JSPS-RIDU

STRATEGI PERANG SEMESTA

Journal of Modern Warfare and Defense Strategy

Cyber Community Empowerment Policy as an Effort to Strengthen Cyber Defense

Dhiah Ayu Duwi Wahyuni, Tri Legionosuko, Sutrimo Sumarlan

Published at 31 July 2022

How to cite this article:
Wahyuni, D. A. D., Legionosuko, T., & Sumarlan, S. (2022). Cyber community empowerment policy as an effort to strengthen cyber defense. *Strategi Perang Semesta, 8*(1), 103-110. https://doi.org/10.56555/sps.v8i1.1196

To link to this article: https://doi.org/10.56555/sps.v8i1.1196

STRATEGI PERANG SEMESTA
Volume 8, Issue 1, 103 - 110. [2022]
e-ISSN: 2830-2877, p-ISSN: 2830-2869

REPUBLIC OF INDONESIA
DEFENSE UNIVERSITY

CYBER COMMUNITY EMPOWERMENT POLICY AS AN EFFORT TO STRENGTHEN CYBER DEFENSE

Dhiah Ayu Duwi Wahyuni*
Republic of Indonesia Defense University

Tri Legionosuko
Republic of Indonesia Defense University, INDONESIA

Sutrimo Sumarlan
Republic of Indonesia Defense University, INDONESIA

Abstract
The universal people's defense and security system is a defense system that involves all citizens, territories, and other national resources, prepared by the government early, implemented in a total, integrated, directed, sustainable and sustainable manner for the sake of upholding the sovereignty, and territorial integrity of the Unitary State of the Republic of Indonesia and its protection. The safety of the entire nation and from various threats. Its hoped that this principle will become a loyal basis for the formulation of defense policies in Indonesia, including those related to cyber community empowerment. From this research, it is concluded that there is a need for testing, demonstration, and evaluation which haves several main functions in policy analysis.

Article history:
Received : June 6, 2022
Revised : July 10, 2022
Accepted : July 28, 2022
Published : July 31, 2022

Keywords:
Policy
Community Empowerment
Cyber Defense

Introduction

Scientific advances, especially the development of information and communication technology, greatly impact various aspects of life and relations between countries. The increasingly widespread and increasing use of information and communication technology, especially through the internet network, can affect the increasing threat activities for an individual and country. Based on the 2008 "McAfee Virtual Criminology Report" report, there are 120 countries that utilize internet technology and cyberspace (cyberspace) for political, military, and various electronic spying activities (electronic espionage) aimed at obtaining various information/data related to the economy, intellectual property rights, and various other critical data and information (Siti et al., 2014).

Morgenthau stated that if a country or a nation wants to survive, it must have national power so that it can ensure the continuity of state life both domestically and internationally. This causes the state to be able to anticipate any threats that are expected to occur and threaten its country. Comprehensively, a country must have national power or National Power, which Morgenthau mentioned in his book Politics Among Nations related to elements of national power, including Geography, Natural Resources, Industrial Capacity, Military Preparedness, Population, National Character, National Moral, the Quality of Diplomacy, and the Quality of Government (Supriyatno, 2016).

Cyberwar is all actions that are carried out intentionally and coordinated with the aim of interfering with the sovereignty of the state. Cyber warfare can be in the form of terrorism (cyber terrorism) or espionage (cyber espionage) that interferes with national security. Cybercrime is still one of the most serious threats to Indonesia. This is due to the increase in cyber-attack cases ranging from phishing, malware attacks, and spams to ransomware which is quite significant.

CONTACT Dhiah Ayu Duwi Wahyuni
dhiahayu18@gmail.com

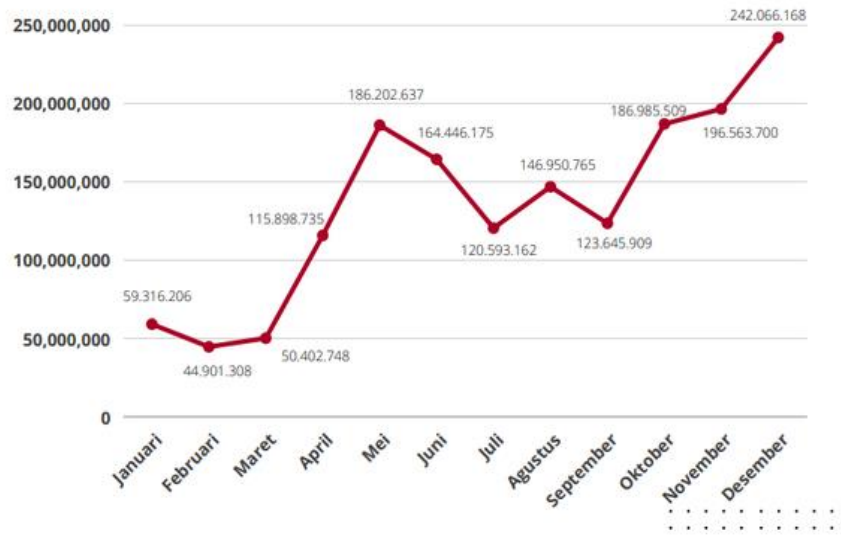
DOI https://doi/org/10.56555/sps.v8i1.1196

In 2019, Indonesian National Cyber and State (BSSN) reported 290 million cyber-attack cases, 25% more than the previous year when cybercrime caused losses of US$ 34.2 billion in Indonesia. Similarly, the CID has seen an increase in reports of cybercrime. In 2019, there were 4,586 police reports filed through cyber patrols. That's an increase from the previous one of about 4,360 reports in 2018 (Rahmawati, 2017).

Meanwhile, based on the BSSN traffic anomaly data report (2021), in 2020, cyber-attacks experienced by Indonesia reached 495.3 million, an increase of 41 percent from the previous year 2019 of 290.3 million. Data from the Global Cyber-security Index (GCI) 2020, which is based on the concept of five assessment categories or called The Five Pillars of the GCI Framework, namely legal, technical and procedure, organizational, capacity building, and international cooperation, shows that Indonesia's cyber-security position is ranked 24th with a score of 94.88, far below Singapore and Malaysia which are in 4th position (98.52)and 5 (98.06) (Berita - Ancaman Kejahatan Siber Di Indonesia Terus Meningkat, n.d.).

From research conducted by Trend Micro, Indonesia's cyber risk index (CRI) in 2020 was at 0.26, in the sense of being moderate risk. In 2021, it dropped to -0.12, which means that the risk has increased, although it has not yet entered the high-risk category. When sorted according to color, 5.01 to 10 is low risk, 0.1 - 5.0 moderate risk, 2.51 to -5.0 elevated risk, and -5.01 to -10 is high risk. So that means Indonesia last year was in yellow, and now it is in the orange area. (Berita - Perang Siber_ Bahayanya Yang Perlu Kita Ketahui & Pahami _ Okezone News, n.d.).

Meanwhile, throughout 2021 based on the National Cyber Security Index (NCSI) ranking, Indonesia's cyber security is ranked 83 out of 160 countries. The Communication & Information System Security Research Center (CISSReC) reported that as of November 2021, there were 1.3 billion cyber-attacks against countries, banks, private, and individuals. According to the State Cyber and Password Agency (BSSN), cyber incidents that occur in Indonesia mostly target citizens' personal data. Personal data has great potential to be misused for a variety of purposes. BSSN data, most cyber-attacks are economically motivated. It means that the quality of cyber-security still needs significant improvement. For example, the State Cyber and Password Agency (BSSN) published an annual "Cyber-security Monitoring" report for 2021.



Graph 1.1 Number of national anomalies in 2021
Source: BSSN's annual "Cyber-security Monitoring" report 2021

This report has been published on the official website of Id-SIRTII/CC (Indonesia Security Incident Response Team on Internet Infrastructure/Coordination Center) under the Directorate of Cyber-security Operations of BSSN. In the report, it explained that there were more than 1.6 billion or precisely 1,637,973,022 traffic anomalies or cyber-attacks that occurred throughout Indonesia throughout 2021.

Based on various official reports, including the annual report from BSSN from 2018 to 2022, Indonesia has experienced hundreds of millions of cyber-attacks; this is a strong indication that Indonesia is very vulnerable to threats and cyber-attacks originating both from within and outside the country. The number of attacks that have occurred is also not comparable to the number of human resources available to deal with these hundreds of millions of attacks, so Indonesia has entered the danger of cyber warfare.

Another impact of cyber-attacks on a large scale can paralyze the critical national infrastructure, which includes various public services ranging from electricity, telecommunications, drinking water, banking, fuel production and refueling etc., which can cause the paralysis of the national economy, and one of the potential paralysis of this paralyses we have experienced together when the power grid in Java and Bali was extinguished three years ago.

By paying attention to the above cyberspace, it is necessary to get proper protection to avoid potential that can harm individuals, organizations, and even the state. Cyber defense exists as an effort to protect a country from various kinds of disturbances and threats. Cyber defense is multilevel from the scope of individuals, working groups, organizations to a national scale. (Ardiyanti, 2016) Special attention is paid to critical infrastructure sectors such as security defense, energy, transportation, financial systems, and other public services. Disruption of electronic systems, falling levels of trust in the government, disruption of public order and others. This risk is a consideration for strong cyber defense in a country (Permanasari, 2017).

In protecting and minimizing cyberspace from cyber threats, cyber-security is needed so that cyberspace can continue to run. Cyber-security consists of practices, actions, and efforts to protect the cyber ecosystem and the assets of companies and users from malicious attacks aimed at disrupting the confidentiality, integrity, and availability of information or data (Fischer, 2005; THAT, 2012).

The state defense system or the universal people's defense and security system is a state defense system in Indonesia that is universal, which in the defense system involves all citizens, territories, and other national resources, prepared by the government early, organized in a total, integrated, directed, harmonious, and sustainable manner for the establishment of sovereignty, territorial integrity of the Republic of Indonesia, and the protection of the safety of the entire nation and from various threats (Law No. 34/2004 on the TNI, article 1 paragraph (6)). Basically, the implementation of state defense is to prevent and overcome threats, both military and non-military, that are real and unreal, both from within and from abroad; the nature of health in *sishankamrata* is interpreted as a form of universal war itself where its management is through a concept called the universe war strategy. The state defense force necessary in the implementation of the universal war strategy to deal with various forms of threats includes all components of the state defense, namely the military defense force (including the main, reserve, and supporting components), as well as the non-military power (covering the main elements and other elements of the nation's power) (Soewardi, 2013).

If you look at several recent cyber-crime cases in Indonesia, the website owned by the Attorney General's Office of the Republic of Indonesia was broken into by a 16-year-old

teenager from Lahat, South Sumatra. He did this because he felt bored because of online schooling since the Corona pandemic. His actions resulted in the website of the Attorney General's Office of the Republic of Indonesia being defaced to change its appearance. On his website, there is a message with a tone of protest and a red stamp HACKED. In addition, he also broke into the database of the Attorney General's Office and sold 3,086,224 staffing data to RAID Forums for IDR 400 thousand. These incidents show evidence that Indonesia's cyber-security is very weak and requires an even better cyber defense strategy. However, it should also be noted related to the capabilities possessed by these Indonesian hackers if they get a platform to channel their capabilities precisely to strengthen the country's cyber defense, it will have a positional impact on the country, such as the Indonesian defense system which should involve the role of the people, territories, and equality.

Community empowerment is an effort to increase human dignity and dignity individually and in social groups. According to the Big Indonesian Dictionary (KBBI), community empowerment is carried out so that the empowered group or community can have the power and ability to act. In other words, empowerment becomes a process to improve the ability and independence of the community in order to improve the quality of life. Empowerment is carried out because of the emergence of an understanding of the community's helplessness; that is, the community does not have power (powerless). In addition, another contributing factor to the absence of power is the presence of inequality, including structural inequality, group inequality, and personal inequality.

There are three strategies that must be applied consistently in dealing with cyber threats, according to Bambang Karsono as Rector of Bhayangkara University, Greater Jakarta (Republika, 2021), including increasing the competence of human resources, structuring the information security governance process, and technology as a solution integrator and product development. Therefore, this makes researchers very interested in studying more deeply related to how cyber community empowerment policies are an effort to strengthen cyber defense.

Method

This study used qualitative descriptive analysis. This method describes and interprets existing conditions or relationships about existing issues or problems, then processes the collected material as a support for problem-solving, then an analysis is carried out, which will later obtain results in the form of conclusions and suggestions (Augina, 2020).

Results And Discussion

The Urgency of Empowering Cyber Communities

In 1929 a columnist named Will Rogers wrote his opinion in a daily The New York Times, in which he argued that every civilization would progress, and every war in that civilization would try to destroy in various cutting-edge ways. In the world of technology, information and communication which are now converging with each other without any national borders, where all communication, both voice and data, will rely on wireless-based communication technology, and also its digital-formatted content so that it will be easier to access through smart handheld telephone devices and others (*Berita - Pengembangan IoT Harus Dibarengi Dengan Kesadaran Keamanan Siber - Medcom*, n.d.).

This then becomes a new problem for each country that is left behind or cannot keep up with existing developments. A country must be able to predict the threats that will be

faced in the future, so that by knowing this, a country can create a defense or deterrent in dealing with these threats in the future in order to maintain the stability of a country's sovereignty.

In the era of technology 4.0, it has implications for four phenomenon in the defense aspect that we need to look at together, namely the evolution of industry 4.0 towards 6.0 in 2026, the formation of a cyber-attack theater with the concept of cyber defense, cyber threats evolving into military or conventional threats (5th generation war) and evolution towards the era of digital transformation based on the Internet of Things. Define and map patterns based on cyber threats, including physical or infrastructure threats in the form of virus threats, malware, DDOS, Brute force, DSB phishing, and for non-physical threats including information warfare, hoaxes, framing to change mindsets. Therefore, cyber threats need to be anticipated, of course, by developing and studying cybercrime and security (Supriyatno, 2016).

The state defense system is universal in nature involving all citizens, territories, and other national resources, and is prepared early by the government and organized in a total, integrated, directed, and continuous manner to uphold the sovereignty of the state, territorial integrity, and the safety of the nation from all non-military threats. In terms of cyber defense, institutionally, the TNI (Indonesian National Army) has had regulatory references in the form of Law No. 11 of 2008 concerning Electronic Information and Transactions (ITE) and Government Regulation (PP) No. 82 of 2012 concerning the Implementation of Electronic Systems and Witnesses. The TNI also refers to the Cyber Defense Guidelines released by the Ministry of Defense in 2014 (Republik Indonesia, 2014).

Cyber defense is a way of enhancing the ability to thwart cyber-attacks. It involves all processes and practices that would defend the network, its data, and code from unauthorized access or manipulation. The most common cyber defense activities are hardware and software infrastructure maintenance that deters hackers. The main asset in cyber-security is personnel or HR, who play a very important role in cyber defense. The biggest challenge in implementing cyber defense is to provide competent human resources and always quickly and swiftly follow the dynamics of the cyber environment that continues to develop along with the development of technology and the social conditions of society. For this reason, the HR development strategy must be supported by a continuous competency improvement program (Republik Indonesia, 2014).

However, it should also be noted related to the capabilities possessed by these Indonesian hackers if they get a platform to channel their capabilities precisely to strengthen the country's cyber defense, it will have a positional impact on the country, such as the Indonesian defense system which should involve the role of the people, territories, and equality. Community empowerment is carried out with the following stages:

a. Awareness related to its existence as an individual or as a member of society, environmental conditions that concern: physical/natural, social, cultural, economic, and political.
b. Indicates the existence of problems, namely undesirable conditions related to nature, humans, infrastructure, institutions, culture, accessibility, physical, technical, socio-cultural, and political environment, including showing the factors that cause internal and external problems.
c. Help solve problems, namely the selection of the best alternative problem solving that can be done according to internal conditions (strengths, weaknesses) and external conditions (opportunities, threats).

d. Demonstrates the importance of changes that are and will occur in their environment. Communities must be prepared to anticipate change through "planned change" activities
e. Conducting tests and demonstrations. This is done on the grounds that not all innovations are suitable for the conditions of society. In addition, to get an idea of the various alternatives that are most beneficial with the least risk or sacrifice.
f. Producing and publishing information. In accordance with the development of technology, the production, and publication of media users need to be adapted to the characteristics of society.
g. Implementing empowerment/ capacity strengthening, namely providing opportunities for the community to determine their own choices concerning information accessibility, involvement in meeting needs, and participation in the development process of public accountability and strengthening local capacity.

Cyber Community Empowerment Policy

Public policy is a series of actions or activities proposed by a person, group in the sense of government in the scope of a certain environment where there are obstacles (distresses) and the possibilities or opportunities where the policy is proposed to be useful in overcoming it to achieve the intended goal. While Empowerment comes from the word "power" which means strength or ability. So, empowerment can be interpreted as a process or series of actions to transform a society that was previously lacking or not yet empowered into empowered. The concept of empowerment itself is in line with community development, which is the process of building interaction networks. This is done to develop the community's quality of life by increasing the capacity of all community members, then carrying out sustainable development (Arief & Widjayanto, 2021).

Empowerment arises because of the helplessness of the community, that is, a society that does not have power (powerless). In addition, other causative factors beyond the absence of inequality include structural inequality, group inequality, and personal inequality. Improving the ability or strength of a community is not easy, so empowerment must be carried out continuously and continuously. The success of empowerment does not only focus on achieving the program but also on the high participation or involvement of the community itself.

Let's examine the increasing cases of cyber-attacks both from within and outside the country in Indonesia every year. It is enough to prove that cyber defense in Indonesia is still fairly weak. Then how can we strengthen cyber defense in Indonesia. From the problems related to the lack of optimal empowerment of the existing cyber community, it is necessary to evaluate existing policies to give rise to new policies that can correct the shortcomings and weaknesses in the old policies.

Formulating policy problems is one of the crucial stages in reviewing public policy because many policy formulations fail to solve public problems not because the method used to solve these problems is wrong, but rather to be freed by problems that are solved incorrectly (Arief & Widjayanto, 2021).

The stages carried out in the implementation of Public Policy are agenda preparation, policy formulation, policy legitimacy, policy implementation, and policy evaluation. These stages are carried out so that the policies built can achieve the desired goals (Budi Winarno, 2007: 32-34):

a. The preparation of events is a very strategic phase and process in the reality of public policy. It is in this process that there is room to interpret the so-called public issues, and priorities in public events are contested. Policy issues are often referred to as policy problems. The preparation of policy events must be carried out based on the level of urgency and essence of the policy, as well as the involvement of stakeholders.
b. Policy Formulation, Issues that have been included in the policy event are then discussed by policymakers. These problems are defined to then find the best division of the problem. The division of the issue comes from several existing policy options.
c. Policy Choice, the purpose of legitimacy is to authorize the basic governance processes. If the sovereignty of the people governs the act of legitimacy in a society, citizens will follow the direction of the government.
d. Policy Implementation: The policy implementation section will find the consequences and performance of the policy. Here it will be found whether the policies that are built achieve the desired goals or not.
e. Policy evaluation is an activity that concerns estimation, aka the quality of policies that cover substance, implementation and consequences. This factor, means that policy evaluation is not only carried out at the end but in the entire policy process. Thus, policy evaluation can include part of the formulation of policy problems, proposed programs to solve policy problems, implementation, and part of policy consequences.

Policy evaluation is seen as functional activity. This means that policy evaluation is not only carried out at the final stage but also at the entire policy process. According to W. Dunn, the term evaluation has a related meaning, each pointing to the application of several scales of value to policy and program results. Evaluation includes conclusions, clarifications, criticisms, adjustments, and re-formulation of the problem. Evaluation has several key functions in policy analysis. First and most importantly, evaluation provides valid and reliable information regarding policy criteria, namely, how far the needs, values and opportunities that have been achieved through public action. In this case, the evaluation reveals how far certain goals and targets have been achieved.

Second, evaluation contributes to the clarification and criticism of the value underlying the selection of goals and targets. Value is clarified by defining and operating goals and targets. Value is also criticized by systematically asking about the appropriateness of goals and targets in relation to the intended problem. Third, evaluations include contributions to the application of other methods of policy analysis, including problem formulation and recommendations. Finally, information about inadequate policy performance can contribute to the redistribution of policy issues. Evaluation can also contribute to the definition of a new policy alternative or a policy revision by indicating that the previously favored policy alternative needs to be removed and replaced with another one.

Conclusion

In the era of technology 4.0, it has implications for four phenomenons in the defense aspect that we need to look at together, namely the evolution of industry 4.0 to 6.0 in 2026, the formation of a cyber war theater with the concept of cyber defense, cyber threats evolving into military or conventional threats (5th generation war) and evolution towards the Internet of Things-based digital transformation era. We also need to identify, define and map patterns based on cyber threats, including physical or infrastructure threats in the form of viruses, malware, DDOS, Bruteforce, DSB phishing, and for non-physical threats including

information warfare hoaxes, framing to change mindsets. Therefore, cyber threats need to be anticipated by developing and learning about cybercrime and security.

There is a need for testing and demonstration. This is done because not all innovations are compatible with the conditions of society. In addition, to get an overview of the most useful alternated with the smallest risk or sacrifice. Then, the need to produce and publish information. in accordance with the development of technology, production, and publication media uses need to be adapted to the characteristics of the community.

With several policies issued by the government related to the empowerment of human resources, it is necessary to have an evaluation that has several main functions in policy analysis. First and most importantly, evaluation provides valid and reliable information regarding policy criteria, namely, how far needs, values , and opportunities have been achieved through public action. In this case, the evaluation reveals how far certain goals and targets have been achieved. Then, carry out empowerment/capacity strengthening, namely providing opportunities for the community to determine their own choices in relation to information accessibility, involvement in meeting needs and participation in the whole process of responsible development (public accountability), and strengthening local capacity.

References

Arief, R., & Widjayanto, J. (2021). Kebijakan pengelolaan wilayah pertahanan dalam konsep pertahanan pulau-pulau besar (Studi TNI-AL). *Jurnal Inovasi Penelitian*, 2(5), 1589–1604. https://doi.org/10.47492/jip.v2i5.942

Augina, A. (2020). Teknik pemeriksaan keabsahan data pada penelitian kualitatif di bidang kesehatan masyarakat. *Jurnal Ilmiah Kesehatan Masyarakat*, 12(33), 145–151. https://jikm.upnvj.ac.id/index.php/home/article/view/102/71

Beritasatu.com. (2021). *Ancaman Kejahatan Siber di Indonesia Terus Meningkat*. https://www.beritasatu.com/archive/763011/ancaman-kejahatan-siber-di-indonesia-terus-meningkat

Medcom.id. (2022). *Pengembangan IoT harus dibarengi dengan kesadaran keamanan siber. https://www.medcom.id/teknologi/news-teknologi/4baqvq0b-pengembangan-iot-harus-dibarengi-dengan-kesadaran-keamanan-siber*.

Okezone.com. (2021). *Perang Siber: Bahayanya Yang Perlu Kita Ketahui & Pahami*. Okezone News. https://news.okezone.com/read/2021/03/18/58/2379668/perang-siber-bahayanya-yang-perlu-kita-ketahui-pahami.

Rahmawati, I. (2017). Analisis Manajemen Risiko Ancaman Kejahatan Siber (Cyber Crime) Dalam Peningkatan Cyber Defense. *Jurnal Pertahanan & Bela Negara*, 7(2), 51–66. https://doi.org/10.33172/jpbh.v7i2.179

Republik Indonesia, K. P. (2014). *Pedoman Pertahanan Siber*, 5, 1–74.

Siti, A., Pradita, D. D., & Otto, S. T. (2014). Haluan negara sebagai arah dan sasaran pembangunan nasional. *Paper Knowledge . Toward a Media History of Documents*, 5(2), 40–51. https://bit.ly/3kbnkdW

Supriyatno, M. (2016). *Evolusi prinsip-prinsip perang*. CV. Makmur Cahaya Ilmu.