the theory put forward by Van Zuidam in 1985, there are several classes of slope that can be classified [Table.1].

2.1.2. Spatial Data Model. Spatial data has the meaning as a data that refers to positions, objects, and relationships including in the space of the earth. Spatial data is one item of information, wherein there is information about the earth including the surface of the earth, below the surface of the earth, waters, the ocean and under the atmosphere (Rajabidfard and Williamson, 2000). The use of the geospatial data model is indeed not quite popular in the military, certainly more due to a lack of Human Resources

(HR) with a background in the field of geography or geodesy. One simple spatial data model that can be used is by utilizing Digital Elevation Model (DEM) data. This data has many advantages, especially for making terrains in 3 dimensions and making the slope class. The following is an example of DEM data that has been processed [Figure. 1] and [Figure. 2].

2.1.3. Offline Android GPS Application. Smartphone technology has developed very rapidly and has been widely used by the public, as evidenced by the release carried out by the digital marketing research agency Emarketer, which stated that in 2018 the number of active smartphone users reached 100 million people. Indonesia's position is the fourth largest in the world after China, India and America. The integration of the spatial model into the smartphone device in question is a spatial data synchronization method that has been processed into an offline GPS application based on android. The offline GPS application has the ability to update real time positions without internet connection. An example is the Avenza Maps application. The offline GPS feature on smartphones has many advantages compared to handheld GPS navigation (Garmin 62s or 63s). The advantage lies in the ease in the data customization process, so that spatial data in shapefile (shp) and pdf format can be entered into a smartphone device [Figure. 3].

2.2. Research Methods

This research is explorative in the form of three-dimensional modeling and geospatial analysis of modified slope data. The general description of research activities from the beginning to the end, can be illustrated in broad outline through the flow of research activities that have been systematically designed below [Figure. 4].

Initial research activities, starting with collecting references and scientific sources that can be used as references, information related to research can be sourced from trusted online sources, reading books, and scientific journals. The reason for using online resources is that there have not been many similar studies that have been developed for the military. In addition, the problems raised by the author are mostly found in online writing sources.

Next is the collection of data needed in supporting research. The data collected in the form of: High-resolution Satellite Image Data and DEM Data (Digital Elevation Model). The data that has been processed with the GIS (Geographic Information System) device is used to solve various problems related to the implementation of troop mobilization in the RI-Malaysia border region in Kalimantan.

Smartphone devices can be combined with spatial data from processing results that are in shapefile (shp) and pdf format. Through an android-based offline gps application, navigation in carrying out security mobilization and patrol can be done without relying on internet connections. An example of an application that can be used is Avenza Maps, this application has an attractive and easy display for customization.This research is the initial stage in the development of closed terrain navigation methods, so that in the future new ideas are expected to emerge that can complement various shortcomings in this study.

2.3. Results and Conclusions

This research produces various kinds of outputs derived from derivatives from DEM (Digital Elevation Model) data, including contour data and slope grade data. Therefore, a type of DEM data is needed that has good spatial resolution, so that the accuracy of detailed topographic elevation data can be obtained with a resolution that can reach below 0.25 meters.

2.3.1. Combination of Topographic Maps and DEM (Digital Elevation Model). The picture above is a display of the results of the data input process in GIS (Geographic Information System) software. The above DEM data has AOI (Area of Interest) in the Republic of Indonesia-Malaysia border region of North Kalimantan. If we look at it, the difference between the lowlands and the hills can be seen clearly and the borders of the country are always on the igir or hilltops. This can be taken into consideration by the commander of the forces in planning troop mobilization towards the boundary line, because carefulness is needed in determining which segments will be passed.

Topographic maps are a type of map that becomes a standard for troops and absolutely must be possessed before conducting an assignment operation, especially in the border region. Sometimes for ordinary people do not have the ability to interpret the map, so that the display of maps that are too complicated will increasingly confuse the warrior in navigating in a closed field. The combination of Topographic Maps and DEM is the first step to simplify the map interpretation process, where the appearance of Topographic Maps will look closer to the actual conditions in the field [Figure. 5] and [Figure. 6].

2.3.2. Simulation of the Troop Mobilization Plan. Utilization of a combination of Topographic Maps and DEM data can be made a simulation of troop mobilization, for example the troops move from the Start Point to the Target there are several recommendation lines available, the task is to determine which path is more effective and efficient in achieving the target [Figure. 7]. The results show in the first track simulation, the distance traveled is 10.11 km and the elevation is between 125 m - 625 m. It can also be seen that in the first 2.5 km the slope is the greatest, so the soldiers need to consider saving energy and logistics in traveling a distance of 10.11 km. In addition, it can be obtained an overview of any segment that needs to be slowed or accelerated based on the graph analysis above [Figure. 8].

The results show the first path simulation, the distance traveled as far as 9.93 km and the elevation between 125 m - 625 m. Although the distance traveled is much closer, it should be noted when you are at a distance of 3 km - 5 km. Soldiers will have difficulty passing through the up and down fields and will drain a lot of energy.

Both simulation 1 and simulation 2 are a means of consideration for the commander in planning mobilization towards the target to be achieved, so that the forces are more effective and efficient in mobilizing. The results shown in simulation 1 look more effective and efficient than simulation 2. This makes simulation 1 the best choice in the plan for mobilizing troops.

2.3.3. Transfer to Android App Offline GPS. The best tracking path simulation can be transferred to each soldier's smartphone device in the field, so that the best route guideline that has been planned will appear. Based on the experience of researchers while carrying out assignments in the border region along with border security forces, the use of this android-based offline gps application is more in demand than conventional GPS. There are a number of underlying reasons, including: easy to use by ordinary people, a more attractive appearance, rich in modification features, and the average device is owned by soldiers [Figure. 9]. This study uses a Base Map in the form of a Topographic Map of the Poso region, which is usually used as the main map in border security activities. The input results on smartphone devices show success and can be used by soldiers on duty in the field to achieve the specified target.

2.3.4. Conclusions. Researchers can draw conclusions about research conducted on the use of smartphone technology for troops in closed terrain, especially the Poso region.

- This research method is suitable for troops who mobilize in closed fields and there is no GSM signal.
- Making tracking or navigation paths adjusted to DEM (Digital Elevation Model) data and information on Topographic Maps.
- The use of smartphones as a navigation aid is far more effective and easier than conventional GPS.
- The results of research and trials show success, so that it can be used for soldiers who are on duty in the field.

3. Figures

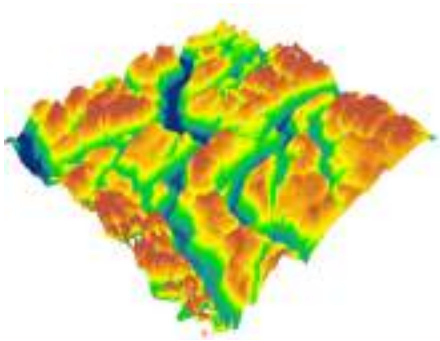


Figure 1. DEM Data Model

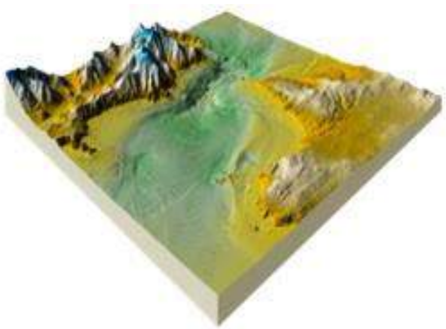


Figure 2. DEM Data Model

Figure 3. Offline GPS application.

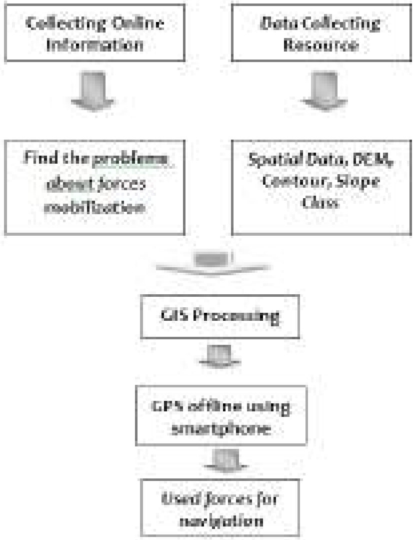

Collecting Online Information
Data Collecting Resource
Find the problems about forces mobilization
Spatial Data, DEM, Contour, Slope Class
GIS Processing
GPS offline using smartphone
Used forces for navigation

Figure 4. Research flow chart.

Figure 5. Topographic Maps

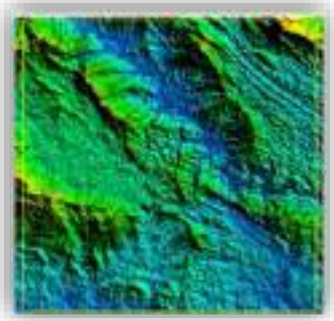


Figure 6. DEM Data Model

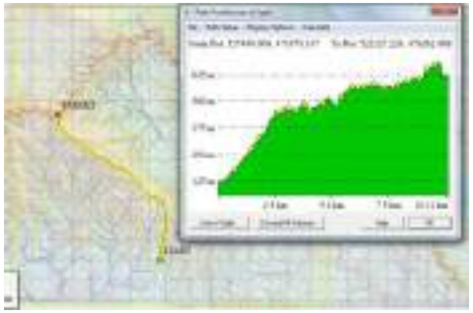


Figure 7. Navigation Path Simulation 1

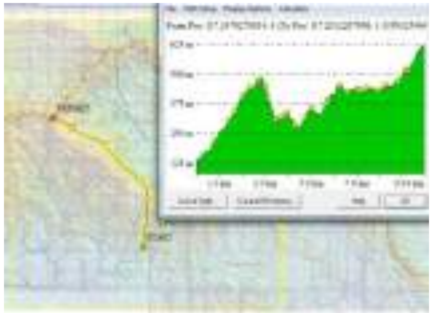


Figure 8. Navigation Path Simulation 2

Figure 9. Map Display on a Smartphone

4. Tables

Table 1. Slope Class (Van Zuidam in 1985)

Slope grade	Topo graphy	Explanation
0-2° (0-2 %)	flat	Flat or almost flat, no erosion big ones, can be processed easily in dry conditions.
2-4° (2-7 %)	declivous	The land has a sloping slope, in the event of a landslide move with low speed, erosion and erosion will leave a very scar in.
4-8° (7-15 %)	sloping	The land has a sloping slope to steep, if there is a landslide moving at low speed, very prone to erosion.
8-16° (15-30 %)	rather steep	The land has a slope which is steep, prone to danger of landslides, surface erosion and groove erosion.
16-35° (30-70 %)	steep	The land has a slope which is steep to steep, frequent erosion and ground motion with speed slowly. Vulnerable area erosion and landslides
35-55° (0-2 %)	very steep	The land has a slope which is steep, often found outcrops rocks, prone to erosion.
>55° (>140%)	very very steep	The land has a slope which is steep, rock outcrops appear on surface, prone to landslides rock.

References

[1] Budi Winarto, 2014, Dinamika Isu-isu Global Kontenporer, Penerbit CAPS (Center of Academic Publishing Service), Yogyakarta

[2] Muta'ali, L.,Marwasta, D., dan Christanto, J. (2018). Pengelolaan Wilayah Perbatasan NKRI. Yogyakarta: UGM PRESS

[3] Rajabidfard, Abbas, and I.P. Williamson. 2000, "Spatial Data Infrastructures : Concept, SDI Hierarchy and Future Directions." Melbourne, Victoria: Spatial Data Research Group, Department of Geomatics, The University of Melbourne

[4] Rizal Sukma, 2003, CSIS Jakarta, POSTUR PERTAHANAN INDONESIA

[5] Zuidam, R.A. Van.. 1985. Aerial Photo-Interpretation in Terrain Analysis and Geomorphology Mapping. Smith Publisher The Hague, ITC

[6] Kusnanto Anggoro said in the Focus Group Discussion held by the IPSK LIPI Border Team,

Jakarta, October 31, 2013

[7] https://www.beritasatu.com/nasional/530706/pengejaran-ali-kalora-dan-pengikutnya-terkendala-medan-sulit. Accessed Mei 18, 2019 at 00.45 WIB

[8] https://nasional.republika.co.id/berita/nasional/hukum/19/01/02/pkov20428-perburuan-ali-kalora-cs-terkendala-medan-sulit. Accessed Mei 18, 2019 at 00.50 WIB

[9] https://gisgeography.com/free-global-dem-data-sources/. Accessed April 23, 2019 at 16.45 WIB

[10] http://terra-image.com/dem-resolusi-tinggi-terrasar-x/ Accessed April 24, 2019 at 10.00 WIB

Cumulonimbus Prediction in Aerodrome Area using Integration of Radar and J48 Algorithm – IIDSS2019

Furqon Alfahmi1, Oky S Hakim2, Ratna C Dewi3 and Amrya Khaerima4

1Center for Marine, Indonesian Agency for Meteorology Climatology and Geophysics, Jl Angkasa I No 2
Kemayoran, Central Jakarta 10720, Indonesia

2Juanda Meteorological Station, Jl Bandar Udara Juanda, Sidoarjo 61253, Indonesia

3Perak II Meteorological Station, Jl Kalimas Baru No 97B, Surabaya 60165, Indonesia

4Bogor Climatological Station, Jl Alternatif IPB, Bogor 16001, West Java, Indonesia

E-mail: pelovom@gmail.com

Abstract. Cumulonimbus is a cloud that causes bad weather phenomena and is dangerous for the aviation world. At Juanda Airport, Surabaya records 64 days throughout the rainy season in December 2018 to February 2019 with Cumulonimbus clouds having the potential to the thunderstorm. In order to realize zero accidents, mitigation efforts must be carried out. Anticipation in forecast information can use the Cell Centroid Tracking (CTR) Product from the Gematronic Radar. The CTR product generates Cumulonimbus cloud characteristic information, namely the central position of the storm, maximum reflectivity value, cell size, and movement speed of the Cumulonimbus cloud. Improved accuracy of forecast results can be helped by data mining classification techniques using the JRip algorithm. Percent Correct, Root Mean Square Error, False Alarm Ratio, and Bias can be used as a reference to test the accuracy of the model. Integration of CTR with JRip algorithm for real-time data obtained an accuracy value of 74.65%. The application of the integrated model in the forecasts for the next 10 minutes can predict Cumulonimbus with the right thunderstorm potential to reach 72%. The factor of the storm central position is a major determinant of thunderstorm potential of the Cumulonimbus cloud.

Introduction

A Cumulonimbus cloud is a type of convective cloud with large vertical thickness and contains a mixture of ice crystals at the top and drops of water at the bottom. Cumulonimbus clouds have a dark colour at the mature stage. The life span of Cumulonimbus clouds ranges from 2 hours with an altitude of 2,000 - 16,000 m or the equivalent of 6,500 - 60,000 feet [8]. The distinctive feature of Cloud Cumulonimbus is lightning and lightning produced because other types of clouds can't produce it

Cumulonimbus clouds are a type of cloud that has a high potential for damage. Natural events caused by these types of clouds include the temperature of the air down, gusts of strong winds, and heavy rain that can be accompanied by thunderstorms [7]. The significant growth of Cumulonimbus clouds has the potential to produce rain with heavy to extreme intensity, which can affect flooding and landslides in vulnerable areas. The effect of rainfall in generating landslides is something that is clear, although it is very difficult to explain precisely [1]. In addition, there are processes such as turbulence and icing on the inside of this type of cloud [7] which are very much aware of flight navigation.

The process of turbulence in cumulonimbus clouds with certain strengths can damage the fuselage, while the icing process at certain temperatures and certain conditions can interfere with the performance of aircraft engines [7]. Cumulonimbus clouds can produce vertical movement that can be updraft or downdraft. In addition, ice particles in Cumulonimbus clouds can freeze aircraft parts and most often produce lightning that can disrupt electrical systems and aircraft navigation [7]. Therefore, in take-off and landing interests, only the Cumulonimbus cloud types that must be reported in the METAR news and their appearance must be immediately made in the SPECI news.

Cumulonimbus cloud growth can be detected using remote sensing, one of which is the Doppler Weather Radar. Doppler Weather Radar can be used for studies of cloud growth and detecting rain [10]. Weather radar can even detect hail events through analysis and interpretation of reflectivity images, radial velocity, and spectral width [2,4,6]. One of the Doppler weather radars is Gematronic Radar with Rainbow's default application. In Rainbow, there is Cell Centroid Tracking (CTR) product that can be used to track and nowcasting of Cumulonimbus cloud movement. CTR products provide information on Cumulonimbus cloud characteristics including maximum reflectivity, coverage area, position, and movement speed.

Based on Cumulonimbus cloud characteristic information obtained from CTR products, it can be integrated with data mining classification techniques for the needs of nowcasting in severe weather. One algorithm in the data mining classification technique is J48. The J48 algorithm implements the C4.5 algorithm [5]. If the J48 algorithm is compared to NBTree, it can be concluded that J48's performance is better and the accuracy level produced by J48 is higher and consumes less computational time [3]. The JRip algorithm is different of the J48 class in the package classifier in the WEKA data mining application. This class implements a propositional rule learner, Repeated Incremental Pruning to Produce Error Reduction

(RIPPER), which was proposed by William W. Cohen as an optimized version of IREP [9].

It is expected that Cumulonimbus's cloud characteristic information from the radar cell centroid tracking processed by the J48 algorithm classification technique can obtain threshold values of bad weather. Furthermore, the threshold value is applied to nowcasting from cell centroid tracking products as a preventive measure. The legislature in April 2007 passed two laws, the Disaster Management Act [11] and the Spatial Planning Act [12] which was a revision of the previous law, namely Number 24 of 1992 which shows, that disaster risk management policies are handled comprehensively and emphasized on preventive efforts, namely not only during natural disasters. The existence of bad weather forecast information will be very helpful in mitigation efforts to realize zero accidents.

Method

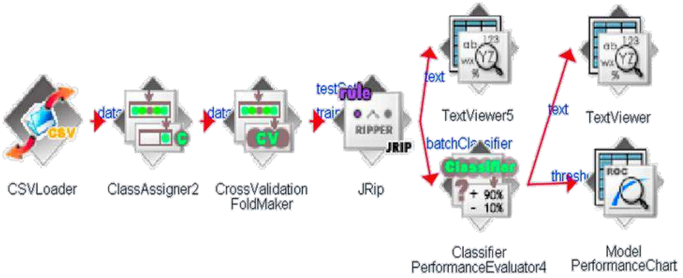


Figure 1. WEKA Knowledge Flow Environment using JRip classifier.

Weather radar at Juanda Airport uses Gematronic Radar. Radar data processing to become a product is used by default application, Rainbow. The radar product that will be utilized to analysis and predict Cumulonimbus's cloud growth potential is Cell Centroid Tracking (CTR). The radar data taken for this case study is data throughout the rainy season from December 2018 to February 2019.

CTR products are set to predict Cumulonimbus's growth potential for 30 minutes ahead with a 10 minutes time step based on input data 1 hour earlier. There are 4 types of CTR output, namely +00 minutes analysis, +10 minutes forecast, +20 minutes forecast, and +30 minutes forecast. The final product of the CTR is exported in CSV format.

The output of the analysis of +00 minutes was further processed with data mining classification techniques to identify the potential of Cumulonimbus clouds which had an impact on thunderstorm events. Factors taken into account for classifying clouds with potentially thunderstorms are maximum cloud reflectivity values, cloud distance from Juanda Airport, cloud size and speed of cloud movement. The classification is helped by using WEKA machine learning. In WEKA there is a classification algorithm that is used to test these factors in classifying clouds with potential thunderstorms according to the plot in Figure 1. The JRip algorithm is chosen to be integrated with CTR radar products because it has good accuracy compared to other classification algorithms.

The algorithms are then validated using the K-Fold Cross Validation method with number of folds is 10. Therefore 10 algorithms are resulted and calculated the accuracy of integrated model. The best algorithm is applied in +10 minutes forecast, +20 minutes forecast, and +30 minutes forecast. The accuracy and reliability values are calculated using Percent Correct (PC) in (1), False Alarm Ratio (FAR) in (2), Root Mean Square Error (RMSE) in (3) and BIAS in (4).

$$PC = \frac{Hits+Correct\ Negative}{N} \qquad (1)$$

$$FAR = \frac{False\ Alarm+Hits}{False\ Alarm} \qquad (2)$$

$$\mathrm{RMSE} = \sqrt{\frac{1}{\mathrm{N}}\sum_{\mathrm{i}=1}^{\mathrm{N}}(\mathrm{f_i}\text{-}\mathrm{o_i})^2} \qquad (3)$$

$$\mathrm{BIAS} = \frac{1}{\mathrm{N}}\sum_{\mathrm{i}=1}^{\mathrm{N}}(\mathrm{f_i}\text{-}\mathrm{o_i}) \qquad (4)$$

Where:

Hits = when predicted to occur and true occur

False alarm = if it is expected to occur but does not occur

Misses = when it is estimated that nothing happened but happened

Correrct negatives = if not expected to occur and true does not occur

N = amount of data

f = approximate value

o = observation value

Discussion

Characteristics of Growing Cumulonimbus Clouds near the Juanda Airport Area

In the rainy season in December 2018 to February 2019, CTR products recorded 3,455 images per 10 minutes that detected Cumulonimbus cloud growth within a radius of ≤ 25 km from Juanda Airport. Recorded 1,214 out of 3,455 images per 10 minutes impacted the thunderstorm phenomenon. It is interesting to know what distinguishes between Cumulonimbus clouds that have the potential to thunderstorm and which have no potential thunderstorm. CTR products produce output in the form of observed cloud characteristics data, including the distance of the central cloud to Juanda Airport, maximum cloud reflectivity value, Size of cloud coverage area and speed of cloud movement.

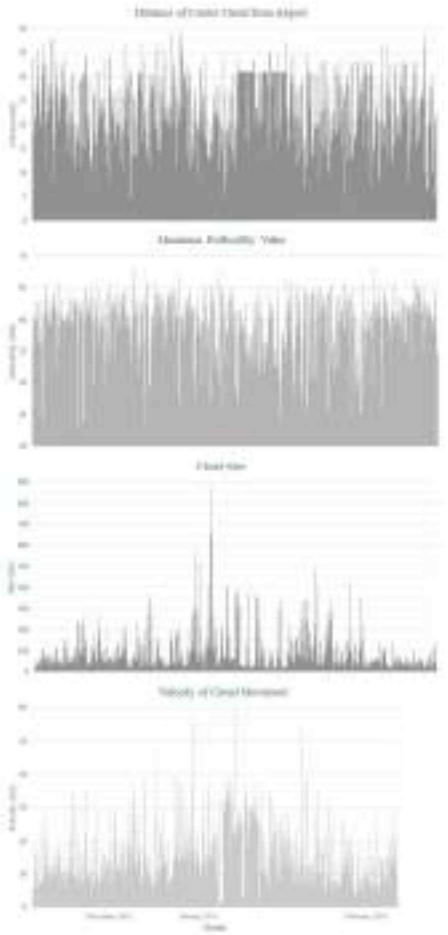


Figure 2. Cloud characteristics of CTR radar products: (a) Distance, (b) Maximum Reflectivity, (c) Size, and (d) Speed of Movement.

In Figure 2 the central cloud is recorded at the airport closest to 0.25 km on December 2nd at 21.20 UTC, which affects Thunderstorm. Conversely, the central cloud distance from the radar has the greatest impact on Thunderstorm within 39.43 km on January 12th at 06.30 UTC. At this time, it was also the record of the smallest cloud coverage, which was 6.62 km^2, while the largest area of 870.37 km^2 occurred on January 17th at 15.30 UTC which had an impact on the norm. In the cloud movement velocity characteristics, the fastest value was recorded at 59 m/s on January 24th at 10.40 UTC which had an impact on the norm. Different things are shown at the maximum cloud reflectivity value, where there are 3 smallest values of 40.0 dBz which have different effects. On January 3rd at 11.50 UTC and January 15th at 13.30 UTC there is no impact on thunderstorm while on January 16th at 09.30 UTC has an impact on thunderstorm. Besides that, the maximum cloud reflectivity value of 68 dBz on December 26th at 09.30 UTC had an impact on the thunderstorm.

The difference in the effect of Cumulonimbus has the potential Thunderstorm or not at the same reflectivity value, giving rise to the suspicion of a combination of relationships between factors with each other. The criteria of factor relationship to difference clouds with thunderstorm effects or not, are interesting to study further. The criteria produced must be able to separate 1,214 thunderstorm events and 2,241 non-thunderstorm events from Cumulonimbus clouds monitored on CTR products.

Integration of CTR Products and JRip Algorithms

The results of the JRip algorithm classification stated that 2,579 of 3,455 Cumulonimbus clouds that were monitored by thunderstorm potential could be detected correctly. The 10 JRip algorithms obtained according to the number of iterations selected in the validation process. The JRip algorithm is able to integrate well with CTR products with the overall value of PC is 74.65% and RMSE is 0.43%. Among the accuracy values of the 10 JRip algorithms that ignored the data in Figure 3, the JRip 4 algorithm has the best value.

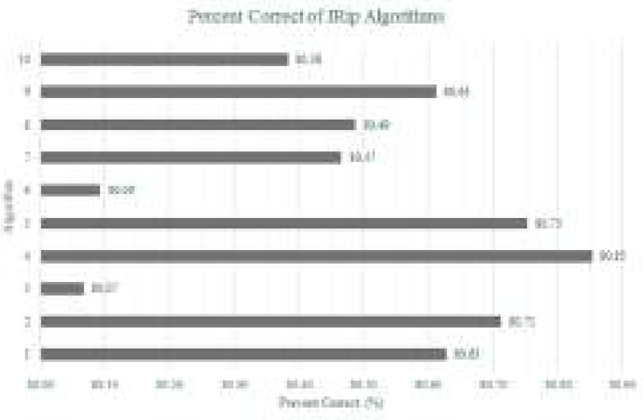


Figure 3. PC value of 10 JRip Algorithms Output Integration Results with CTR Product Analysis +00.

In the JRip 4 algorithm chosen to be integrated with the CTR forecast results, it is stated that there are 3 Cumulonimbus cloud criteria that have the potential to the thunderstorm. The first criteria only based on 2 factors, namely if the cloud central distance from the airport is ≤ 11,087 km and the size of the cloud coverage area is ≥ 32.15 km^2. The second criteria also have 2 factors, namely the cloud central distance from the airport ≤ 16,545 km and the size of the cloud coverage area ≥ 49.83 km^2. The third criterion has 3 factors, namely the cloud central distance from the airport ≤ 17,878 km, cloud coverage area ≥ 30.49 km^2 and cloud movement speed ≥ 13 m s.

JRip 4 is a classification algorithm that will be selected to be integrated with CTR products in predicting thunderstorm potential. In the algorithm, the cloud central distance factor from radar and the extent of cloud coverage are the main factors in predicting thunderstorm potential. Conversely, the speed factor of cloud movement is the least influential factor. The maximum cloud reflectivity factor is not taken into account in this algorithm, which means that this factor has no effect on thunderstorm potential in Cumulonimbus clouds.

Predicted Cumulonimbus Cloud with Potentially Thunderstorm

In the application to predict Cumulonimbus clouds with potentially thunderstorm, the best accuracy value of 72% is obtained for the next 10 minutes. The accuracy of the model decreases as the time span of the forecast increases linearly. But the difference in the value of accuracy is not too much different, only 2% at odds for the next 20 minutes and 6% for the next 30 minutes.

Similar results obtained Bias value which is also linear with time. The bias value for the next 10 minutes is only 0.37 to approach the perfect value. The results are not much different indicated by forecasts for the next 20 and 30 minutes, which are respectively 0.39 and 0.47 to approach the perfect value. But the output model results are always stable and underestimate in predicting.

Different results are indicated by the FAR value which is stable for up to 30 minutes. The FAR value is obtained by 26% for the next 10, 20 or 30 minutes.

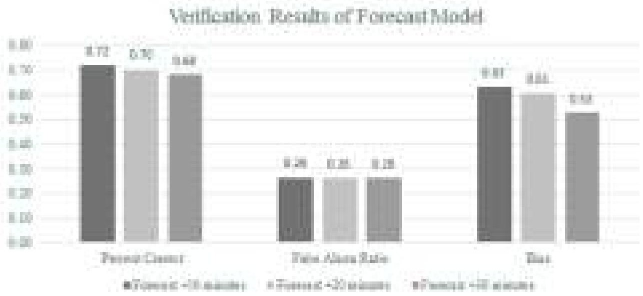


Figure 4. Comparison of the results of verification of the forecast models +10, +20, and +30 minutes with PC, FAR, and Bias values.

The results of applying the integration model in the forecasts of 10, 20 and 30 minutes in the future produce output values of accuracy and bias that have a negative linear relationship with time. This relationship means that the longer the time span in predicting, the more accurate the value of bias and bias away from perfect values. The model forecast results can be relied on especially for the next 10 minutes, because only 2.67% of the accuracy value of the real time analysis results.

Conclusion

Based on the integration results of CTR radar product with data mining technique classification of JRip algorithm obtained a model that consists of 3 rules. The application of rules get 3conclusions are as follows:

The characteristics of Cumulonimbus clouds which are the determining factors for predicting the presence of thunderstorm potential based on the JRip 4 algorithm are the cloud central distance, cloud size, and speed of cloud movement.

The most important factor for predicting thunderstorm potential is the distance of the Cumulonimbus cloud central from Juanda Airport, with a maximum distance threshold of 17,878 km.

In applying the model to predict Cumulonimbus clouds that have the potential to thunderstorm up to the next 30 minutes, the value of accuracy ranges from 68% to 72% which has a negative linear relationship with increasing time span forecasts.

Acknowledgements

We feel helpful for all those who have supported the availability of data, especially the aeronautical meteorological officer in Juanda Airport for the acquisition of data radar.

References

[1]. Blong R J and Dunkerley D L 1976 Landslides in the Razorback area New South Wales Australia Geogr Ann Vol 58A pp 139–149.

[2]. Bottenheim J W Peter C B Tom F D Daniel K W Fred K. Allan J G Kurt G A H Allan W 1997 Non-Methane Hydrocarbons and CO during Pacific '93 Atmospheric Environment Vol 31 no 14 pp 2079 – 2087.

[3]. Diwandari S and Setiawan N A 2015 Perbandingan Algoritme J48 Dan Nbtree Untuk Klasifikasi Diagnosa Penyakit Pada Soybean Seminar Nasional Teknologi Informasi dan Komunikasi 2015 (SENTIKA 2015) Yogyakarta.

[4]. Gros V Kostas T Bernard B Maria K Casimiro P 2002 Factors controlling the Diurnal variation of CO above a forested area in Southeast Europe Atmospheric Environment 36 pp 3127 – 3135.

[5]. Kunang Y N and Andri A 2013 Implementasi Teknik Data Mining Untuk Memprediksi Tingkat Kelulusan Mahasiswa Pada Universitas Bina Darma Palembang. Seminar Nasional Informatika 2013 UPN "Veteran" Yogyakarta.

[6]. Mollmann-Coers M Dieter K Katja M Franz S 2002 Statistical study of the diurnal variation of modeled and measured NMHC contribution Atmospheric Environment 36 Supplement No 1 S109 – S122

[7]. Pertiwi B D 2018 Analisis Karakteristik Awan Cumulonimbus Menggunakan Citra Satelit dan Data Cuaca Permukaan Wilayah Banyuwangi (Studi Kasus di Stasiun Meteorologi Kelas III BMKG Banyuwangi). Fakultas Matematika dan Ilmu Pengetahuan Alam Universitas Negeri Yogyakarta

[8]. Rusandi R Klimatologi Paper Awan Retrieved from http://www.slideshare.net/RioRusandi92/klimatologi-paper-awan

[9]. Ross J 1992 Quinlan: Learning with Continuous Classes 5th Australian Joint Conference on Artificial Intelligence (Singapore) pp 343-348

[10]. Sinatra T Noersomadi Nugroho G A 2015 Mengenal Tentang Transportable Radar Cuaca Doppler X-Band Media Dirgantara Vol 10 No 4 Desember 2015 Jakarta

[11]. Undang-undang No 24 Tahun 2007 tentang Penanggulangan Bencana

[12]. Undang-Undang No 26 Tahun 2007 tentang PenataanRuang

Natural Defence of Cyber Security for Facing Cyber Attack Threats: Defence of Cyberspace Users

Riska Nurtantyo Sarbini1,*, Rizky Arief Shobirin1, Supriyono1

1Islamic University of Kadiri, Jl. Sersan Suharmaji No. 38, Kediri 64128, Indonesia

*Corresponding e-mail: riskanurtantyosarbini@gmail.com

Abstract. The pattern of the information technology development recently has been made major changes to the society perspective. At present, interactions between humans cannot be limited physically, because of flexibility interactions for each other through media information systems. It is not only on a small scope, but also a wide scope which in this case between countries. All communication forms are limitless, so strategies and protocols are needed in facing the era of cyber communication for national defence. Cyberspace should be a strategic area for state sovereignty, where the defence approach is applied out on users of cyberspace.

Introduction

In the last decade the pattern of the information technology development has been successfully made major changes towards society perspective. It is because humans have been facilitated by media information system, so interactions between humans cannot be limited anymore physically. It is been transpired in wide scope around countries in the world, so it is not only occurred in a small scope. Strategies and protocols are needed in facing the era of cyber communication for national defence, because all forms of communication are limitless.

Cyberspace normatively should be a strategic area for sovereignty of national state. At the present time, the emergence of the Internet and its relations are integrated with the pattern of human growth development from administration to financial sector. Cyberspace is a space created by the emergence of internet that supports each other in living interactions, e.g. in politics, finance, governments and so on.

Nowadays upper and lower currents news broadcasted massively through Cyberspace, which is spread widely in a moment without going through the regulation and supervision of news broadcasting. In several hours it can spread to all people in a country. Indeed, in the end news removal and damping can be performed and being done, however if the social climate is not right, it will potentially offer chaos effect. This news cannot be directly reviewed and ceased by news readers; subsequently it is feared to be false news which potentially divisive state unity of the countries.

Fake news is currently being a powerful weapon which is very fast, cheap and effective in driving public perspective with demanded issues. Hence, the news readers are determinant who must be provided further knowledge intended to preserve create chaos in cyberspace. In this paper we would like to propose a method of defence approach to cyberspace naturally from the side of cyberspace user.

Concept of Cyber Security Strategy

The security portion has been experiencing significant development during the last decades. Fundamental understanding of post-cold war security is unlike armed relations or cooperation between countries, yet also centralised on security for public society [1]. Arnold Wolfers in Perwita & Yani [1] defines security as follows, "Security, in any objective sense, measures the absence of values and in subjective sense, the absence of fear that such values will be tacked". Steven Spiegel in Winarno [2], explained that the expansion definition of national security has consequence of threats increasing: nuclear, economic, social and cultural sectors. The concept of security could be illustrated on following figure (Fig. 1) [2],

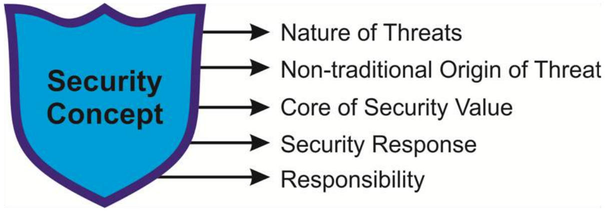


Figure 1. Security Concept, adapted from Winarno

Figure 1 shows that if viewed from the dimensions of the origin of threats, the threat can come from domestic. For examples, the threats are primordial issues related to race, ethnicity, group and religion. Threats may also come from global environment, which carried out by state and non-state actors. The next dimension is nature of threats if the threat to traditional security is military. However, as the era of threat grows, it may become much more complicated not only military in nature. It is also a threat that is non-military in nature, or related to economic, social, cultural, environmental aspects, human rights and other security issues which are more comprehensive.

Meanwhile, Strategy which promoted by John P. Lovell [3] was defined as "A series of steps or decisions which were designed beforehand in a competitive situation where the end result is not merely chancy". Strategy is a method used to achieve a goal or interest by using available power, including military power. In foreign policy, strategy is a pattern of planning that is used by decision makers to advance and achieve their national interests accompanied by efforts to prevent others from doing collisions or inhibiting the achievement of those interests.

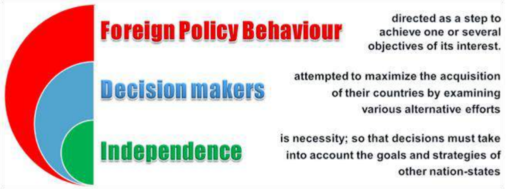

Foreign Policy Behaviour
directed as a step to achieve one or several objectives of its interest.
Decision makers
attempted to maximize the acquisition of their countries by examining various alternative efforts
Independence
is necessity; so that decisions must take into account the goals and strategies of other nation-states

Figure 3. Generated concept of strategy theory, according to the references [3].

There are three assumptions from the theory of strategy, which well-addressed by Figure 2 [3],

1. The foreign policy behaviour of a nation-state must be directed as a step to achieve one or several objectives of its interest.

2. Decision makers always attempted to maximize the acquisition of their countries by examining various alternative efforts, each of which is assessed based on cost and yield analysis.

3. In this world, interdependence is necessity; so that decisions must take into account the goals and strategies of other nation-states.

Cyberspace in National Security

There are many terminologies and interpretations which can be related to the concept of "cyber security". It is because cyberspace is a virtual space formed from the results of the union between humans and technology. The technology in question is technology of information and communication [4]. So the concept of cyber security no longer only touches the technology area, but has become threat towards national security. In fact, national security is very rarely associated with technology. However, along with the increasing threat of domestic and international cyber attacks on public and private infrastructure, the awareness to popularise that cyberspace security is not merely a simple matter of password protection. Moreover cyber security requires a series of strategies because it involves national interests.

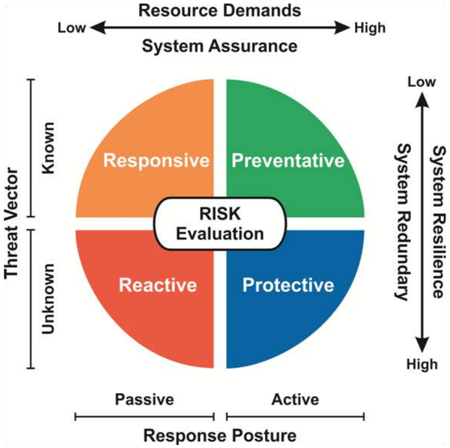


Figure 3. Risk Security Framing, according to the references [4-6].

The development of information technology has also provided significant changes regarding the concept of security. For now, the space for interaction cannot be limited physically but also extends to cyberspace. Consequently, the nation state ought to adapt to this information technology development, the concept of cyber security (cyber security) is time to be set as one of the "territories" of the state that safeguards its security as well as the state's obligation to secure its territory. Moreover, cyber attacks were not only occurred in public institutions, but also attack government institutions [4].

Cyber security cannot be abstracted for more from its implementation area and socio-cultural environment. Unfortunately, simple and significant validation of prevention is sometimes heavy enough to be identified. Determining strategic decisions is very important to understand the challenges posed by cyberspace and develop mitigation strategies to respond, as shown in Figure 2 [4].

Figure 3 shows the relationship between threat posture and response leads to four alternative approaches to cyber defence that will have a significant impact on the threats that came. If the threat that comes is blurred, then the point of attack will be unknown, and so much redundancy or process development is defined first. Prevention efforts will be in vain.

By understanding these problems, it is important if we firstly provide experience for users of cyber space. Understanding the impact of cyber events in this sequence is very important to understand the known risks, which described on bellowed figure (Fig. 3) [4].

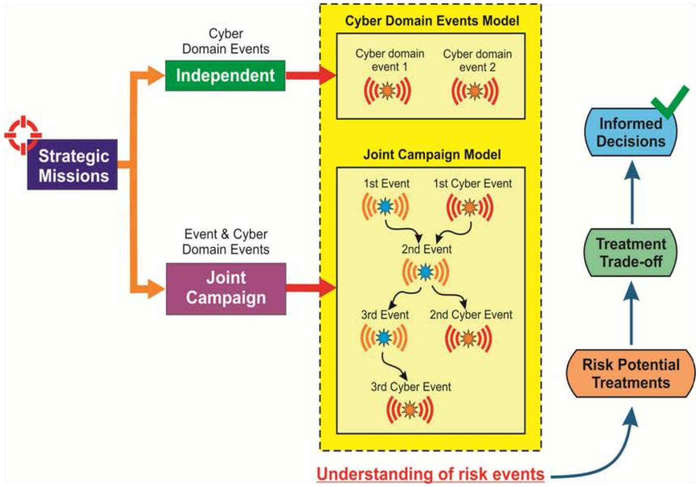


Figure 4. Schematic illustration for understanding all cyber events and the linkages to strategic mission, refer to Ween, *et.al*. [4] and Garvey [7].

From Figure 4, it can be seen that the distribution pattern of news attacks is spread across many targets. If there is no preventive measures are taken against destructive attacks, chaos will be occurred in the early stages of cyber attacks. This won't be happened if cyber space users have sufficient knowledge by providing good education to users of cyberspace, providing information transparency that is clarifying and constructive, there is a central information service that is easily accessible and always provides updated information.

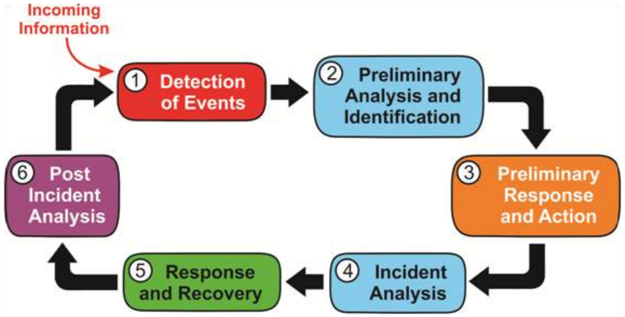


Figure 4. US's Department of Defense (DoD) Cyber Incident Handling Life Cycle (CIHLC) (CJCSM 6510.01B) for detecting, analyzing, and responding to information or events or cyber incidents, refer to U.S. Department of Defense [8].

Figure 5 represents the life cycle of cyber incident handling (CIHLC), which is been published previously by US' DoD [8]. Overall, there are three main points which required for the security operators or cyber space users to review alert of cyber events, they are record, identification, and report [8]. The incoming information should be detected then recorded for being analyzed and identified. Analysis and identification steps should be performed, in order to find out the reason behind the event or information. During this step, the operators or cyber space users has to review the events and information by literature study and/or direct observation on the field. After this, they can provide response and action by considering the obtained analysis and identification results. This step requires well technical and organisational coordination among its stakeholders for the response and action being well accepted [9]. In addition, preliminary analysis and identification, and response and action steps are need to be performed so that event or information cannot be widespread immediately. Depth analysis and further response towards the event and information are still required for assigning a comprehensive clarification formally. Also, it is important to provide recovery of unstable situation which caused by the event and information. However, post incident analysis step is still needed to observe how stable the situation after the comprehensive clarification had been published. If the condition is still unstable, the CIHLC should be performed again with more and depth evaluation.

Conclusions

One of the advantages of this approach is presence of stability in representation across a wider system. Therefore, people could compare and distinguish cyber warfare with other forms of warfare using the same language. Moreover, people may begin to develop models that can be identified from the characteristics of cyber attack patterns. At least, cyber space users can take preventive actions in filtering information/sources that come.

Individually, if the information user has a concrete understanding, it will provide experience of all kinds of attacks that come and clarify the obtained information. Finally, each cyber space users will have fundamental knowledge which potentially useful to use the information before being disseminated to the public with a wider scope.

Acknowledgements

Authors would like to thank Islamic University of Kadiri and Moslem Scholar of Pancasila Foundation (Yayasan Bina Cendekia Muslim Pancasila) for the great moral and financial support to undergo proposed cyber security defence system in order to protect our national state sovereignty. No Authors in conflict.

References

[1]. Perwita, Banyu A A, Yani and Yanyan A 2005 Pengantar Ilmu Hubungan Internasional (Bandung: Rosdakarya)

[2]. Winarno B 2014 Dinamika Isu-isu Global Kontemporer (Yogyakarta: CAPS (Center of Academic Publishing Service))

[3]. Mas'oed M 1989 Studi Hubungan- Internasional, Tingkat Analisis dan Teorisasi (Yogyakarta: Pusat antar Universitas-studi Sosial UGM)

[4]. Ween A, Dortmans P, Thakur N, and Rowe C 2017 Framing Cyber Warfare: an Analyst's Perspective Journal of Defense Modeling and Simulation: Applications, Methodology, Technology 16(3) pp.1–11

[5]. Gisladottir V, Ganin A A, Keisler J M, Kepner J, and Linkov I 2017 Resilience of Cyber Systems with

Over- and Underregulation Risk Analysis 37(9) pp.1644–1651.

[6]. Ganin A A, Quach P, Panwar M, Collier Z A, Keisler J M, Marchese D, and Linkov I 2017 Multicriteria Decision Framework for Cyber Security Risk Assessment and Management Risk Analysis DOI: 10.1111/risa.12891

[7]. Garvey P R 2008 Analytical Methods for Risk Management: a Systems Engineering Perspective (Boca Raton: Chapman and Hall/CRC)

[8]. U.S. Department of Defense (US's DoD) 2012 Chairman of the Joint Chiefs of Staff Manual, Cyber Incident Handling Program CJCSM 6510.01B

[9]. Frederiks E R, Stenner K, and Hobman E V 2015 Household Energy Use: Applying Behavioural Economics to Understand Consumer Decision-making and Behaviour Renewable and Sustainable Energy Reviews 41 pp.1385–1394

Establishing Regional Security Regime through ASEAN Cooperation in Cybercrime Issue – IIDSS2019

Sereffina Yohanna Elisabeth Siahaan1

1 Master Student of Indonesia Defense University, Sentul, Bogor 16810, Indonesia

E-mail: sereffina.yohanna@gmail.com

Abstract. Cybercrime is non-traditional security issues whose effects to damage all activities by using a computer system. Globally, internet users in ASEAN are the largest with 350 million users in 2018. Losses caused by cybercrime in ASEAN also increase every year. Facing this condition, ASEAN needs to comprehend cyber security and to enhance cooperation thus ASEAN could be able to address common threats. ASEAN has become an institution for all member states to achieve national interests in order to support national security in the cyber field. ASEAN has currently formulated various documents regarding handling cybercrime, but ASEAN has not yet sought concrete agreements that can counter this threat. This paper uses a qualitative method with a descriptive analysis approach. This paper is analyzed by regional security regime theory by approaching on forums and dialogs within ASEAN. This paper aims to provide advice to establish regional security regime through ASEAN in developing cyber cooperation as a new concept of regional collaboration. ASEAN is expected to benefit from maintaining cyber security stability in the region.

1. Introduction

At present the issue of non-traditional security is an important issue because the impact it poses is no less than a threat to traditional security issues. One issue in non-traditional security is cyber threats that are closely related to computer and internet technology. The rapid development of computer and internet technology has created enormous dependence on society. Every activity that is usually supervised by relying on human power is slowly transferred to the computer. Not only that, the internet has simplified human life because all information can be accessed easily only from behind the desk. Dependence on computers and the internet is then disrupted by cyber attacks.

There are 350 million internet users in the Southeast Asia in 2018 and of that number, 150 million of them are from Indonesia, which is referred to as the country with the most number of cyber users in Southeast Asia. Google and Temasek research also found that the use of the Internet through smartphone devices was very large, reaching 90 percent in Southeast Asia. [1] The Hootsuite study found mobile internet users in countries like Indonesia, the Philippines and Malaysia spent 4 hours accessing the internet on mobile devices per day. While mobile internet users in Thailand spend the longest time in Southeast Asia, which is 4 hours 56 minutes per day. [2]

These threats can come from governments, organizations, individuals, or entrepreneurs, whether intentionally or not in order to gain financial, military, political and other purposes. Cyber can be a threat to a country because of its scope that can be used to steal information, disseminate destructive ideas, and attack information systems in various fields in military networks and civil networks such as data theft of companies and agencies. Given the losses that can be caused by cyber attacks, the report of Ponemon Institute in 2018 stated that the average loss due to global data violations this year reached 3.86 million US dollars, an increase of 6.4 percent from 2017. [3]

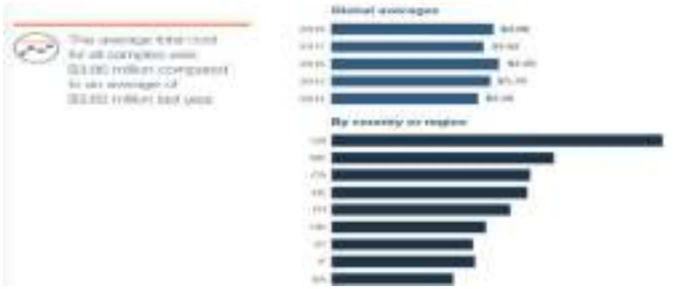


Figure 1. Data Breach Cost (Phenomenon Institute)

The world conditions faced by fourth and fifth generation wars also require different deterrence strategies. If, the concept of the previous generation of war is conventional and involves more physical contact, then the concept of fourth generation war is in communities that are interconnected (networked), cross-country, and information-based. [4] The attacks used vary, both in the form of information interventions through the media and the use of computer viruses that can cause damage to the country's critical infrastructure. In addition, the war of ideas / ideas, the development of opinion through social media can ultimately influence the political, social and cultural conditions of a country as a manifestation of the threat of the fourth generation of war. Without the mastery of cyber space, it is very possible that a country's security and political stability can be disrupted. Therefore, a leader in this generation is demanded not only to master the art of war (traditional) but also technology. [5] Fourth generation war is a new concept that rests on networked, transnational and information based. Tactically, the fourth war involves a combination of international, transnational, national and subnational actors. In contrast to the previous generation of warfare, in this generation of war the state's control of war diminished as it involved non-state actors, so there was no longer a difference between civil and military forces.

Therefore, this paper aims to provide advice for ASEAN to strengthen cooperation in anticipation of this cyberattack. To achieve the above objectives, this paper will explain the complexity of cyber threats in Southeast Asia, analysis of ASEAN cyber cooperation and recommendations and recommendations as conclusions.

2. Cybercrime in Southeast Asia

2.1. Complexity of Cyber Threats in Southeast Asia

In two UN Congress documents cited by Barda Nawawi Arief regarding The Prevention of Crime and Treatment of Offenders in Havana Cuba in 1990 and in Vienna Austria in 2000, two terms related to definition of cybercrime, namely cybercrime and computer related, were explained crime. [6] The cybercrime is divided into two categories, first, cybercrime in a narrow sense is called computer crime, as well as cybercrime in the broad sense which is called computer related breach.

The cybercrime is a type of crime related to the use of an infinite information technology and has strong characteristics with an engineering technology that relies on a high level of security and credibility of information that is delivered and accessed by internet customers. Cybercrime can include things like computer intrusion (hacking) in order to attack property, economic espionage (data theft or confidential transactions, internet extortion, money laundering, identity stealing, and a number of attacks facilitated through the internet) in fact the type continues to grow every day. [7]

Further, cybercrime as mentioned above is not easy to identify, specifically related to the method used, location until the time of occurrence of cybercrime. Internet anonymity, makes cybercrime increasingly rampant with various instruments and forms of crime. In some large cases, cyberattacks that occur not only come from one country or one source. Even cyber attacks, are more often carried out by non-state actors with diverse targets. Unlimited and lawless cyberspace or cyberspace provides various possibilities for how and where attacks originate, so cybercrime is often not handled in an easy and concise way, or only relies on the performance of one actor.

According to the World Threat Assessment 2013 report in the European Commission's proposal of 2.1 billion internet users worldwide, the majority of users are in Asia (922,200,000). Meanwhile, the next most significant area in terms of the number of internet users is Europe with

476,200,000 users. China alone has 485 million internet users - more than other countries or regions (including Europe and the rest from Asia) - and has an internet attack of only 36.3 percent. The growth of ICT in Southeast Asia is actually not too far behind the US, Europe and countries in Northeast Asia such as Japan and the Republic of Korea. [8] According to the ASEAN E Commerce Database Project released in 2010, ASEAN represented 6 percent of Internet users and ASEAN member countries' 20 percent global penetration rate, with Brunei Darussalam, Singapore and Malaysia having the largest share of internet penetration, and Indonesia, the Philippines, and Vietnam has the largest internet user. [9] The Indonesian government even expects companies in ASEAN to potentially risk a loss of US $ 750 billion or Rp.10,000 trillion due to the impact of cyber attacks. [10]

Based on the report of the global consulting company, AT Kearney, ASEAN countries are being used as launchpads in dealing with cyber attacks- either as target for the release of malware attacks. [11] In a cyber-crime operation held by Interpol and investigators from seven countries in Southeast Asia in 2017, it was revealed that nearly 9,000 servers were infected with malware and hundreds of other websites were targeted for attacks in the region. Various types of malware, such as those targeting financial institutions, spreading ransomware, conducting Distributed Denial of Service (DDoS) attacks, and spreading spam, are some of the threats posed by these infected servers. [12] According to a Symantec report entitled Internet Security Threat Report Volume 24 which was released in February 2019, there are 4 ASEAN countries from 10 countries in the world that have presentations on cyber attacks, namely Vietnam, Indonesia, Thailand and Singapore. Vietnam is in the third largest country position after China and India with a 3.54% cyberattack percentage. Cybercrime in the country have increased where in 2017 the number of cyber threats in Vietnam was 2.07%. Indonesia follows next with a percentage of 2.23% cyber attacks in 2018, up from 1.67% a year earlier. Thailand and Singapore sequentially received cyberattack percentages of 1.54% and 0.75%. [13]

2.2 Cyber Security Regimes in ASEAN

According to Krasner, an international regime is an order that contains a collection of principles, norms, rules, decision-making processes, both explicit and implicit, which are related to expectations or expectations of actors, and contain the interests of these actors in International Relations. [14] This study fulfills the need for conceptualization of forces that can enable it to focus on the control of events that are concerned with the problems being faced by international actors. [15] The principle of the international regime is related to the belief in facts, causation, and honesty; norms are standards of behavior that are manifested as rights and obligations; regulation is a clear and specific prohibition on actions taken; while the decision making procedure is a procedure that must be taken in implementing joint choices. Rules, procedures and norms that exist within the regime regulate and become behavioral controls of members of the regime. [16]

Regime is the result of cooperative behavior as an effort to facilitate cooperation. This statement is focusing on the control of events that are concerned with the problems being faced by international actors. The regime can be said is a continuation of the form of cooperation, and encourage better cooperation. The fundamental difference between the regime and the institution is how to view actors in international relations. The regime refers to the influence of behavior generated by international organizations on other actors, especially state actors by focusing on actor expectations. It is different from institutions that look more at what is happening in the organization than to see the influence that international organizations have on other actors. [17] This is especially significant for the Southeast Asia region where ASEAN's centrality in regional architecture has a potential role as a significant "neutral area" in terms of international cyber security cooperation. The ASEAN cyber security regime is a "common" condition formed in Southeast Asia in the face of non-traditional forms of threats that arise in "uncertain" conditions. Regime calculates the results that an actor or State can get in a condition of uncertainty or when there is no specific calculation.

In establishing a security regime in the region, ASEAN needs to make rules, procedures and norms that exist within the regime to regulate and be a behavioral control of members of the regime by strengthening forums and dialogs. ASEAN already forum by ARF (ASEAN Regional Forum) concept to organize interactions among ASEAN member countries in order to combat cybercrime. ARF is different from the concept security cooperation by the North Atlantic Treaty Organizations (NATO) which was formed based on treaty or post-war defense alliance World II. ARF is intended to build taste mutual trust that adopts an approach multilateral to prevent conflicts in the region. ARF is not as identical as NATO with the use of military power, but rather more to dialogue and engagement as a means of preventing conflict. Thus, the concept ARF can be used for major capital in the formation of regional regimes.

In responding to these challenges, since 2001 the issue of cyber security has become one of the agenda of the meeting which resulted in the agreement of AMMTC (ASEAN Ministerial Meeting on Transnational Crime). Member countries in ASEAN agreed to include cybercrime in the working program to be implemented on the ASEAN Plan of Action in order to combat transnational crime.[18] In 2003 at the 9th AMMTC meeting held in Vientiane, Lao PDR, ASEAN Ministers welcomed the new framework of SOMTC Working Group on Cyber Crime which is part of transnational crime (ASEAN Senior Officials Meeting on Transnational Crime). The response from ASEAN is increasingly refined with the ARF Statement on Cooperation in Fighting Cyber Attack and Terrorist Misuse of Cyber Space, in Kuala Lumpur on July 28, 2006, which generally emphasizes the creation of a legal framework (regulation) against cybercrime, encouraging collaboration and collaboration in handling crimes, including cyber terrorism (cyber terrorism), and strengthening increased public awareness in using cyber.

ARF on cybersecurity initiatives was initiated in 2006 through a joint statement at a meeting in Malaysia and reaffirmed at ARF Statement Cooperation in Ensuring Cyber Security, in Phnom Penh, 12th July 2012, as follows: [19]

1. Promoting further consideration of vision and strategies to discuss threats emerging in this field consistent with international law and its basic norms and principles;

2. Promoting forum on confidence building measures (CBM), risk reduction measures and stability to address the implications of ARF external participants' use of ICTs, including exchange of views on the potential use of ICTs in conflict;

3. Encouraging and enhancing partnership in bringing about culture of cyber security in the region;

4. Developing the ARF work plan on security in the use of ICTs, focused on practical collaboration on CBM, which could set out corresponding targets and a timeframe for their implementation;

5. Reviewing a possibility to explain common terms and definitions relevant to the sphere in using ICTs.

The results of the statement was implemented in the form of workshops, seminars, and various training at the level regional. One focus of the workshop that is how a country is inside respond and coordinate when there is something cyber incidents. The discussion includes coordination of national responses, methods of mitigation, how to prosecute perpetrators of crimes between countries, and the perspective on an incident involving actors from other countries and as far as how other countries respond to an incident that emerged from their country.[20]

Since 2003, the Singapore ASEAN Telecommunications and IT Ministers Meeting (TELMIN), and the Telecommunications Senior Officials Meeting (TELSOM) emphasized the efforts to establish an ASEAN Information Infrastructure in order to promote interoperability, inter-connectivity and security integrity. All Ministers of Telecommunications and IT in ASEAN decided that all ASEAN member states need to develop and operationalize the National Computer Emergency Response Team (CERT) in 2005 in accordance with the agreed minimum performance criteria. As the agreement was formed, a virtual forum for ASEAN cyber security is being formed to develop a general framework for coordinating information exchange, establishing standards and collaborating among law enforcement agencies. This effort was enhanced by the establishment of the 2015 ASEAN ICT Masterplan (AIM 2015) which was approved at the 10th TELMIN meeting on 13-14 January 2011 in Kuala Lumpur, Malaysia. AIM 2015 emphasized the development of trust related to cyber security through empowerment and community engagement and infrastructure development efforts with initiatives to promote information security, network integrity, data protection and CERT collaboration.

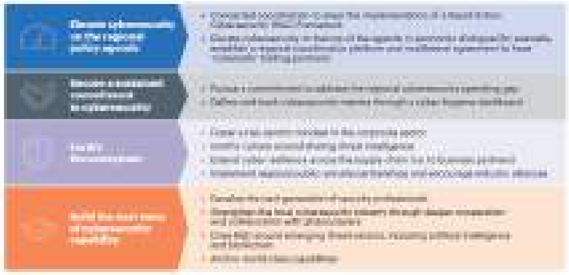
In building a regional security regime, ASEAN must also improve its cyber proactive strategy built on the awareness that cyberspace is a tool that creates economic progress and increases living standards. For example, AMCC in October 2016 has built a discussion platform on cyber issues at the ministerial level to discuss cyber security using a harmonization perspective among stakeholders. The 3rd ASEAN Ministerial Conference on Cybersecurity (AMCC) was convened in 2018, specifically to increase coordination on cybersecurity efforts among various platforms of the three pillars of ASEAN. The AMCC agreed that there is a need for a formal ASEAN cybersecurity mechanism to consider and to decide on inter-related cyber diplomacy, policy and operational issues. It was recommended that the proposed mechanism should be flexible and also take into account multiple dimensions, including economic considerations. [21] ASEAN should strengthen cooperation by enhancing capacity building efforts, thus ASEAN's efforts will be focus, effective, and coordinated holistically on cybercrime issues.

ASEAN should make cybersecurity programs by working together to defend and to take benefit of the region's collective resources. The trust and resilience are the main points for policy makers and non-state actors that should be improved by working together in appearing awareness on cybersecurity and adopting a stance of active defense within ARF and AMCC. Following this is an ASEAN's cybersecurity playbook as a new concept that could be implemented on the upcoming forums:

- Steering the implementation of a Rapid Action Cybersecurity Framework

- Improving cybersecurity issues to the top of the agenda in regional forum within ASEAN framework

Table 1. Regional Cybersecurity Defense Playbook (AT Kearney)



Elevate cybersecurity on the regional policy agenda	• Concerted coordination to steer the implementation of a Rapid Action Cybersecurity Framework • Elevate cybersecurity to the top of the agenda in economic dialogues [illegible]
Secure a sustained commitment to cybersecurity	• Pursue a commitment to address the regional cybersecurity spending gap • Define and track cybersecurity metrics through a cyber hygiene dashboard
[illegible]	• [illegible] • Instill a culture around sharing threat intelligence • Extend cyber defence across the supply chain [illegible] • [illegible]
Build the next wave of cybersecurity capability	• Develop the next generation of security professionals • Strengthen the local cybersecurity industry through deeper cooperation and collaboration with global players • Stay ahead of emerging threat vectors, including artificial intelligence and blockchain • Build world-class capabilities

3. Conclusion

The condition of cyber in ASEAN is faced with a dangerous situation. The use of cyberspace has touched various aspects of the nation's life which include social, cultural, economic, politics and security. Internet network penetration in ASEAN continues to expand, even social networking and internet users are one of the largest regions in the world. On the other hand, the trend of cyber threats that increasingly leads to the national interest of a nation is a challenge for each country at the strategic and operational level that has not been fully able to establish a comprehensive cybersecurity system. This unpreparedness of the government in the national scope needs to be addressed by implementing regional collaborative efforts to eliminate or minimize the potential threats. ASEAN needs to use increasing cooperation to become a regional security regime to protect its national security by reducing potential threats and establishing regional stability.

The issue that should be addressed among ASEAN countries is collaboration and information sharing is indeed a vital aspect of cyber security. Without collaboration, cyber security ecosystems are easily compromised. ASEAN must also try to increase capacity through norms, knowledge and information in the field of cybersecurity within ARF, AMCC or other forums. The ASEAN's response to the cybersecurity challenges need to forward-looking, comprehensive, engaging an array of all stakeholders to deal with the cyber threats and support ASEAN's leap into effective platform. ASEAN should use all forums and dialogs such as ARF and AMCC in order to push every stakeholder taking role to play in cybercrime. ASEAN should create security regional regime by building the practices, procedures and processes and establishing military-civil collaboration to address cybercrime issues.

References

[1] Ananda, Rajan. Etc 2018 E-Conomy SEA 2018: Southeast Asia's Internet Economy Hits An Inflection Point. Think with Google. (online), (https://www.thinkwithgoogle.com/intl/en-apac/tools-resources/research-studies/e-conomy-sea-2018-southeast-asias-internet-economy-hits-inflection-point/)

[2] Digital Report. 2018. Global Digital Report 2018 World's Internet Users Pass The 4 Billion Mark. (online), (https://digitalreport.wearesocial.com/)

[3] Ponemon Istitute 2018 Ponemon Institute 2018 Cybersecurity Report. (online), (https://www.gosolis.com/blog/ponemon-institute-2018-cybersecurity-report-information/)

[4] Ali, Alman Helvas 2015 Angkatan Laut dan Peperangan Generasi Keempat. Forum Kajian Pertahanan dan Maritim. (online), (http://www.fkpmaritim.org/angkatan-laut-dan-peperangan generasi-keempat/)

[5] William S. Lind, et all 1989 The Changing Face of War: Into The Fourth Generation. Marine Corps Gazette pp 22

[6] Nawawi Arief, B 2006 Kebijakan Penanggulangan Cyber Crime Dan Cyber Sex. Law Reform, (online), Volume 1(1), pp 24

[7] Govil, Jevish 2007 Ramifications Of Cyber Crime And Suggestive Preventive Measures. (online), (https://www.researchgate.net/publication/4287237_Ramifications_of_cyber_crime_and_suggestive_preventive_measures)

[8] Clapper, JR 2013 Worldwide Threat Assessment. Director of National Intelligence of US Government. (online), (https://www.dni.gov/files/documents/Intelligence%20Reports/UNCLASS_2013%20ATA%20SFR%20FINAL%20for%20SASC%2018%20Apr%202013.pdf)

[9] ASEAN 2015 ASEAN e-Commerce Database Project. (online), (https://id.scribd.com/document/111765095/ASEAN-e-Commerce-Database-Project#)

[10] Ariyanti, Fiki 2018 Serangan Siber Potensi Bikin Rugi Perusahaan ASEAN Capai Rp 10 Ribu T. Liputan 6, (online), (https://www.liputan6.com/bisnis/read/3337398/serangan-siber-potensi-bikin-rugi-perusahaan-asean-capai-rp-10-ribu-t)

[11] AT. Kearney Report 2018 Cybersecurity in ASEAN: An Urgent Call to Action

[12] Sarkar, Himani and Clarence Fernandez. 2017. Interpol-Led Operation Finds Nearly 9,000 Infected Servers In Southeast Asia. Reuters. (online), (https://www.reuters.com/article/us-singapore-interpol-cyber-idUSKBN17Q1BT)

[13] Symantec 2019 Internet Security Threat Report Volume 24. (online), (https://www.symantec.com/content/dam/symantec/docs/reports/istr-24-2019-en.pdf)

[14] Krasner, Stephan D 1982 Structural Causes and Regime Consequences: Regimes as Intervening Variables. Within: Krasner, Stephan D. [eds.]. International Organization, Vol. 36/2. (New York: Cornell University Press)

[15] Haggard, Stephan and Simmons, Beth A 1987 Theories of International Regimes. Within: International Organization, Vol. 41 (Cambridge: MIT Press)

[16] Keohane, Robert O and Joseph. S Nye 1987 Power and Interdependence. Within: International Organization, Vol. 41 (Cambridge: MIT Press)

[17] Barkin, J.S 2006 International Organization: Theories and Institutions (New York: Palgrave Macmillan)

[18] ASEAN Secretariat 2011 ASEAN ICT Masterplan 2015 (AIM)

[19] ASEAN Regional Forum. 2015. ASEAN Regional Forum on Security of and in The Use of Information and Communications Technologies (ICT's) Cooperation in Ensuring Cyber Security (Phnom Penh: ARF Library) pp 1

[20] Setyawan, David Putra and Sumari, Arwin Datumaya Wahyudi Sumari 2016 Diplomasi Pertahanan Indonesia Dalam Pencapaian Cybersecurity Melalui Asean Regional Forum On Cybersecurity Initiatives (Bogor: Jurnal Penelitian Politik)

[21] Timur, F. G. Cempaka 2017 The Rise of Cyber Diplomacy — ASEAN's Perspective in Cyber Security, KnE Social Sciences. ICoSaPS Conference Proceedings The 3rd International Conference on Social and Political Science The Impact of Information Technology on Social and Political Dynamics, 2016

The Effect of Temperature Differences on Synthesis of Silicon Carbide 6H-SiC Politypes With X-Ray Diffraction Analysis Using Match 3

Selly Pratiwi1, Sovian Aritonang2, I Nengah Putra3, Musfirah Cahya4

1,2,3Power Motion Technology Study Program

Faculty of Defense Technology, Indonesia Defense University, Kawasan IPSC, Sentul, Bogor, Indonesia

3Physics Program, National Institute of Science and Technology, Jakarta, Indonesia

Komplek Indonesia Peace and Security Center (IPSC) Sentul, Bogor - Jawa Barat

Email: selly.pratiwi@tp.idu.ac.id ; sovian.aritonang@idu.ac.id ; nengah.putra@idu.ac.id; musfirah@istn.ac.id

Abstract: Indonesia is one of the developing countries in the World, with a growing population. This increase caused various impacts on aspects of human life. One aspect that is quite affected by the increase in population is the use of energy to support living needs. The increasing demand for fuel oil as the most widely used energy causes the scarcity of oil. This condition will continue to be a threat to the State both from within the country and from abroad. One alternative to prevent the occurrence of petroleum scarcity is to change lifestyles to use gas fuel. Pore carbon which is characterized by specific surface area very high(SSA) can store large amounts of liquid or gas, making carbon as one of the materials intensively studied as a gas fuel storage material. Experimentally, very high pores carbon can be produced through selective thermo chemical etching from silicon derived from silicon carbide. The purpose of this study was to analyze the effect of temperature changes on temperature variations of 900oC, 1000oC and 1200oC on the pores of carbon formed from the synthesis of Silicon Carbide 6H-SiC Politics using HCl and 10-hour ultrasonic on the parameters of structural formation Crystals which include the Crystal system, Grid Parameters, Space Groups and Crystal Fields formed using software Match.3. The method used is to analyze the results of X-Ray Diffraction characterization of silicon carbide synthesis materials using ultrasonic 10 hours with temperature variations using Match 3 software. The results obtained that the optimum temperature is 900oC, 1000oC and 1200oC. The analysis results obtained that carbon formed at a temperature of 1000oC as much as 56.3% where carbon formed mineral Diamond with C m m a space group with crystal system orthorhombic, and has cell parameters a = 4.9640 Å, b = 5.1630 Å, c = 4.3870 Å.

Introduction

Indonesia is one of the developing countries in the World, where the population continues to increase. This increase caused various impacts on aspects of human life. One aspect that is quite affected by the increase in population is the use of energy for menus which are necessities of life which include the sectors of industry, transportation, households and so forth. This resulted in the emergence of various issues regarding energy in the form of renewable energy sources, alternative energy resources to the development of energy storage systems.

Fuels that are still superior and are in great demand by the world community are fuels made from petroleum, the abundance of petroleum is mostly used to produce gasoline and other types of fuel. The high community demand for petroleum fuels has resulted in higher oil exploration and does not rule out the possibility that oil reserves will be depleted and reach the limit phase. The depletion of the availability of petroleum reserves will certainly affect the availability of fuel oil marketed. One of the impacts of this situation was the increase in domestic fuel prices that occurred in almost every Indonesian government. The limitation of world petroleum reserves has resulted in the high price of World crude oil and is a strong reason to raise fuel prices in the country to save the country's financial condition. This will certainly be a serious threat to Indonesia. This is because the high oil prices not only lead to public unrest accompanied by protests in Indonesia, but also developed countries such as Britain, Germany, the Netherlands, France and various other parts of the world. The impact of rising oil, especially in developed countries, has caused energy transfer, namely by utilizing food ingredients such as corn, palm oil and soybeans for fuel. As a result, developing countries including Indonesia experience inevitable food difficulties. The surge in prices of food and other agricultural commodities, especially in Indonesia, has resulted in increased cases of malnutrition, deaths of children under five and mothers of childbirth. Utilization of agricultural commodities to fulfill fuel is considered to result in disruption of food supplies to the world.

Today, the development of energy is highlighted to produce a concept of energy that is cheap, easily obtainable, environmentally friendly and (renewable energy), now, technology leads to the engineering of solid materials that can be used as easily produced gas storage materials. The challenge is how to design materials that have sufficient absorption capacity, control the distribution of their flow and life span. One of the materials currently being investigated intensively for the purpose of storing gas fuels is nano pore carbon. Nano pore carbon, which is characterized by specific surface areas very high(SSAs) can store large amounts of liquid or gas.

Nano pore carbon consists of solid material containing carbon with an empty cavity (pore) with a pore size of less than 100 nm1. Nano pore carbon has become one of materials that is being investigated intensively for gas fuel storage purposes. in addition to its use as a gas storage material, nanopore carbon is also used as a storage of hydrogen gas, an energy storage electrode and can absorb uranium metal ions. In utilizing Nano pore carbon as energy storage or as a capacitor electrode material, it takes high porosity carbon and has a total pore volume above 90%.

Much effort has been made to obtain material as a gas storage material because the next development in industrial technology intended for gas fuel storage requires materials that have a high surface area with controlled pore size distribution. Experimentally several studies have been conducted to obtain carbon with a controlled pore distribution. In these studies there are several main ingredients used to obtain carbon Nano pore including Arthur (2007) research conducted a study on pure carbon with a hexagonal structure with the method used was graphite intercalation using potassium (KC24). Meanwhile Ramadhani I, et al (2018) who used coconut shell as Nano pore carbon-producing material with experimental methods in the form of preparation, carbonation and activation and the characterization used using Nitrogen Isotherm Physisorbtion.

Very high pore carbon synthesis data is produced from various carbides such as Al4C3, TiC, MO2C, Fe3C4, TaC and Ti3SiC4. Musfirah CF (2010) conducted a synthesis of porous carbon from SiC material, the method used was a wet method (leaching) using HCl solution and combined with Ultrasonic at a temperature of 900oC, 1000oC and 1200oC. Ultrasonic lowered the temperature used in making Nano pore carbon. Ultrasonic waves produce and distribute implants cavitation in fluid media. Ultrasonic is an efficient way for wet grinding and micro grinding of particles.

Based on this research, in this study we will discuss the effect of temperature differences on the synthesis of the silicon carbide crystals using a 10-hour Ultrasonic with HCl at a temperature of 900oC, 1000oC and 1200oC using the Match.3 application to determine the optimum temperature needed in the formation of Nano pore carbon which has a controlled pore distribution.

Method of Research

Match 3is a program that functions to analyze the results of bacterial characterization with X-Ray Diffraction (XRD). Match application! 3 which is used in this study is the latest version, version 3.6.0, which was released on November 17, 2017. This application will provide information in the form of Crystal structures from X-Ray Diffraction characterization, information obtained includes Crystal systems, lattice parameters, groups space and fields of diffraction formed. The steps for using Match 3 software are as follows.

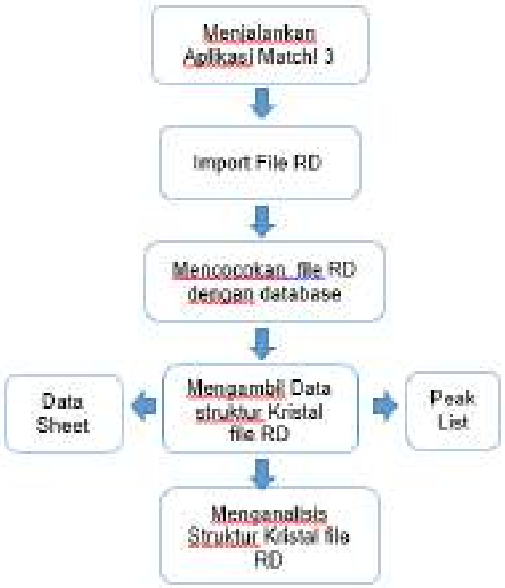

Menjalankan Aplikasi Match! 3
Import File RD
Mencocokan file RD dengan database
Mengambil Data struktur Kristal file RD
Data Sheet
Peak List
Menganalisis Struktur Kristal file RD

Figure 1 Flowchart of Program Use Match 3

Results and Discussion of Results

From the results of Material characterization using XRD crystallographic data were obtained which included space groups , crystal systems and cell parameters (cell parameters).

From the results of data acquisition using the Match 3 program, it is also obtained data that describes the crystal fields formed (peak list) which includes the Bragg diffraction angle (Θ), Intensity (Peak Height) and the value of the maximum half-peak width (FWHM) that will be a comparison in each treatment. In this study the author uses 3 highest peak data from diffraction patterns, the following data obtained from XRD characterization using Match 3.

SiC Crystal Structure 6H-SiC Politype Before Synthesis.

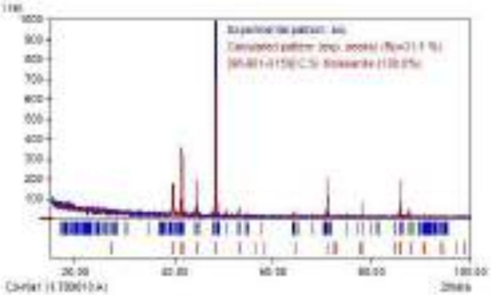


Figure 2 Diffraction Pattern of Silicon Carbide Before Synthesis

Figure 2 Is a pattern of diffraction results from the Match.3 program that has been matched with the database in the Match.3 program. With crystallographic data and peak data of the Crystal fields as follows.

Table 1 Crystallographic Data of Silicon Carbide Before Synthesis

Name	Silicon Carbide
Mineral name	Moissanite
Formula	Si C
Quality	C (calculated)
Space group	P 63 mc

Crystal system	Hexagonal
Cell parameters	α = 3.0810 A c = 15.1245 A

Table 2 Data 3 Peak Highest SiC Diffraction Pattern

Before Synthesis

From table 1, it is known that this SiC material has a space group P 63 mc and has a hexagonal Crystal system. While from table 2 it is known that the highest peak is at bragg angle 48.47o with 1000 intensities and with the number of FWHM is 0.0800o.

SiC Crystal Structure Politics 6H-SiC 10 hours Ultrasonic Synthesis Results without Heating

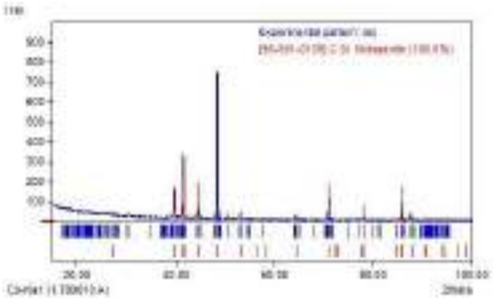


Figure 3 SiC Diffraction Pattern Ultrasonic Results 10 Hours with HCl without Heating

Figure 3 is a diffraction pattern of 10 hours ultrasonic SiC with HCl without heating, data obtained from the characterization of the diffraction pattern crystallography is the same as SiC crystallographic data before experiencing heating which can be seen in table 1. While, the 3 highest peak data from the results of the diffraction pattern characterization can be seen in table 3 as follows.

Table 3 Data 3 Highest Peak SiC Diffraction Pattern Ultrasonic Synthesis 10 Hours With HCl Without Crystallization

Crystal Field	2 θ	Peak Height	FWHM
1	41.57	338.9	0.0800
2	48.47	1000.0	0.0800
3	70.95	188.7	0.0800

Field	2 θ	Peak Height	FWHM
1	41.57	338.9	0.0800
2	48.47	751.8	0.0800
3	70.95	188.7	0.0800

From table 3 it is known that in the process SiC synthesis without heating does not change the crystallographic data which means that the 10-hour ultrasonic process with HCl does not change the Crystal system on the SiC. While from table 4 it is known that there is a decrease in intensity in one of the Crystal fields, namely at bragg angle 48.47o The intensity becomes 751.8.

SiC Crystal Structure Politics of 6H-SiC Synthesis Ultrasonic Synthesis of 10 Hours at C

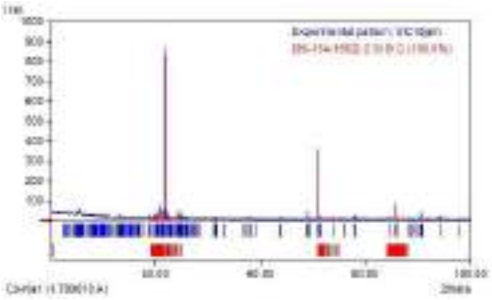


Figure 4 SiC Diffraction Pattern Ultrasonic Result 10 Hours with HCl at 900oC

Figure 4 is a diffraction pattern of SiC ultrasonic results of 10 hours with HCl at From the characterization of the diffraction pattern obtained crystallographic data which is still the same as crystallographic data on SiC before synthesis and after experiencing a 10-hour Ultrasonic with HCl without heating which can be

seen in table 1. Meanwhile, from the diffraction pattern changes in data from peak fields were obtained diffraction, here are 3 highest peak data from the SiC diffraction pattern 10 hours Ultrasonic results with HCl at .

Name	Carbon
Mineral name	Diamond
Formula	C
Quality	C (calculated)
Space group	C m m a
Crystal system	Orthorhombic
Cell parameters	a = 4.9640 Å, b = 5.1630 Å, c = 4.3870 Å

Table 4 Data The Top 3 SiC diffraction pattern results for Ultrasonic Synthesis In 10 Hours With HCl Temperature

Bidang Kristal	2 Θ	Peak Height	FWHM
1	40.84	78.0	0.1200
2	41.72	865.0	0.1200
3	41.93	56,0	0.1200

From the table it is known that at a temperature of ,peak data diffraction field has decreased intensity. In addition, at , the value of the maximum half-peak width or Full Width Half Maximum (FWHM) is widening to and causes a shift in bragg angle to the highest peak data.

SiC Crystal Structure 6H-SiC Political Result of 10 Hour Ultrasonic Synthesis at Temperature C

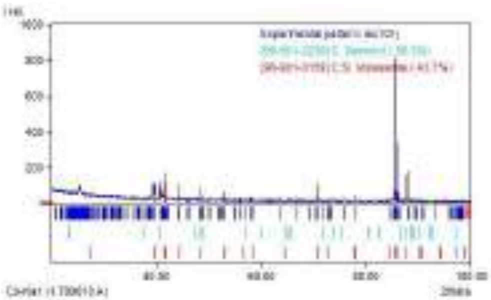


Figure 5 SiC Diffraction Pattern Ultrasonic Result 10 Hours with HCl at 1000oC

In Figure 5 It can be seen that the characterization results show that Carbon C has volume 56, 3% who have crystallographic data as follows.

Table 5 Data Crystallography of Carbon Results of Ultrasonic synthesis 10 Clock with HCl at 1000oC

The peak data from the SiC diffraction pattern of 10 hours ultrasonic results with HCl at a temperature of C can be seen in table 6 below.

Table 6 Data 3 Highest Peak SiC Diffraction Pattern Ultrasonic Synthesis 10 Hours With HCl AtTemperature

Crystal Field	2 tetha	Peak height	FWHM
1	85.68	805	0.1200
2	85.82	328	0.1200
3	87.92	180	0, 1200

Table 6 shows that there is a shift in the diffraction plane angles for the highest peak data, while the FWHM value obtained is still constant at .

SiC Crystal Structure Politics of 6H-SiC Synthesis of 10-Hour Ultrasonic Synthesis at C

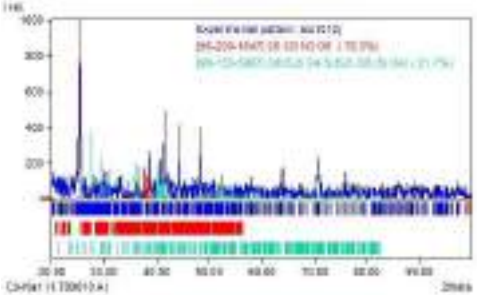


Figure 6 SiC Diffraction Pattern of 10-Hour Ultrasonic Result with HCl at 1200oC

Figure 4.5 shows the results of SiC diffraction analysis of 10-hour ultrasonic results with HCl at 1200oC. the results of the characterization of the match3 program show that the material formed is C6Cl3N3O6 as much as 78.3% and the impurity of SiO4 is 21.7%. Crystallographic data formed can be seen in table 7 below.

Table 7 Crystallographic Data of Ultrasonic Synthesis 10 Hours with HCl at 1200oC

Name	C6Cl3N3O6
Mineralname	
Formula	C6Cl3N3O6
Quality	C (calculated)
Spacegroup	
Crystalsystem	Triklinik(anorthic)

Cell parameters a = 12,1370 Å
b = 12,1810 Å
c = 11,6940 Å.

In addition, the diffracted pattern experienced a bragg angle phase change at the highest peaks and also increased the value of the FWHM to 0.1600o. The following data 3 highest peak SiC diffraction results of 10 hours ultrasonic with HCl at a temperature of 1200oC.

Table 6 Data 3 Highest Peak SiC Diffraction Pattern Ultrasonic Synthesis 10 Hours with HCl at

Crystal field	2 tetha	Peak height	FWHM
1	25,43	1000,0	0,1600
2	41,49	491,5	0,1600
3	44,49	412,6	0,1600

Discussion

characterization results indicate that SiC material in this group (space group) P 63 m c , so it can be proved that the sample used is silicon carbide with 6H or 6H-SiC polyps. On the results of SiC synthesis using 10 hours of ultrasonic without heating causes a decrease in the intensity value at the peaks of the diffraction pattern. This proves that there has been a cavitation and implosion process when the material is subjected to ultrasonic treatment. In areas that experience cavitation and implosion, bubbles will break and cause shock to nearby walls. The liquid will enter suddenly into the room formed by the burst of the steam bubble, resulting in a collision. This event will cause damage. So that there is a decrease in the intensity of the peak of the diffraction pattern of SiC which has 10 hours of ultrasonic experience with HCl.

The analysis results using a match.3 program for SiC ultrasonic results of 10 hours with HCl at 900oC. It can be seen that the temperature affects the bragg angle shift in the XRD results because this increase in temperature will cause an increase in the cavitation and implosion process. there has been a new reaction in this case what is meant is the reaction between SiC and HCl which is assisted by ultrasonic. Meanwhile, the results show that the temperature also affects the value of FWHM. The increase in the value of FWHM is due to the compressive and heat forces so that the crystals are close to each other. Crystallites will break and possibly fill the space between the crystals so that this increases the widening of the crystal lattice. An expansion of the diffraction peak will affect the size of the crystallite and damage to the crystal lattice.

From the results of characterization using Match 3 program obtained diffraction patterns obtained at a temperature of 1000oC Si release occurs from SiC compounds and reacts with Cl4 this can be proved by the ratio of volume C and SiC formed. The ratio of volume C and SiC formed is 56.3%: 46.7%, this proves that at temperatures of 1000oC as much as 56.3% Si reacts with Cl4. So that carbon released from the bond with Si is what can be used as porous carbon which will later be used as energy storage or other uses. The reaction between SiC and HCl which is influenced by the temperature treatment which results in the breaking of the bond between Si and C produces carbon which is a mineral Diamond with a C m m a space group with an crystal system orthorhombic, and has cell parameters a = 4.9640 Å, b = 5.1630 Å, c = 4.3870 Å. While the remaining SiC still has the same crystallographic data as SiC before warming up.

the results of analysis of SiC diffraction patterns of 10 hours ultrasonic results with HCl at a temperature of 1200oC. The results of the match3 program characterization showed that the material formed was C6Cl3N3O6 as much as 78.3% and SiOimpurities4 of 21.7%. Crystallographic data obtained from the match program shows that the crystal system formed is triclinic (anorthic) with cell parameters a = 12.1370 Å, b = 12.1810 Å, c = 11.6940 Å. Material C6Cl3N3O6 is formed because at temperatures of 1200oC chlorine (Cl) gas is actually more reactive to carbon (C), so Si reacts with oxygen (O) this is proven by the formation of SiOcompounds4 as much as 21.7 %. While the element carbon (C) has pores due to release Si reacts with clori gas (Cl), Nitrogen (N) and Oxygen (O).

Conclusion

From this study it can be concluded that Temperature plays an important role in the process of synthesis of silicon carbide to produce carbon which can be used as gas storage material. from the results of the analysis obtained shows that the optimum temperature in producing carbon is at a temperature of C, as evidenced by the formation of carbon as much as 56.3%, which proves that at C Si is reactive to Cl so that it produces carbon.

Reference

[1]. Arthur Lovell. (2007), Tuneable Graphite Intercalates For Hydrogen Storage, Department of Physics and Astronomy, University College London, 3326.

[2]. Deal, D. (1994). Coming Clean What's Ahead in Silicon Wafer Cleaning Technology, Precision Cleaning, II(6) (pp 24).

[3]. Dwi Setyawan, Yeyet C Sumirtapura, Sundani N Soewandh dan Daryono Hadi Tj (2011) Characterization Of Physical Properties Of Binary System Of Erythromycin Stearate-Sodium Starch Glycolate By Compression Force Effect. Sekolah Farmasi Institut Teknologi Bandung.

[4]. Henry Irawan., Sukendro Broto S., Anzhaldy (2017). Studi Eksperimental Deformasi Kristal Pada Daerah Haz Dengan Menggunakn XRD Dan Metode Scherrer. Vol. 02 No.01 (pp 10-16)

[5]. Huang, P.-H., Cheng, H.-H., & Lin, S.-H. (2015). Adsorption of Carbon Dioxide onto Activated Carbon Prepared from Coconut Shells. Journal of Chemitry, 1

[6]. Kotarumalos Nur Aisyah () "Menuju Ketahanan Energi Indonesia: Belahar dari Negara Lain" Peneliti Pusat Penelitian Sumber Daya Regional Lembaga Ilmu Pengetahuan Indonesia.

[7]. Muhammad Asyrik Kurniawan S (2016) "Studi Komputasi Metode Ab Initio Dft Dalam Kajian Struktural Dan Sifat Elektronik Senyawa Kalsium

Borohidrid-Diamonia Sebagai Penyimpan Hidrogen" 2503-2364

[8]. Musfirah Cahya Fajrah Toana, (2010). Sintesa Karbon Nanopori Dari Bahan Silikon Karbida Politipe 6h-SiC.

[9]. Ramadhani I., Handayani I.P., Rosi M (2018) Effects of Coconut Shell's Contents to the Spesific Surface Area of Nanoporous Carbon., e-Proceeding of Engineering : Vol.5 ISSN : 2355-9365 ,5777

[10]. Rosi, M., Abdullah, M., & Khairurrijal. (2009). Sintesis Nanopori Karbon dari Tempurung Kelapa sebagai Elektroda pada Superkapasitor. Jurnal Nanosains dan Nanoteknologi, 26.

[11]. Sethia, G., & Sayari, A. (2015). Activated carbon with optimum pore size distribution for hydrogen storage. Carbon 99, 289.

[12]. Sitti Rahmah, M. Zakir, Musa Ramang, (2014) . Sintesis dan Karakterisasi Karbon Nanopori Sekam Padi Melalui Iradiasi Ultrasonik dengan Aktivator H3PO4 sebagai Bahan Penyimpan Energi Elektrokimia

[13]. Suslick. K. S. (1988). Ultrasound Chemicals, Physicals and Biological Effect, VCH Publishers, Inc

[14]. Suslick. K. S. (1988). Ultrasound Chemicals, Physicals and Biological Effect, VCH Publishers, Inc

[15]. Thommes, M., Kaneko, K., Neimark, A. V., Olivier, J. P., Rodriguez-Reinoso, F., Rouquerol, J., et al. (2015). Physisorption of gases, with special reference to the evaluation of surface area and pore size distribution (IUPAC Technical Report). Pure Appl. Chem., 1054.

Synthesize and Characterization Of $Ni_{(0,5-x)}Nd_xFe_{2,5}O_4$ As A Radar Absorbing Material On Missile – IIDSS2019

Maspin Apit[1], Yunasfi[2], Emriadi[3], Romie O Bura[1]

[1]Weaponry Technology Department, Defense Technology Faculty, Indonesia Defense University, Bogor, Indonesia
[2]Science And Technology Of Advanced Materials, National Nuclear Energy Agency Of Indonesia, Serpong, Indonesia
[3]Chemistry Department, Mathematics and Natural Sciences Faculty, Andalas University, Padang, Indonesia

E-mail: maspinapit@gmail.com

Abstract. Technology needs to be developed on missiles so that they are not detected by enemy RADAR (radio detection and ranging). One of these technologies is the provision of RADAR absorbing material on missiles. The aim of this study is to get a RADAR absorbing material based on ferrite magnetic. $Ni_{(0,5-x)}Nd_xFe_{2,5}O_4$ was synthesized by a co-precipitation method. The result from XRD shows that the sample is 3 phases $NiFe_2O_4$, Fe_2O_3 and $NdFeO_3$. The surface morphology of $Ni_{(0,5-x)}Nd_xFe_{2,5}O_4$ powder was seen using a 20000x SEM magnification, the average particle size of $Ni_{(0,5-x)}Nd_xFe_{2,5}O_4$ is at 100 - 200 nm. The elemental content found in $Ni_{(0,5-x)}Nd_xFe_{2,5}O_4$ powder was seen using EDS which proved that only the peaks of Ni, Fe, O and Nd appeared. VNA (Vector Network Analyzer) characterization show the ability to absorb RADAR electromagnetic waves with maximum RL value by the sample x = 0.2 at about -24 dB which occurred at a frequency of 10.6 GHz.

1. Introduction

Air defense systems have been developed in a sophisticated manner, countermeasures to counteract air defense systems are important considerations in missile design [1]. Missiles are usually difficult to attack on land targets or ships equipped with antiair defense systems. The radar on the anti-defense system is able to intercept missiles fired in the air [2]. Radar (Radio detection and ranging) shows a system that uses reflected radio frequency energy to detect and find objects, measure distance or altitude, navigation, bombing and other uses. Because radar technology has increased dramatically, the development of "stealth" technology to avoid radar detection has become more important [3]. Therefore, technology needs to be developed on missiles so that they are not detected by enemy radar. One such technology is the provision of radar absorbing material on missiles [4]. Radar absorbing materials can significantly improve the survival and penetration of military hardware that is widely used in modern warfare by reducing radar detection [5].

Magnetic metal oxides, such as Fe3O4, Co3O4, CoFe2O4 and NiFe2O4 have many functions because is cheap, non-toxic, environmentally friendly, and various magnetic properties [6]. Nickel ferrite (NiFe2O4) has high permeability, high resistivity, and high magnetic saturation, so it can be used as a radar absorbent material [7]. Addition of rare earthmetals can change the electrical and magnetic properties of nickel ferrite [8]. Examples of rare earth metals that can enhance the magnetic saturation properties of nickel ferrite are neodimium [9]. This radar absorbent material can be utilized on missiles. Missiles that have been coated with this radar absorbing material can avoid detection from enemy radar [4].

One method of synthesis of ferrite compounds is the co-precipitation method. The versatility and simplicity of the co-precipitation method makes it one of the more desirable techniques for making nanoparticles [10]. The co-precipitation method can also be carried out under normal environmental conditions. Using this method, the crystal structure and magnetic properties of the synthesized samples can be optimized by controlling synthesis parameters such as temperature, solvent, pH of the solution, stirring speed, stirring time, metal salt concentration, coprecipitating concentration and surfactant concentration [11]. The purpose of this study was to obtain a cheap, effective and efficient RADAR absorbing material on missile.

2. Materials and Methods

2.1. Materials

The material used is powder $FeCl_3.6H_2O$ (merck), $NiCl_3.6H_2O$ Powder (merck), Nd_2O_3 powder (99.5% purity), 25% HCl solution, NH_4OH 4M solution, Demineralisized water (DM Water).

2.2 Methods

2.2.1 *Preparation of* $Ni_{(0,5-x)}Nd_xFe_{2,5}O_4$. Nd_2O_3 powder was weighed 33.56 g, added 25% HCl solution as much as 78.04 mL, distilled and heated at 80°C until $NdCl_3$ precipitate was formed. Then dried in an oven at 120°C. Then $FeCl_3.6H_2O$ powder, $NiCl_3.6H_2O$ powder, and $NdCl_3$ powder were prepared, each powder material was weighed according to the $Ni_{(0,5-x)}Nd_xFe_{2,5}O_4$ phase stoichiometry with (x = 0; 0,1; 0,2 ; 0,3; and 0,4) then put in a beaker glass. Each powder mixture was dissolved with Demineralisized Water (DM Water) then heated to 80°C while stirring with a magnetic stirrer and then added NH_4OH solution to pH = 9 to form precipitate. The precipitate formed is washed several times until it shows pH = 7. Then dried to a temperature of 120°C in oven. Each mixture of dry powder is continued with a sintered process at a temperature of 1200°C for 3 hours.

2.2.2 *Characterization of* $Ni_{(0,5-x)}Nd_xFe_{2,5}O_4$. Each powder produced by synthesis was carried out phase identification with XRD. Surface morphology and composition with SEM-EDS. Measurement of electromagnetic wave absorption with VNA.

3. Results and Discussion

3.1. X-ray diffraction analysis of $Ni_{(0,5-x)}Nd_xFe_{2,5}O_4$

Figure 1 shows the results of measurements of x-ray diffraction patterns of modification of nickel ferrite with the addition of Nd^{3+} variations (x = 0; 0.1; 0.2; 0.3; and 0.4). The diffraction pattern formed indicates the formation of the $NiFe_2O_4$ phase with its main peak appearing at an angle of 2θ around the 35 ° angle which is the peak field of $NiFe_2O_4$ spinel-shaped cubic and supported by other peaks at angles 18°, 30°, 37°, 43°, 54°, 57° and 63°, which corresponds to the data in the literature (COD card no. 1006116). In addition to the peaks which are the characteristic peaks of $NiFe_2O_4$, there are also other peaks that appear namely Fe_2O_3 and $NdFeO_3$.

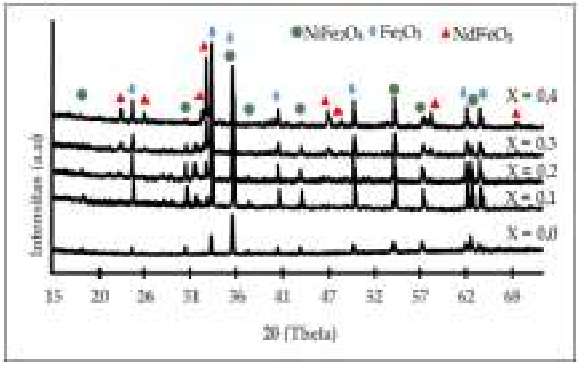


Figure 1. X-ray diffraction pattern of nickel ferrite with Nd^{3+} ion substitution, $Ni_{(0,5-x)}$ $Nd_xFe_{2,5}O_4$ (x = 0 to x = 0,4).

From the XRD pattern the variation of the value of x indicates that the higher the concentration of Nd^{3+} ions added the smaller the intensity of the $NiFe_2O_4$ peak formed while the peak intensity of $NdFeO_3$ is higher, which indicates that the higher the value of x the ability of Nd^{3+} ions to enter into nickel ferrite structures becomes more difficult. This is related to the ability of rare earth metal ions to have limitations in entering spinel structures [12]. These results prove based on mass calculations in Figure 2 which shows the number of neodymium atoms in the core structure then forms the phases of NdFeO3 and Fe2O3 with increasing mass fraction.

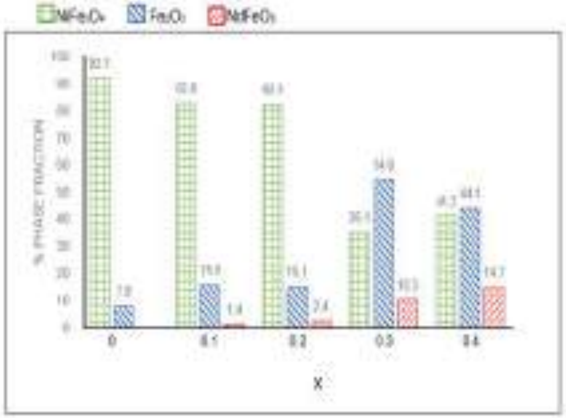


Figure 2. Diagram of % phase fraction at $Ni_{(0,5-x)}Nd_xFe_{2,5}O_4$ (x = 0 to x = 0,5)

Table 1 Cationic distribution in the system of $Ni_{(0,5-x)}Nd_xFe_{2,5}O_4$

Based on Figure 2, it can be determined the cationic distribution of neodymium atoms in nickel ferrite spinel structure as shown in Table 1. Table 1 shows the imperfect neodymium atom substitutes nickel at nickel ferrite structures. At the value of x = 0,1 to 0,2 the presentation of Nd^{3+} in nickel ferrite has increased, while the value of x = 0,2 to 0,4 has decreased. This is due to the difference in particle size between neodimium and nickel, causing a certain limitation of neodymium atoms to substitute nickel atoms in spinel ferrite structures. The highest presentation of neodymium in nickel ferrite is found in the value of x = 0,2 with a value of 88%.

3.2 SEM-EDS analysis of $Ni_{(0,5-x)}Nd_xFe_{2,5}O_4$

The surface morphology of $Ni_{(0,5-x)}Nd_xFe_{2,5}O_4$ powder was seen using a 20000x SEM magnification, the results are shown in Figure 3. From SEM, the average particle size of $Ni_{(0,5-x)}Nd_xFe_{2,5}O_4$ is at 100 - 200 nm. The elemental content found in $Ni_{(0,5-x)}Nd_xFe_{2,5}O_4$ powder was seen using EDS in Figure 4 which proved that only the peaks of Ni, Fe, O and Nd appeared. This indicates that the synthesized powder is free from the elements of the reaction byproducts such as N, H, Cl, and O which are the constituent elements of NH_3, Cl_2 and H_2O compounds. This result is in accordance with the results of XRD which shows the absence of peaks of compounds NH_3, Cl_2 and H_2O.

X composition	%Nd^{3+} in Nickel Ferrite	%Nd^{3+} in $NdFeO_3$
0	0	0
0,1	86	14
0,2	88	12
0,3	64	36
0,4	60	40

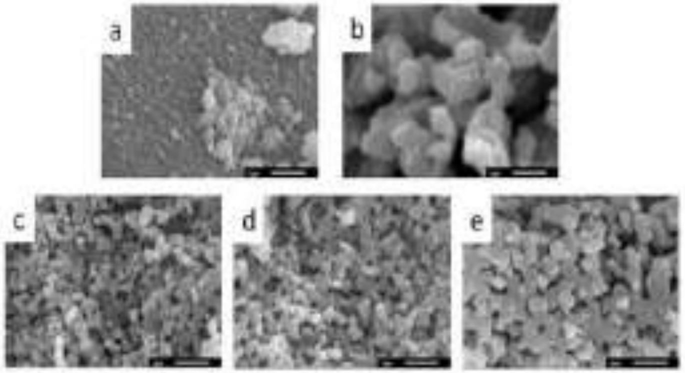


Figure 3. Surface morphology of $Ni_{(0,5-x)}Nd_xFe_{2,5}O_4$ powder with variations x (a) 0,0 ; (b) 0,1; (c) 0,2; (d) 0,3; and (e) 0,4

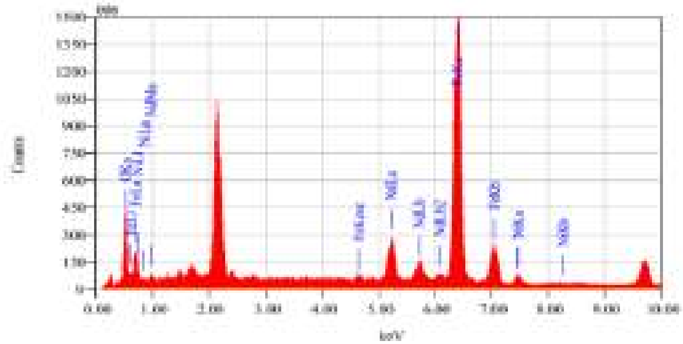


Figure 4. EDS spectrum of $Ni_{(0,5-x)}Nd_xFe_{2,5}O_4$ powder

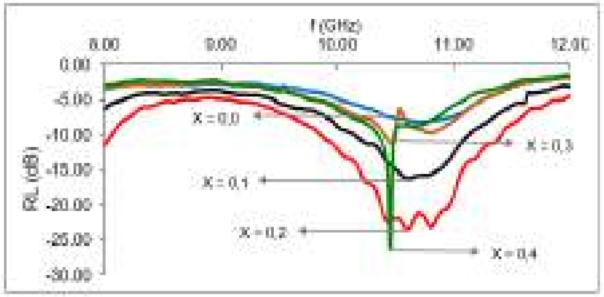


Figure 5. Reflection loss (RL) of $Ni_{(0,5-x)}Nd_xFe_{2,5}O_4$ powder with variation of Nd^{3+} ion doping at a frequency 8-12 (Ghz).

3.3 VNA analysis of $Ni_{(0,5-x)}Nd_xFe_{2,5}O_4$

The relationship between reflection loss (RL) and the frequency of $Ni_{(0,5-x)}Nd_xFe_{2,5}O_4$ powder can be seen in Figure 5 electromagnetic wave absorption is carried out at a frequency of 8-12 GHz. From the picture it can be seen that the increase in the nature of the electromagnetic wave absorption by the $Ni_{(0,5-x)}Nd_xFe_{2,5}O_4$ sample increases as the number of Nd^{3+} ion doping increases. But it is not the case with the doping variation of Nd^{3+} x = 0,3 and x = 0,4 ions.

Table 2 The maximum RL values and bandwidth for each sample

X	RL max (dB)	*Bandwidth* under -5 dB (GHz)
0	-8,22	10,02 – 11,24
0,1	-16,36	9,48 – 11,62
0,2	-23,52	9,10 – 11,92
0,3	-11,26	9,82 – 11,24
0,4	-26,27	9,76 - 11,10

In doping Nd^{3+} x = 0,3 ion has decreased the absorption properties of electromagnetic waves, while at x = 0,4 has narrowed the frequency range of absorption of electromagnetic waves. This is because at x = 0,3and x = 0,4 the $Ni_{(0,5-x)}Nd_xFe_{2,5}O_4$ compound is formed very little, while Fe_2O_3 and $NdFeO_3$ are formed more and more. According to Muflihatun et al, The appearance of an antiferomagnetic phase of Fe_2O_3 can reduce the magnetic properties of nickel ferrite [11]. This resulted in reduced absorption properties of $Ni_{(0,5-x)}Nd_xFe_{2,5}O_4$. But it is not the case with $NdFeO_3$ which is slightly ferromagnetic [13], the combination of this composite make a unique properties in absorbing electromagnetic wave. Table 2 shows the best results obtained on doping Nd^{3+} x = 0,2 ions. Where the maximum RL value is -23,52 dB at 10,6 Ghz with a wide bandwidth value below -5 dB at a frequency of 9,10 to 11,92 Ghz when compared to other samples.

4. Conclusion

From the research that has been done, it can be concluded that the composition of $Ni_{(0.5-x)}Nd_xFe_{2,5}O_4$ can be synthesized using the co-precipitation method while there are still impurities such as Fe_2O_3 and $NdFeO_3$. The optimal x value is obtained on Nd^{3+} x = 0.2 doping ion which has a maximum loss loss (RL) value of -23.52 dB at 10.6 Ghz and also has the widest bandwidth value at the frequency of 9.10 to 11.92 Ghz if compared to other samples. $Ni_{0,3}Nd_{0,2}Fe_{2,5}O_4$ is able to absorb RADAR electromagnetic waves by almost 94% at a frequency of 10.6 GHz. Thus, the $Ni_{(0.5-x)}$ $NdxFe_{2,5}O_4$ can be applied as a RADAR absorbing material on missiles.

Acknowledgements

On this occasion the author would like to say thanks to Science And Technology Of Advanced Materials, National Nuclear Energy Agency Of Indonesia, Serpong, Indonesia, which facilitated this research.

References

[1] Yogaswara 2018 Guidance Synthesis for Evasive Maneuver against Intercept
Missile based on Improved Repulsive Potential Function (Aerospace Engineering, faculty of Korea Advanced Institute of Science and Technology)

[2] Jianbo Z and Shuxing Y 2018 Integrated cooperative guidance framework and cooperative guidance law for multi-missile Chinese Journal of Aeronautics 31 (3) pp 546-555

[3] Dongyoung L, Ilbeom C and Dai G L 2019 Development Of A Damage Tolerant Structure For Nano-Composite Radar Absorbing Structures Composite Structures

[4] Sachin T, Pandey V S, Himangshu B B, Nitin T, Avesh G, Shivanshu G and Trilok C S 2018 RADAR absorption study of BaFe12O19/ZnFe2O4/CNTs nanocomposite Journal of Alloys and Compounds 731 pp 584-590

[5] Wanchong L, Lihai L, Chusen L, Yan Wang and Jinsong Zhang 2019 Radar absorbing combinatorial metamaterial based on silicon carbide/carbon foam material embedded with split square ring metal Results in Physics

[6] Kaichuang Z, Xinbao G, Qian Z, Tianpeng L, Hao and Xuefang C 2017 Synthesis, characterization and electromagnetic wave absorption properties of asphalt carbon coated graphene/magnetic NiFe2O4 modified multi-wall carbon nanotube composites Journal of Alloys and Compounds 721 pp 268-275

[7] Zhu Y and Juhua L 2016 Effects of Ce-Zn co-substitution on structure, magnetic and microwave absorption properties of nickel ferrite nanoparticles Journal of Alloys and Compounds 695 pp 1185-1195

[8] Lenin N, Sakthipandi K, Rajesh R K and Rajesh J 2018 Effect of Neodymium ion on the Structural, Electrical and Magnetic Properties of Nanocrystalline Nickel Ferrites Journal Ceramics International 44 (10) pp 11562-11569

[9] Munir A, Ahmed F, Saqib M, and Anisur R M 2016 Partial correlation of electrical and magnetic properties of Nd substituted Ni–Zn nanoferrites, Journal of Magnetism and Magnetic Materials 397 pp 188–197

[10] Sylvia L 2005 A Multifunctional approach to development, fabrication, and characterizations of Fe3O4 composite (Gorgia Institut of Technology)

[11] Muflihatun, Shofiah S, dan Suharyadi E 2015 Sintesis nanopartikel Nickel Ferrite (NiFe2O4) dengan metode kopresipitasi dan karakterisasi sifat kemagnetannya Jurnal Fisika Indonesia 55 XIX

[12] Dixit G, Singh J P, Srivastava R C, and Agrawal H M 2013 Structural optical and magnetic studies of Ce doped NiFe2O4 nanoparticles Journal of Magnetism and Magnetic Materials 345 pp 65–71

[13] Przeniosto R, Sosnowska I, Fischer P, Marti W, Bartolome F, Bartolome J, Palacios E, and Sonntag R 1996 Magnetic moment ordering of Nd3+ and Fe3+ in NdFeO3 at low temperature Journal of Magnetism and Magnetic Materials 160 pp 370-371

[14] Yunasfi, Maspin A, Wisnu A A dan Emriadi, 2018, Analisis Fasa Dan Sifat Magnetik Bahan Absorber Ni(0,5-x)NdxFe2,5O4 M.I.P.I. 12 (1) pp 25 – 32

Managing the growing risk against drone threats - IIDSS

Tom Park[1] and Nugroho Sasongko

[1]Dronemap Technology, a startup from the University of NSW, 60 Station Street, Parramatta NSW 215, Australia. www.dronemap.com.au

E-mail: tom.park@dronemap.com.au

Abstract. The rapid growth of drone use has highlighted a growing risk to national safety. What is the current technology capability of drones today? And how can security forces safeguard against the use of drones for terrorism. In this paper, we discuss the draft proposal of the Australian Civil Aviation Services Authority (CASA), National Drone registration and accreditation scheme, which is planned to be released by the end of 2019. We explore that reason for this policy and the implication for national security, by taking a dive into the current and future technology trend. We highlight the importance of collaboration between the regulators, industry, and drone manufacturers, for developing an effective and commercially viable solution against drone threats.

1. Introduction

There is no disagreement that drones are here to stay and that they will continue to evolve and be integrated into our everyday society. Businesses and governments are all embracing affordable drone technology as a way to do their work faster, safer, and more efficiently, Figure 1 [1]. What was once a recreational hobby has now become one of the most disruptive inventions in our modern times. The days of watching science fiction movies like Star Wars and fantasizing are over, the dawn of drones is upon us.

As more drones are used, the risk for flying in sensitive airspace and unauthorised areas are increasing. Many incidents have been documented showing the various dangers and interference that brings about a new challenge for maintaining safety. Some of the incidents include; a drone crashing on the White House lawn by passing a high level of security [3], possible new danger to political leaders. It has also been reported that major sporting events with thousands of people, such as the US Tennis Open and the World Cup Skiing Race, were disrupted by a drone crashing from the sky [5]. The presence of drones has also interfered with firefighting planes [4], putting lifesaving rescue officers in further danger. In fact, the FAA (Federal Aviation Authority) has published data showing more than 300 incidents involving drones were reported in California between April 2014 to Jan 2016, which is estimated at 15 incident per month on average or 1 every 2 days [6]. A growing and concerning trend is the use of drones by criminals, often used for smuggling drugs and contraband items into prisons [2]. But an even more concerning trend has been the easy accessibility of drones with capable features, to use for acts of terrorism. An assortment of methodologies have been investigated to prohibit drone threats. These include shooting nets at the unauthorised drones to alter their propeller to cut them down [7], the use of lasers [8], spoofing GPS to trick the drone of its location [9], taking control of the drone software system by hacking into them [10], using another drone to intersect the flight path of the illegal drone [11], and some have used the old traditional method of training a falcons to assault and cripple drones [12]. In any case, these ban techniques ordinarily assume that the drone have been identified and confirm as unauthorised, which is a supposition that is right now hard to achieve and complex.

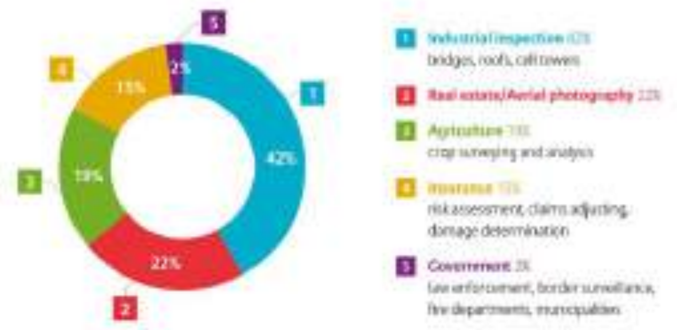


Figure 1. Drone usage by industry, a forecast for the coming decade.

In this paper with discuss at high levels the current technology that is most effective for detecting drones, namely RF communication, and discuss the policy changes that local authorities are adopting to mitigate this emerging risk. In particular, we explore the Australian Civil Aviation Safety Authority (CASA) drone registration legislation, as well as the future safety plan to be introduction by the world largest drone manufacturer DJI's. Our aim is show that the most effective way to mitigate this growing risk is for security intelligence agencies, drone manufacturers, and security solution providers collaborate together. There is no one silver bullet solution as it involves a complex design and development of the right detection technology with good regulations and policies.

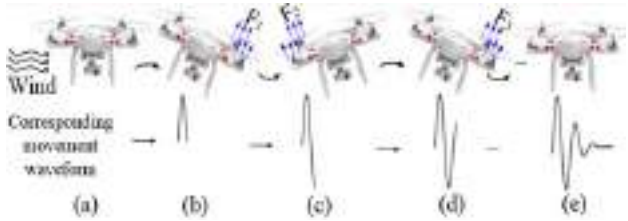
2. Drone detection technology

There is no cost-effective method of detection drones in the market that is fully reliable, although the current method of using radar system is possible, often it is difficult to distinguish a drone from flying objects such as birds. RF-based and Acoustics detection systems are the two most feasible and inexpensive solutions available in the market which can be deployed at large scale.

RF-based detection is an inexpensive solution. By examine the wireless signal transmitted by drones as it communicates with the controller system, the physical features of the drone, the body sifting and body vibration can be used to identify and detection established. This method is passive in that it examines the RF communication channel (Wi-Fi standard) to uniquely differentiate the drone from other surrounding wireless signals such as mobiles and vehicles also carrying Wi-Fi. Using a low-cost COTS hardware platform, passive aerodynamics motions of the drone's movement (flight signature) can be identified, its body shifting signals as it vibrates due to the spinning propellers.

A drone's unique signature or flight signature that current detection technologies leverage, is mainly determined by the adjustment that the drones make to steady itself from the unpredictable environment in its flight path; such as gust of wind, magnetic storms, and sensors not working correctly. As the controller adjusts for the undesired physical movement of the drone, its persistent movement changes are what defines a unique identifiable signature. The main components to determine the drone signature are the drone's body sifting and body vibration behaviour.

Drone body shifting. Body shifting of a drone can be considered as a sequence of discrete events. Figure 2 illustrates how wind (a, b) can influence the drone body movement as the consequence of rebalancing from the drone's controlling mechanism (c, d). As the unexpected conditions surrounding the drone causes it the drone's body to drift and change orientation, the angular velocity by the rotors creates a force, F1, in the rotors directional axis, along due to acceleration, torque around the rotor axis is also created. When unforeseen forces like the wind changes the balance of the drone, the drone (or controller) navigates to bring stability by right side propeller speeding up to create counter balance for F2, ,(F1 ⇡F2). If force F2 continues more than required, it produces a shift that unbalances the drone again, thus the controller or internal algorithm automatically exerts a force F3 to bring the drone back to balanced state. This process goes



several times depending on the environment until the drone reaches equilibrium. This is the most specific method of detection drones and it is this behaviour can be considered as a unique signature of a flying drone, distinguishable from other flying objects.

Figure 2. Drones shifts due to the effect of unexpected wind and environmental conditions speeds the propeller of the drones to exert corresponding Forces (F) to keep them in steady equilibrium and balance.

Drone body vibrations. Depending on the design and rotation of their propellers, drone vibration can be detected at certain frequency range. The resulting vibration is the vector sum of vertical, longitudinal, and lateral vibrations and the frequency of the vibration is close to the frequency of the force or inserted motion, with the magnitude correlating to the actual mechanical system such as the brand and make [13]. By sample various drones' models we are able to create a library of vibration signatures, models can be developed and used in detecting known specific drones mechanical design by matching. This strategy is known as Event Sound Classification (ESC) and is a current research topic for researchers who are using the latest machine learning techniques to find features and classifiers. Some of the most common features and classification models are build using the Mel-frequency Cepstrum Coefficients (MFCC) [14] combined with the Gaussian Mixture Model (GMM) [15]. Currently with the exponential development of AI Methods, there has been more accuracy established with Deep Neural Networks (DNNs), more precisely using Convolutional Neural Network (CNN) [17] and Recurrent Neural Network (RNN) [16]. The Australian startup called Dronemap [23] uses these AI methods and is currently investigating the use of acoustic sounds to improve the efficiency of detection.

3. Drone manufacturers and regulators collaboration is the key to safety

With the rise in concerns about the potential security threats of drones, there has been increased usage of anti-drone technology to neutralize the drones. The global anti-drone market is estimated to grow a CAGR of approximately 20% from 2018 to 2023. To capitalise on the growing opportunity, DJI the world largest drone manufacturing has released a paper conveying the safety features that will be incorporated in the future drone releases and to spark discussion between industry and regulators on how to prevent the dangers and risk posed by unauthorised use of drones[18]. Their outline 10 initiatives which are shown in Table 1. Although it is perceived to be a burden on drone users, industry and governments regulators, the collaborative implementation of these initiatives is essential for maintaining safety and public confidence.

Table 1. DJI have identified 10 clearly beneficial steps for drone manufacturers, the industry, and government / regulators and are campaigning for immediate implementation

Item	Recommendation Plan
1st	DJI will install data collection receivers in all new drones above 250 grams
2nd	DJI will develop a new automatic warning for drone pilots flying at extended distances
3rd	DJI will establish an internal Safety Standards Group to meet regulatory and customer expectations

4th	Aviation industry groups must develop standards for reporting drone incident
5th	All drone manufacturers should install geo-fencing and remote identification
6th	Governments must require remote identification
7th	Governments must require a user-friendly knowledge test for new drone pilots
8th	Governments must clearly designate sensitive restriction areas
9th	Local authorities must be allowed to respond to drone threats that are clear and serious
10th	Governments must increase enforcement of laws against unsafe drone operation

To coincide with DJI initiatives, the Australian Civil Aviation Safety Authority (CASA) is planning to introduce drone registration and accreditation scheme from later 2019[19]. This has been conducted with community consultation and feedback. The proposed registration and accreditation requirements apply (with certain exceptions) to:

- Drones more than 250 grams operated recreationally
- All drones operated commercially regardless of weight.
- Flyers under 16 years of age need to be supervised by someone 18 or older who is accredited
- Accreditation will be an online education course to make sure you know the rules
- Registration for recreational flyers will be less than $20
- For commercial flyers registration is likely to be from $100 to $160 per drone.

Note: CASA has yet to determine if registration needs to be before or after purchase of the drone.

The registration of drones into a centralised database is very crucial for the future safety of drones. As the ADS-B(Automatic Dependent Surveillance-Broadcast) replaces radar as the primary surveillance method for air traffic control [20], it is expected that drones will follow a similar type of broadcasting mechanism to quickly identify unregistered or non-compliant drones for a potential threat. DJI's has a software system, called AeroScope, and is one of the first widely available remote identification solutions, It allows airport operators, law enforcement, safety agencies and other authorities to automatically determine the location, direction, altitude and the serial number of DJI drones in the area. It even broadcasts the location of the drone pilot [21]. DJI has stated that they will install the AirSense ADS-B feature on every new drone it releases after January 1, 2020, that weighs more than 250 grams [22]. This solution is in use in at least 20 airports in the United States alone, as well as 13 large U.S. sporting venues and dozens of other facilities where safety and security are top concerns. It must be highlighted that DJI does not identify their customers' details unless they choose to disclose their use of the system. This calls for policymakers and regulators to collaborate together so as to develop a risk management framework that could be adopted as a blueprint by the global drone community.

4. Conclusions

The era of drones has arrived. Drones uptake for commercial use has been steadily increasing and grow faster with the advances in computer image recognition and AI. As technology becomes mainstream, there is a growing risk for terrorist to use drones to commit violent attacks.

We have seen from our discussion that the most efficient way of detecting drones is to listen and identify the drones RF-Signatures, suing algorithms that recognise the body movement and vibration during flight. In practise the algorithms could be developed for all detection systems like radar, acoustics and even visual CCTV cameras, and the required solution will depend on the risk management approach taken. Government authorities such as CASA in Australia, are mandating that drone ownership be recorded into a centralised registry database. This step will be crucial for the next generation of integrated IoT data-driven management system. The combination of centralised registration intelligence and the self-broadcasting (e.g. ADS-B) features of future drones, will make it possible to detect unauthorised drone threats quickly and without the need of having an expensive infrastructure. It is recommended that jurisdictions and authorities unify together and regulate that all drone manufacturers install the self-broadcasting features into their future products and make it a mandate for drone pilots to be registered into a centralised system similarly to Australia's CASA initiative.

References

[1] Source: FAA Aerospace Forecast FY2016-2023

[2] W. Post. Prisons try to stop drones from delivering drugs, porn and cellphones to inmates. https://goo.gl/6DapQM, October 13, 2016.

[3] B. Jansen. Drone crash at white house reveals security risks. USA Today, January 26, 2015

[4] P. McGreevy. Private drones are putting firefighters in 'immediate danger,' california fire ocial says. LA Times, August 18, 2015.

[5] D. Waldstein. Drone crash interrupts match. New York Times, September 3, 2015.

[6] L. Times. To keep drones out of high-risk areas, companies try hijacking them and shooting them down. https://goo.gl/MqDag5, 2016. [Online; accessed Nov 01, 2016].

[7] D. Sathyamoorthy. A review of security threats of unmanned aerial vehicles and mitigation steps

[8] R. Vander Schaaf. What technologies or integrating concepts are needed for the US military to counter future missile threats looking out to 2040? PhD thesis, US Army, 2014.

[9] T. HUMPHREYS. Statement on the security threat posed by unmanned aerial systems and possible countermeasures, 2015.

[10] J.-S. Pleban et al. Hacking and securing the ar. drone 2.0 quadcopter: investigations for improving the security of a toy. In SPIE Electronic Imaging, 2014.

[11] CNN. Dubai deploys a 'drone hunter' to keep its airport open. https://goo.gl/iXJMu3, 2016. [Online; accessed Nov 01, 2016].

[12] BBC. Dutch police fight drones with eagles. https://goo.gl/PnJCcd, September 12, 2016.

[13] L. L. Beranek. Noise and vibration control engineering: principles and applications. Wiley, 1992.

[14] Berger et al. Signal processing for passive radar using ofdm waveforms. IEEE Journal of Selected Topics in Signal Processing, pages 226–238, 2010.

[15] Bluetooth. Bluetooth hc-05. https://goo.gl/0PKs6r, 2016. [Online; accessed Nov 01, 2016].

[16] Buonanno et al. Wifi-based passive bistatic radar by using moving target indicator and least square adaptive filtering. In IEEE International Symposium on Phased Array Systems & Technology, pages 174–179, 2013.

[17] E. Bregu, N. Casamassima, D. Cantoni, L. Mottola, and K. Whitehouse. Reactive control of autonomous drones. In ACM MobiSys, pages 207–219, 2016.

[18] DJI White Paper: Elevating Safety: Protecting The Skies In The Drone Era.

[19] CASA Website www.casa.gov.au

[20] P&E: ADS-B, THE BUZZ ABOUT TRANSPONDERS https://www.aopa.org/news-and-media/all-news/2015/september/pilot/adsb

[21] www.dji.com/aeroscope

[22] dronelife.com/2019/05/22/dji-to-install-airsense-ads-b-receivers-drones-from-2020

[23] www.dronemap.com.au

NUMERICAL APPROACHES FOR OPTIMIZED DESIGN OF HULL PROTOTYPE FAST PATROL CRAFT 40 METERS MATERIAL ALUMINIUM ALLOY

Syarifuddin[1], Sovian Aritonang[2]

[1]Power Motion of Technology, Faculty of Defense Technology Indonesia Defense University, Komplek Indonesia Peace and Security Center (IPSC) Sentul, Bogor, Indonesia

E-mail : [1]syarifuddin@tp.idu.ac.id, [2]sovian.aritonang@idu.ac.id

ABSTRACT

Basic design of hull fast patrol craft 40 meters material aluminum alloy using performance speed optimal with scope numerical work : evaluation of the bare hull form in the terms of resistance at operating condition, optimization of hull form in terms of resistance at operating condition, evaluation of the final hull form in terms of resistance at operating condition. Input data and numerical parameters with input file provided by design (CAD files, hydrostatic particulars, line plan, update hydrostatic particulars and general arrangement plans), coordinate systems, simulation parameters and solvers (calm water resistance, solvers), description of CFD solvers (free surface, turbulence models, meshing, other characteristics), geometry and hydrostatic particulars, hull form estimation constraints. Conclusion performance speed optimal with scope numerical work ad: Evaluation and speed prediction of the initial hull form (the initial hull form was evaluated in term of resistance for hull loading condition and three speeds, considering a hull efficiency of 0.98, a propeller efficiency of 0.70 and a sea margin of 15%, the speed of the initial patrol craft at 100%MCR = 27.8 knots and at 85%MCR = 25.7 knots. Hull form optimization (gains at observed when moving afterward the LCB, emphasizing the V shape of the hull, moving inward the step, enlarging the step, moving forward the bow, increasing the bow slop and moving downward the transom. Maximum gains with separate deformations are observed for the asymmetric lacked by deformation, ID070 and area equal to 5.72%, the combination of global deformation leads to a maximum of again equal 8.22% for the hull form ID079. Evaluation and speed prediction of the final hull form (the final hull form ID079 was evaluated in the terms of resistance for full loading condition and four speeds, considering a hull efficiency of 0.98, a propeller efficiency of 0.70 and sea margin of 15%, the speed of the optimized patrol craft at 100%MCR = 28.9 knots and 85%MCR = 26.6 knots.

1. Introduction

Scientific interest on the resistance of shallow water effect existed with the growth of ship size and added shipping routes congestion. Prakash and Chandra [1] stated that the resistance of ship in shallow water is quite sensitive and the flow around the hull changes appreciably. Therefore, a comprehensive understanding on the shallow characteristic in respect to peculiar added hydrodynamic forces is obviously required to obtain a more appropriate prediction of the power requirement [2]. The sinkage and trim in very shallow water can set an upper limit to the speed so that the ship can operate without grounding. The wave patterns, created by the moving ship, change in shallow water and lead to change in the wave making resistances. Jachowski [3] stated that during ship motion in shallow water there are phenomenon when the clearance decrease. There are different flow velocities and change in water pressure along the hull. In shallow water there is a small pressure value at the midship as compared to the deep water condition and a bigger pressure value exists in the ship bow and aft parts. Design of hull fast patrol craft 40 meters material aluminum alloy using performance speed optimal with scope numerical work : evaluation of the bare hull form in the terms of resistance at operating condition, optimization of hull form in terms of resistance at operating condition, evaluation of the final hull form in terms of resistance at operating condition. Input data and numerical parameters with input file provided by design (CAD files, hydrostatic particulars, line plan, update hydrostatic particulars and general arrangement plans), coordinate systems design, simulation parameters and solvers (calm water resistance, solvers), description of ISIS-CFD solvers (free surface, turbulence models, meshing, other characteristics), geometry and hydrostatic particulars, hull form estimation constraints.

2. Parametric Model

2.1 Design of ship parametric as the follow is length over all 45.50 meters, length water line 40.80 meters, breadth 7.90 meters, depth mold 4.80 meters and draft 1.8 meters and analysis with the follow scope of numerical work : phase-1 is evaluation of the bare hull form in the terms of resistance at operating condition, phase-2 is optimization of hull form in terms of resistance at operating condition with 3 (three) operating conditions (1 loading condition : full load, 3 speeds : 26.0, 28.0 and 30.0 Knots), phase-3 is optimization of hull form in terms of resistance at operating condition with 1 operating condition (1 speed : 28.0 Knots), evaluation of the final hull form in terms of resistance at operating condition with 3 operating conditions (1 loading condition : full load, 4 speeds : 24.0, 26.0, 28.0 and 30,0 Knots).

2.2 Simulation parameters and solvers is calm water resistance with full scale simulation, a fixed velocity is imposed to the hull (from rest to the target speed), simulation are unsteady with free heave and pitch, mean values are averaged after a stabilization phase of forces and motions speeds (26.0, 28.0 and 30.0 Knots), resistance is performed using a towing point located at : x = 2.24 m, y = 1.50 m, z = 0.442 m, shaft angle 8^0, the center of gravity is located at full load condition : x = 18.25 m, y = 0.00 m, z = 3.00 m, water characteristic are for salt water is density : 1025. Kg/m^3, dynamic viscosity : 1.22 x 10^{-3}Pas, solver with ISIS-CFD using the k-w SST turbulence model.

2.3 Coordinate system which using dynamic trim and dynamic sinkage are given with respect to coordinate system design as the difference from hydrostatic position (in degrees and meters), they are given at the center of gravity of ship, origin is located at the intersection of symmetry plane, aft perpendicular and keel line, X axis is oriented toward ship bow,Y axis is oriented port side and Z axis is oriented up.

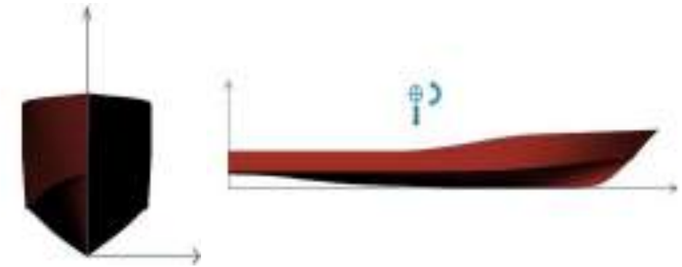
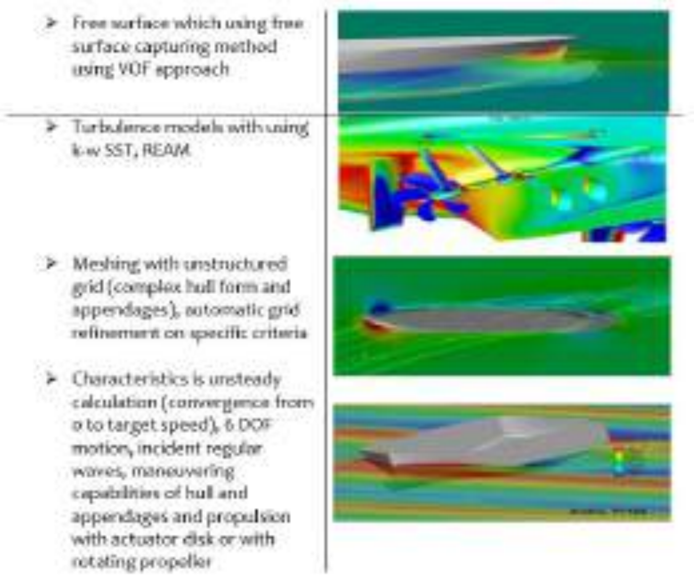


Fig. 1. Coordinate system x, y, z

2.4 Description of ISIS-CFD solver.

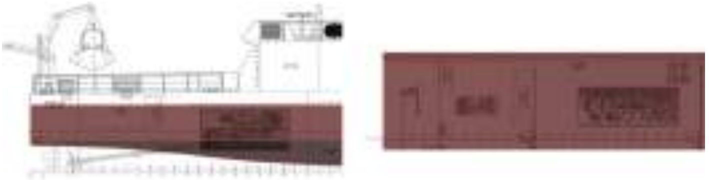


- Free surface which using free surface capturing method using VOF approach
- Turbulence models with using k-w SST, REAM
- Meshing with unstructured grid (complex hull form and appendages), automatic grid refinement on specific criteria
- Characteristics is unsteady calculation (convergence from o to target speed), 6 DOF motion, incident regular waves, maneuvering capabilities of hull and appendages and propulsion with actuator disk or with rotating propeller

2.5 Input data files provide are listed the following table :

Name of file	Descriptions
FPC 40 Meters	CAD files
FPC 40 M- Opt - Hydrostatic	Hydrostatic particulars
Lines plan Based 8-degree Engine. dwg	Lines Plan
Hydrostatic Data FPC 40 M	Updated hydrostatic particulars
General Arrangement FPC 4 M	General Arrangement plan

2.6 Hull form optimization constrains with one constraint have to be respected where the aft hull form must not be 15-20% more slim in order to not affect the engine, the following figure present the cylinder used to validate that hull form deformation respect constraint.



3. Numerical Analysis

3.1 Resistance of ship

Resistance is a fluid force that works on the body of the ship in such a way that it works against the movement of the ship [4]. Ship resistance is defined as follows:

$R_T = ½.C.\rho.\ S.\ V^2$

(1)

Where:

R = Resistance total of ship (KN)

V = Speed of ship (m/s)

ρ = sea water specific gravity (Kg/m^3)

S = wet surface area of ship (m^2)

3.2 Effective horse power

Effective horse power (EHP) is the power needed to move the ship in water or to pull the ship at speed. Calculation of ship's effective horse power (EHP) according to the defined as follows:

$EHP = R_T \text{ x } V$ (2)

Where :

EHP = Effective horse power (MW)

R_T = Resistance total of ship (KN)

V = Speed of ship (m/s)

3.3 Lift coefficient

Lift coefficient is indicated by the location of a fast ship deadrise (β), when the deadrise angle formed is zero, (β = 0), the lift coefficient [5] is expressed as follows::

$$Clb = \frac{\Delta}{0.5 \text{ x } \rho \text{ x } V^2 \text{x } B^2} \quad (3)$$

Where :

Clb = Lift coefficient

Δ = Displacement (ton)

ρ = sea water specific gravity (kg/m^3)

V = Speed of ship (m/s)

B = Maximum chine beam (m)

The value of λ which is the average value of comparison between the length and width of the wet area of the ship. Savitsky assumed the prismatic hull form. This assumption carries the consequence that the value of the dead rise angle is a constant number along the hull of the ship. So that the use of Graph Equilibrium planning is used to determine the amount of trim angle (τ) that works on the ship[6].

ISBN 978-602-5808-52-4

9 786025 808524