UNTAG Law Review (ULREV)
Volume 3, Issue 1, May 2019, PP 71-87
ISSN 2549-4910 (online) & ISSN 2579-5279 (print)
http://jurnal.untagsmg.ac.id/indeks.php/ulrev/indeks
www.fakhukum.untagsmg.ac.id

NATIONAL CYBERSECURITY POLICY IN THE U.S AND INDONESIA

Anang Setiyawan
Law Faculty
Universitas Wiraraja, Sumenep
Email : anang.setiyawan.sh@gmail.com

ABSTRACT : Cyber attacks are a dangerous threat to a country that has a high dependence on communication and information technology. Cyber attacks can be used systematically to disrupt and dysfunction an infrastructure and network so that it can cause not only physical damage but also fatalities. Cyber attacks are complex and multidomain; consequently, they require comprehensive and targeted policies. Indonesia in the early stages of developing cyber policies, therefore it can learn from America in developing policies in dealing with cyber threats.

Keywords : Indonesia, U.S, national, cyber, security, policy.

INTRODUCTION

The development and dominance of technology have evolved into increasingly sophisticated and complex threats carried out through information technology. The use and level of dependence on the use of communication and information technology in a country are directly proportional to the potential risks and threats to the national interests of a nation.

Modern threats in the form of cyber attacks can be carried out systematically, effectively, efficiently and anonymously to disturb, weaken, destroy, function a vital infrastructure belonging to a country that is very difficult to limit and predict its impact and size. This attack can not only cause physical damage but can result in injury or loss of life. Cyber threats are currently a concern for countries that have very high levels of use and dependence. Eugene Kapersky states that cyber attacks globally will become increasingly dangerous and increase every year and will be more systematic and more sophisticated than before.[1]

Indonesia has around 140 million internet users.[2] The higher level of use of information technology also increases the risk of cyber domain security in Indonesia. Indonesia has

1 http://rt.com/news/mini-flame-malware-kaspersky-519/ accessed june 2019
2 http://www.internetworldstats.com/asia.htm#id accessed june 2019

experienced millions of cyber attacks; even Indonesia has become one of the main targets of cyber attacks in Asia. In 2009 Indonesia was also one of the targets of the Stuxnet virus attack, which was considered by many cyber experts as the most sophisticated cyber weapon at this time because it was able to attack specific targets. [3] The cyber attacks if directed at Indonesia's vital infrastructure, will not only cause program damage, malfunction but also potentially cause fatalities. Likewise, with America, this country is the target of multiple cyber attacks compared to the number of cyber attacks on Indonesia, as a developed country, America has a high level of use and reliance on communication and information technology. Even America has a policy in securing this domain and forming special units related to cyber domain defense and security.

Indonesia in 2013 just started the stage of drafting policies in the field of cybersecurity and defense,[4] so it is very important to learn the lessons of how America assesses potential, takes benefits while being aware of threats to this domain seriously.

1. National Cybersecurity Policy in The U.S

a. Policy

According to America, Cyberspace is a vital sector of the global economy that can drive the economy and innovation. The development of this domain brings new challenges to national security, the economy and the global community. National security issues in the cyberspace have attracted the attention of this country since 1992 and have been a threat to national security since 1996.[5] President Obama stated that cyber threats had become one of the severe threats to the economy and national security; therefore, America must be prepared to face them.[6] The CSIS report states that the damage from cyber attack is real. In 2007, DoD, state, DHS, and Commerce, NASA, and the National Defense University suffered major intrusions by unknown foreign entities....our most dangerous opponents are the militaries and intelligence services of other nations. They are sophiscated, well resource and persistent.[7]

3 http://inet.detik.com/read/2012/01/20/105656/1820779/323/7-negara-asean-yang-paling-sering-kena-serangan-web/). Accessed june 2019
http://www.merdeka.com/teknologi/hacker-china-incar-militer-negara-negara-asia-indonesia-termasuk.html Accessed june 2019
http://tekno.kompas.com/read/2017/06/08/10050037/s erangan.cyber.makin.kencang.indones ia.sudah.sia p. Accessed june 2019
https://www.cert.or.id/media/files/survey_malware_report_nov.pdf Accessed june 2019

4 http://www.antaranews.com/berita/399394/cyber-army-antisipasi-cyber-warfare. Accessed june 2019

5 Schmitt, Michael N., Computer Network Attack and the Use of Force in International Law: Thoughts on a Normative Framework (1999). Columbia Journal of Transnational Law, Vol. 37, 1998-99.

6 Office of the Federal Register (U.S.). Public Papers of the Presidents of the United States: Barack Obama, 2009 (Book I). Government Printing Office, 2011

7 International Strategy for Cyberspace: Prosperity, Security, and Openness in a Networked World (Washington, DC: The White House, May 2011)

The Director of National Intelligence (DNI) stated that cyber threat is the number 1 strategic threat in the United States to replace the terrorist threat that first appeared in the 911 incident. U.S. The National Intelligence Officer for Science and Technology states that the increase in cyber threats is driven by a number of things such as increased connectivity between secure and insecure networks, creating new gaps for interference into the system in vital infrastructure and the complexity of computer networks that grow faster than the ability to understand and protect it.

Cyber attacks and operations against America are mostly carried out by State and non-state actors to penetrate and disrupt the networks and systems. Cyber attacks are used because their military power is not comparable if directly confronted. In addition, the cyber operations and attacks carried out against America often contain economic, industrial and military motives.[8] In February 2003, Bush issued a policy in the form of the National Strategy to Secure Cyberspace which highlighted three priorities, namely preventing attacks on America's vital infrastructure, reducing national vulnerability to cyber attacks and minimizing damage and recovery time from cyber attacks. The policy also identifies five critical national priorities, namely; Implement cybersecurity response systems, reduce threats and vulnerability cyberspace, increase awareness of cybersecurity training, secure the realm of cyberspace government and enhance cooperation in the field of cyberspace both nationally and internationally.

The five policy priorities aim to improve the security system of the government cyberspace and also the vital infrastructure of the private sector. Of the 5 priorities, it is further elaborated through several actions & initiatives, including; Encourage partnerships through public-private partnerships to respond to cyber incidents, Increase information sharing related to cyber attacks, threats and vulnerabilities, Give priority to research and development of cybersecurity, Develop training and educational programs in the field of cybersecurity, Strengthen cyber counterintelligence, Improve ability to do attacks and responds to attacks, builds international partnerships to protect information infrastructure, builds national and international monitoring networks to detect and prevent cyber attacks.[9] In May 2011, the United States drafted an international policy strategy for cyberspace which stated that it would strive internationally to encourage open, safe, reliable infrastructure to support international

Lior Tabansky. Basic Concept in Cyberwarfare.Military and Strategic Affairs.Vol 3. No 1. May 2011. Pg 75-92.
Walters, R., 2014. Cyber attacks on US companies in 2014. Heritage Foundation Issue Brief, 4289.
Langevin, J.R., McCaul, M.T., Charney, S. and Raduege, H., 2008. Securing cyberspace for the 44th presidency. Center for Strategic And International Studies Washington DC.

8 Charles G. Billo, Welton Chang. Cyber Warfare An Analysis Of The Means And Motivations Of Selected Nation States. The Institute for Security Technology Studies at Dartmouth College. 2004.

9 Chen, T.M., 2013. An assessment of the department of defense strategy for operating in cyberspace. Army War College Carlisle Barracks Pa Strategic Studies Institute.

trade and encourage freedom of expression and innovation. To realize this strategy, America combines several approaches, namely diplomacy, defense, development to improve welfare, the openness that is expected by all parties to benefit from this technology. The strategy steps are carried out by arranging seven priority policies, including;[10]

a) Economy: Promoting International Standards and Innovative, Open Markets.

b) Protecting Our Networks: Enhancing Security, Reliability, and Resiliency.

c) Law Enforcement: Extending Collaboration and the Rule of Law.

d) Military: Preparing for 21st Century Security Challenges.

e) Internet Governance: Promoting Effective and Inclusive Structures.

f) International Development: Building Capacity, Security, and Prosperity.

g) Internet Freedom: Supporting Fundamental Freedoms and Privacy

b. Structure

In America, the responsibility for cybersecurity is carried out by the Department of Homeland Security (DHS), the Department of Defense (DoD) and the Federal Bureau of Investigation (FBI). DHS is responsible for internal security. DHS has a National Cyber Security Division whose duty is to work with public, private and international agencies to secure cyberspace and American interests in cyberspace. This division has the National Cyber Response Coordination Group, which consists of 13 federal agencies and responsible for coordinating federal responses to cyber incidents that have a national impact.

DHS has the National Cybersecurity & Communications Integration Center (NCCIC) and the United States Computer Emergency Readiness Team (US-CERT) which is in charge of overseeing cybersecurity for 24 hours. NCCIC seeks to create a secure and resilient cyber infrastructure and communication that supports state, economic, safety and health by reducing the possibility and severity of the impact of cyber incidents that can disrupt the security and vital security of information technology and communication networks.[11] This organ is responsible for cyber operations and communications in the federal, state, intelligence, private sector and law enforcement.

US-CERT is leading efforts to improve the cybersecurity posture, coordinate information sharing and proactively manage cyber risk while protecting the constitutional rights of the American people.[12]

10 Obama, B., 2011. International Strategy for Cyberspace: Prosperity, Security, and Openness in a Networked World (Washington, DC: White House, May 2011), 14. *Issued in*, pp.11-14

11 http://www.dhs.gov/national-cybersecurity-communications-integration-center accessed June 2019

12 https://www.us-cert.gov/about-us accessed June 2019

This organ is responsible for analyzing and reducing cyber threats, cyber vulnerability, disseminating information about cyber threats and coordinating response actions for cyber incidents. US-CERT creates programs that encourage and facilitate information sharing and cybersecurity-related collaborations on governments, industries, academics and international entities, such as the US-CERT Portal, Government Forum of Incident Response Security Teams (GFIRST), US-CERT Einstein Program.[13] Since the 2006 DHS has held four cyber attack simulation exercises, this simulation aims to look at the cyber forces readiness in the public sector and the private sector, including aimed at computer systems involved in operating vital infrastructure owned, especially in the fields of information technology, energy, communications, emergency management, military and transportation.[14]

The second responsibility for cybersecurity in America is the Federal Bureau of Investigation (FBI). The FBI is a federal body that acts as a domestic intelligence agency as well as federal law enforcement officers. This body is responsible for defending the state from all forms of crime, acts of terrorism, foreign intelligence, law enforcement, and protecting civil rights. The FBI focuses on dealing with threats to the foundations of the American people or involving vast and complex threats to state governments that are difficult to overcome on their own.

In order to deal with threats as well as cyber-based attacks and high-tech crime, the FBI formed the FBI Cyber Division which led national efforts to investigate and prosecute crimes in the cyber world including cyber terrorism, espionage, computer intrusion and fraud in cyberspace. This mission is carried out through the National Cyber Investigative Joint Task Force (NCIJTF) mandated by the US President to become the central point for all government agencies to coordinate, integrate and share all information related to investigating cyber threats. The FBI is responsible for developing and supporting this joint task force consisting of 19 intelligence and law enforcement agencies to work together to identify the leading actors and patterns. The aim is to predict, prevent and pursue cyber attackers.[15] Every year the FBI through NCIJTF pioneered Clean State operations. This is a joint operation between the American government, international partners, internet service providers, the financial sector, and other related sectors to eliminate botnet that endangers America while pursuing its makers[16] The third agency responsible for cybersecurity is the Department of Defense. This department is responsible for protecting the homeland and American interests from various types of attacks, including those carried out through cyberspace. This department has three

13 https://www.us-cert.gov/sites/default/files/publications/infosheet_US-CERT_v2.pdf accesed june 2019
14 http://searchsecurity.techtarget.com/definition/Cyber-Storm;
http://www.dhs.gov/cyber-storm-securing-cyber-space accessed June 2019
15 https://www.fbi.gov/about-us/investigate/cyber/ncijtf accessed June 2019
16 http://www.ledger-dispatch.com/news/the-battle-against-botnetsall-americans-share-cyber-security-risk accessed June 2019
http://www.wpcug.org/Downloads/National%20Cyber%20Investigative%20Joint%20Task%20Force.pdf accessed June 2019

main cyber missions, namely:

1) Defend DoD networks, systems, and information;

2) Defend the homeland and national interests gainst cyberattacks of significant consequence;

2) Provide cyber support to military operational and contingency plans.

The responsibility of this field is carried out by the United States Cyber Command (USCYBERCOM). This command plans, coordinates, integrates, synchronizes and takes action to operate directly and maintain the information network of the defense department and is ready to carry out military spectrum operations in cyberspace to enable action in all domains and ensure the freedom of America and its allies in activities in cyberspace and ward off common enemies. The main task of this command focuses on maintaining the defense ministry's information network, providing support to commanders to be able to carry out their missions that are spread throughout the world and strengthen the nation's ability to survive and respond to cyber attacks.

USCYBERCOM is under the United States Strategic Command. USCYBERCOM consists of cyber units developed from each component of the American armed forces, including Army Cyber Command, Cyber Fleet Command, Cyber Air Force Command and Marine Forces Cyber Command. It also includes the Coast Guard Cyber Command which, although under the Department of Homeland Security, has direct support to USCYBERCOM.

In 2011, the US DoD issued the DoD Strategy for Operating in Cyberspace which aimed to be able to take advantage of opportunities while managing risks that could have an impact on the national economic, defense and security systems.[17] In 2015 the US DoD re-drafted the DoD Cyber □□Strategy. This cyber strategy is a reflection of the National Cybersecurity Strategy 2015 and the 2014 Quadrennial Defense Review. This DoD Cyber Strategy focuses on building cybersecurity and cyber capabilities effective operation to maintain and maintain networks, systems and information of the ministry of defense, safeguard the State from cyber attacks that have a significant impact and simultaneously support operational and backup plans. The DoD sets five strategic objectives for the implementation of its cyberspace, namely:

1) Build and maintain ready forces and capabilities to conduct cyberspace operations;

2) Defend the DoD information network, secure DoD data, and mitigate risks to DoD missions;

3) Be prepared to defend the U.S. homeland and U.S. vital interests from disruptive or

17 Department of Defence Strategy for Operating In Cyberspace.US Department of Defense. July 2011

destructive cyberattacks of significant consequence;

4) Build and maintain viable cyber options and plan to use those options to control conflict escalation and to shape the conflict environment at all stages;

5) Build and maintain robust international alliances and partnerships to deter shared threats and increase international security and stability

National Cybersecurity Policy in Indonesia

1. Policy

The Indonesian government is currently at the stage of policy formulation, resilience strategy and information system security in the context of facing cyber threats. Based on the analysis of the development of the environment and the strategic context of the estimates of threats, challenges and risks of the implementation of national defense, the Ministry of Defense stipulates that national defense policies, both military defense and non-military defense will later have cyberdefense capabilities.[18] The government sees that even though conventional weapons technology innovations are still developing, the advances in science and technology today also greatly influence the shape and pattern of war in the future, one of which is creating a network of information and communication technology-based wars. This war base has significantly changed strategic security, especially with the use of communication and information networks throughout the sector, especially in the defense sector.

Indonesia's efforts in realizing and developing the capabilities of this field will face several challenges, such as inadequate cyber law policies and arrangements, coordination and cooperation in very weak government and private sectors, governance and national cybersecurity organizations that have not yet synergized, there is no standard and protection mechanisms for vital infrastructure, vital information infrastructure that has not been integrated and the limited quality and quantity of human resources, especially in the cybersecurity field.[19] The fundamental legal problem related to cyber attacks in Indonesia is the use of the same perspective in looking at the issue of cyber attacks. The cyber attack is still considered as cybercrime whose handling is under the domain of the Indonesian National Police. This happened because of the limited regulation of legal issues in terms of violations, crimes and cyber security in Indonesia. Some of the Indonesian legal rules relating to cyber domains and threats through cyber domains include:

2. The Criminal Code (KUHP)

The Criminal Code is not specifically designed to deal with crimes committed in cyberspace,

18 Buku Putih Pertahanan Indonesia 2014, Kementerian Pertahanan Republik Indonesia.

19 Zainal A. Hasibuan, Indonesia National Cyber Security Strategy: Security and Sovereignty in Indonesia Cyberspace. Dewan Teknologi Informasi dan komunikasi Nasional. 2013

but several articles in the Criminal Code can be used to ensnare certain types of crimes committed in this domain using extensive interpretations. Some criminal cases in Indonesia that use this interpretation such as the case of electricity theft that extends the interpretation of the word "goods" in article 362 of the Criminal Code not only to "tangible goods" but also "intangible goods", extension of the word goods also used by judge bismar siregar when adjudicating cases of obscene acts, according to him "goods" in article 378 can also be interpreted as "genitals".[20] This extensive interpretation can be used against several articles in the Criminal Code related to crimes committed in the cyber domain, including article 282 which can be used to ensnare pornography through internet media, article 311 which can be used to ensnare cases of defamation through internet media Article 362 and 378 can be used for cases of theft of credit card numbers and Article 303 which can be used to ensnare online gambling case.

3. Law No. 11 of 2008 concerning Information and Electronic Transactions

This Law regulates cybercrime, e-commerce, Haki protection, consumer protection and unfair competition. Some actions that are prohibited related to information technology crimes include:

a. Article 30 concerning the prohibition of illegally accessing, breaking, breaking down computer systems or electronic systems;

b. Article 31 concerning the prohibition of interception of electronic and or information systems;

c. Article 32 concerning the prohibition of damaging, removing, transferring, hiding electronic information and or electronic documents;

d. Article 33 concerning the prohibition of illegal actions, which results in the disruption of the electronic system.

e. Article 34 concerning the prohibition on producing, selling, holding for use, importing, providing computer software for the purpose of decency or sexual exploitation of children, tapping, damaging and eliminating electronic information and or electronic documents;

f. Article 35 concerning the prohibition of making changes, creating, damaging, removing and manipulating electronic information data or electronic documents.

20 Putusan Bonda yang 'Mengayun' Bismar. http://www.hukumonline.com/berita/baca/lt559fba87c3065/putusan-ibonda-i-yang-mengayun-bismar accessed June 2019
Christianto, H., 2010. Batasan dan Perkembangan Penafsiran Ekstensif dalam Hukum Pidana. Pamator Journal, 3(2), pp.101-113.
Black, H.C., 1911. Handbook on the Construction and Interpretation of the Laws (No. 5). West Publishing Company.

4. Law No. 36 of 1999 concerning Telecommunications;

Provisions related to information technology crime in this Act are as follows:

a. Article 21 concerning the prohibition of telecommunications operators to carry out telecommunications business activities that are contrary to the public interest, security, morality, and public order;

b. Article 50 regulates acts without rights, illegitimate or manipulating access to special telecommunications networks;

c. Article 55 governs actions that can cause electromagnetic physical disturbances to telecommunications operators;

d. Article 56 prohibits conducting eavesdropping on information channelled through telecommunications networks.

5. Presidential Regulation No. 97 of 2015 concerning the National Defense Policy 2015-2019

This Presidential Regulation is a reference for planning, managing and overseeing the national defense system in order to handle a variety of complex and multidimensional threats that originate from the dynamics of the global, regional and national strategic environment. These threats include cyber threats, espionage threats and even the possibility of open conflict or conventional war that needs to be watched by the Indonesian state. National defense policy in the face of cyber threats is carried out through the development of technology and information and communication systems in the defense sector to improve the quality of the national defense system in stages, continuously and integrated. Technology development is carried out by research and development as well as integrated technology transfer by utilizing national satellite technology involving research institutions both government, universities and industries related to the national defense sector.

The empowering the national defense policy in increasing awareness of the threats that arise is carried out by maintaining and developing the strength and potential of defense in an integrated and directed manner and involving all citizens, utilizing resources, national facilities and infrastructure. The policy of empowering national defense is divided into military defense empowerment, non-military defense empowerment and empowerment of defense potential. Military defense empowerment policy is an effort to deal with threats in the form of military operations for war and military operations other than war. Empowerment policy and the policy of mobilizing the state defense force rests on the TNI as the main defense element supported by reserve components and supporting components. This policy is carried out by stabilizing strategic policies, maintaining and enhancing TNI's capabilities,

proportionally and holding TNI forces in a balanced manner.

Non-military empowerment policy is an effort to increase capacity, synergy and role/institution as the main elements in the context of facing non-military threats. The policy of deploying defense forces in the face of non-military threats places the TNI as a supporting element of ministries/institutions and local governments as the main element in dealing with non-military threats that have ideological, political, economic, socio-cultural, public safety, technology and legislation dimensions.

Defense potential empowerment policies are carried out by synergizing the functions of ministries/institutions and local governments to foster human resources, natural resources, artificial resources, national infrastructure, values, technology and synchronization of defense area arrangements with national, regional spatial plans that are prepared to become strengths National Defense. The deployment of national defense forces in the face of this threat is carried out with a pattern of military defense along with non-military defense forces that are informed as supporting components in accordance with the nature and level of escalation of threats that arise.

This policy is categorized cyberthreat as a non-military threat even though this threat in many developed countries is considered a dangerous strategic threat to the security, defense and national interests of their country. These countries have even designated cyber domains as the domain of a new war after the land, sea, air and space domains and made cyber capabilities as part of the country's military strategy. They consider that maintaining cyber domains is just as important as securing a country's borders. Therefore, cyber threats in Indonesia today deserve to be called a military threat or at least as a hybrid threat because of the difficulty of separating the linkages between emerging threats and the multidimensional nature of threats.[21] The government also needs to establish that cyber domains are the domain of the new Indonesian war so that cyberwarfare threats are no longer underestimated and the development of defensive and offensive cyber capabilities becomes a more comprehensive part of the national defense strategy.

6. The Minister of Defense Decree No. KEP / 435 / M / V / 2016 concerning 2017 National Defense Policy

The National Defense Policy is carried out with a universal defense system through the development and development of resources, national infrastructure and the entire territory of the Republic of Indonesia as a unit of defense in the face of threats. This defense policy divides threats into two types, namely military threats and non-military threats. Military threats are

21 Anton Dengg, Michael Schurian (Eds.), 2016. On the Concept of Hybrid Threats. . In: DENGG, Anton, ed., Michael SCHURIAN, ed.. Networked Insecurity : Hybrid Threats in the 21st Century. Wien:Landesverteidigungsakademie, pp. 25-80.

faced with the military defense system by placing the Indonesian Armed Forces as the main component supported by reserve components and supporting components. Non-military threats are faced with the non-military defense system by placing government institutions outside the defense sector as the main element in accordance with the form and nature of the threats faced with the support of other elements of the nation's strength.

This policy is prepared by considering the dynamics of the strategic environment that pose threats and impacts on national defense, such as American policies in the Asia Pacific region, China's economic and military development, terrorism threats to the development of information technology that raises cyberthreats. These dynamics bring changes to the dimensions of threats, both real and unreal threats such as the threat of open conflict (conventional war), which is less likely to occur but cannot be ruled out. This country's defense policy has a vision of developing national defense "the realization of a sovereign, independent Indonesia and a personality based on mutual cooperation". This vision is realized through seven national defense development missions, including;

a. Realizing national security that can maintain regional sovereignty, sustain economic independence by securing maritime resources, and reflect the personality of Indonesia as an archipelago.

b. Realizing an advanced, balanced and democratic society based on the rule of law.

c. Realizing free-active foreign policy and strengthening identity as a maritime country.

d. Realizing the quality of life of Indonesian people who are high, advanced and prosperous.

e. Realizing a competitive nation.

f. Realizing Indonesia to be a maritime country that is independent, advanced, strong and based on national interests.

g. Creating a community that has a personality in culture

One of the main points of national defense policy is the development of defense technology, information and communication. The development of technology and information and communication is carried out, among others, by integrating national defense information systems using satellites, optimizing cyber defense in accordance with cyber defense guidelines, encouraging relevant ministries and institutions in mastering defense technology in producing defense equipment, encouraging relevant ministries and agencies in developing resources human power and development of information and communication technology infrastructure.

The Cyber Defense Guidelines stipulated in Defense Minister Regulation No. 82 of 2014

concerning Cyber Defense Guidelines is a primary reference for the Ministry of Defense and the TNI in the context of implementing cyber defense. Cyber defense guidelines are defined as the embodiment of determination, principle and will to carry out cyberdefense on information, control and communication systems in the defense sector. This guideline embodies a framework for implementing cyber defense that must be understood and guided by each task and function. Cyber defense is a non-military defense force that makes ministries outside the defense sector, namely the Ministry of Communication and Information as of the main element and the ministry of defense as one of the supporting elements.

This policy gives attention to sectors that manage critical infrastructure in the fields of defense, security, energy, transportation, the financial system and various other public services. Where disruption to the sector can affect the economy and decrease the level of trust in the government and public order. In determining the vital infrastructure sector, the government needs to define, describe and classify each of the vital infrastructure sectors while at the same time pointing to the leading sector as the cybersecurity coordinator for each sector. In addition, the government needs to harmonize the policy of determining this vital infrastructure with a policy on vital national objects stipulated in Presidential Decree No. 63 of 2004.

Defense development preparation within the Ministry of Defense and the TNI requires an understanding of the principles, objectives, tasks, roles and functions of cyber defense that will be carried out. These cyber defense guideline points are ten cyber defense principles, namely:

a. Structured and integrated information security model and adopting various standards and guidance on information security established by authorized institutions;

b. Confidentiality, integrity and availability of cyber defense must be ensured from the design stage as one of the basic principles of information security;

c. Cyber defense contains policy, institutions, technology and supporting infrastructure and human resources;

d. The implementation must be carried out by HR who have competence, high integrity and are protected;

e. Performed effectively and efficiently in the form of physical security and logical security in an integrated manner by utilizing as much as possible the open technology and Indonesian products in the framework of independence and sovereignty;

f. Determination of security zones based on the classification of involved human resources such as administrators, users and other types;

g. Refers to governance principles that guarantee the realization of supervision inherent in cyber defense;

h. Ensure that the implementation of the cyber system is safe and resistant to cyber attacks;

i. Develop conditions that are more favourable for offensive actions;

j. Avoid losses to unwanted computer systems.

Structure

1. Ministry of Defense of Republic of Indonesia

a. Directorate General of Defense Potential of the Ministry of Defense

In order to support the implementation of national defense, directed and continuing manner, the Indonesian Ministry of Defense considers that it is necessary to plan, monitor and evaluate the use of information technology and communication measurably for the national defense information system and cyber defense within the Ministry of Defense. The Ministry of Defense views technology as one of the aspects of military defense that needs to be utilized to support the success of the main tasks in the field of national defense.

The Minister of Defense issued a Decree of the Minister of Defense No. 387 year 2015 appointed the Director General of Defense Potential as the executor of defense duties and functions under and directly responsible to the minister of defense. The Director-General implements, formulates, monitors and evaluates the use of ICT in the National Defense Information System and Cyber Defense Information System and provides advice and input as the basis for the Minister of Defense to formulate national defense information and communication technology policies.

b. Defense Strategic Installation Agency

The structure of the defense ministry changed on May 18, 2015, through Presidential Regulation No. 58 of 2015 concerning the Ministry of Defense. In this regulation, there are several new bodies in the structure of the Ministry of Defense, including the Defense Facility, Research and Development Agency, the Education and Training Agency and the Defense Strategic Installation Agency. Related to dealing with cyber issues that were previously under the Directorate General of Pothan according to the Perpres, they will be explicitly handled by the Defense Strategic Installation Agency.

c. TNI Headquarter (Pusinfolahta)

TNI Headquarters has organs related to the cyber field, namely the Center for Information and Data Processing of the TNI (Pusinfolahta TNI). This organ is the central implementing body at the level of the TNI Headquarters, which is directly under the TNI Commander. Pusinfolahta TNI has to prepare information and carry out data processing on the use of TNI forces in administration and operations and to carry out information technology support and

information system security to support the TNI's main tasks.

2. Coordinating Ministry for Political, Legal, and Security Affair (National Cyber Security Information and Resilience Desk)

The government is aware of the adverse effects of potential threats, disruptions, obstacles and challenges to Cyber resilience and national information security is also considered a threat to national interests towards national assets. The government realizes that handling various problems, threats, disruptions, challenges and additions to cybersecurity and information security it cannot only be handed over to government / non-government / sectoral institutions but must be coordinated and integrated on a national scale. Considering this, the government through Kemenkopolhukkam took initiation and strategic steps by establishing a desk organization under Coordinating Ministry for Political, Legal, and Security Affair through the Ministry Decree Number 24 of 2014 concerning National Cyber Security and Information Resilience Desk which was amended by Ministerial Decree No. 5 Year 2015.

3. Ministry of Communication and Information of the Republic of Indonesia (Information Security Directorate)

The Directorate of Information Security formulates and implements policies, drafting norms, standards, procedures and criteria, as well as providing technical guidance and evaluation in the information security field.

4. National Cyber And Crypto Agency

Indonesian Government established the National Cyber And Crypto Agency through Presidential Regulation No. 53 of 2017. The establishment of this body is a government effort to safeguard Indonesian cybersecurity as one of the areas of Government that needs to be encouraged and strengthened to increase national economic growth and realize national security. It is a non-ministerial government institution that is under and responsible to the president through ministers who organize coordination, synchronization and control of the administration of Government in the fields of politics, law and security.

This agency is a combination of the State Code Institution and the Information Security Directorate of the Ministry of Communication and Information. This institution carries out duties and functions in the field of coding as well as implementing all tasks and functions in the field of information security, securing the utilization of internet protocol-based telecommunications networks, and security of telecommunications networks and infrastructure. This agency is implementing cybersecurity effectively and efficiently by utilizing, developing and consolidating all elements related to Indonesian cybersecurity.

Conclusion

Strengthening policies in the form of laws are needed to clarify, reinforce cyber domains as part of Indonesia's sovereignty domain and provide a legal basis that can reach complex, dynamic and multidomain levels of cyber threats. The law must be able to collaborate on authority, strength and all relevant stakeholders considering the handling of the nature of cyber threats that are very complex, dynamic and multidomain towards security, defense and national interests of Indonesia. In addition, the government must immediately harmonize the laws and regulations related to defense, security and national interests, such as provisions concerning the country's infrastructure / vital objects.

References:

Anton Dengg, Michael Schurian (Eds.), 2016. On the Concept of Hybrid Threats. . In: DENGG, Anton, ed., Michael SCHURIAN, ed.. Networked Insecurity : Hybrid Threats in the 21st Century. Wien:Landesverteidigungsakademie, pp. 25-80.

Buku Putih Pertahanan Indonesia 2014, Kementerian Pertahanan Republik Indonesia.

Black, H.C., 1911. Handbook on the Construction and Interpretation of the Laws (No. 5). West Publishing Company.

Christianto, H., 2010. Batasan dan Perkembangan Penafsiran Ekstensif dalam Hukum Pidana. Pamator Journal, 3(2), pp.101-113.

Carter, A., 2015. The Department of Defense cyber strategy. The US Department of Defense, Washington, DC.

Charles G. Billo, Welton Chang. Cyber Warfare An Analysis Of The Means And Motivations Of Selected Nation States. The Institute for Security Technology Studies at Dartmouth College. 2004.

Chen, T.M., 2013. An assessment of the department of defense strategy for operating in cyberspace. Army War College Carlisle Barracks Pa Strategic Studies Institute.

Department of Defence Strategy for Operating In Cyberspace.US Department of Defense. July 2011

International Strategy for Cyberspace: Prosperity, Security, and Openness in a Networked World (Washington, DC: The White House, May 2011)

Langevin, J.R., McCaul, M.T., Charney, S. and Raduege, H., 2008. Securing cyberspace for the 44th presidency. Center for Strategic And International Studies Washington DC.

Lior Tabansky. Basic Concept in Cyberwarfare.Military and Strategic Affairs.Vol 3. No 1. May 2011. Pg 75-92.

Office of the Federal Register (U.S.). Public Papers of the Presidents of the United States: Barack Obama, 2009 (Book I). Government Printing Office, 2011

Obama, B., 2011. International Strategy for Cyberspace: Prosperity, Security, and Openness in a Networked World (Washington, DC: White House, May 2011), 14. *Issued in*, pp.11-14

Schmitt, Michael N., Computer Network Attack and the Use of Force in International Law: Thoughts on a Normative Framework (1999). Columbia Journal of Transnational Law, Vol. 37, 1998-99.

Walters, R., 2014. Cyber attacks on US companies in 2014. Heritage Foundation Issue Brief, 4289.

Zainal A. Hasibuan, Indonesia National Cyber Security Strategy: Security and Sovereignty in Indonesia Cyberspace. Dewan Teknologi Informasi dan komunikasi Nasional. 2013

Internet:

Http://www.dhs.gov/national-cybersecurity-communications-integration-center accessed June 2019

Https://www.us-cert.gov/about-us accessed June 2019

Http://www.us-cert.gov/sites/default/files/publications/infosheet_US-CERT_v2.pdf accessed June 2019

Http://searchsecurity.techtarget.com/definition/Cyber-Storm accessed June 2019

Http://www.dhs.gov/cyber-storm-securing-cyber-space accessed June 2019

Https://www.fbi.gov/about-us/investigate/cyber/ncijtf accessed June 2019

Http://www.ledger-dispatch.com/news/the-battle-against-botnetsall-americans-share-cyber-security-risk accessed June 2019

Http://www.wpcug.org/Downloads/National%20Cyber%20Investigative%20Joint%20Task%20Force.pdf. accessed June 2019

Http://www.hukumonline.com/berita/baca/lt559fba87c3065/putusan-ibonda-i-yang-mengayun-bismar accessed June 2019

Http://rt.com/news/mini-flame-malware-kaspersky-519/ accessed june 2019

Http://www.internetworldstats.com/asia.htm#id accessed june 2019

Http://inet.detik.com/read/2012/01/20/105656/1820779/323/7-negara-asean-yang-paling-sering-kena-serangan-web/). Accessed june 2019

Http://www.merdeka.com/teknologi/hacker-china-incar-militer-negara-negara-asia-indonesia-termasuk.html Accessed june 2019

Http://tekno.kompas.com/read/2017/06/08/10050037/serangan.cyber.makin.kencang.indonesia.sudah.siap. Accessed june 2019

Https://www.cert.or.id/media/files/survey_malware_report_nov.pdf Accessed june 2019

Http://www.antaranews.com/berita/399394/cyber-army-antisipasi-cyber-warfare. Accessed june 2019