THE ANALYSIS OF CYBER CRIME THREAT RISK MANAGEMENT TO INCREASE CYBER DEFENSE

ANALISIS MANAJEMEN RISIKO ANCAMAN KEJAHATAN SIBER (CYBER CRIME) *DALAM PENINGKATAN* CYBER DEFENSE

Ineu Rahmawati[1]
Prodi Manajemen Pertahanan, Universitas Pertahanan Indonesia
(rahmawati.ineu@gmail.com)

Abstrak – Kemajuan teknologi dan informasi menimbulkan ancaman baru di ruang siber yakni kejahatan siber. Kejahatan siber merupakan kejahatan yang lahir sebagai suatu dampak negatif dari perkembangan aplikasi pada internet. Dalam menganalisis dampak kejahatan siber terhadap pertahanan sebuah negara, diperlukan identifikasi manajemen risiko yang dapat mengetahui seberapa besar probabilitas dan konsekuensi yang ditimbulkan dari kejahatan siber. Risiko yang dihadapi dalam mengatasi ancaman kejahatan siber tidak kalah dengan perang konvensional. Hal ini menyebabkan risiko yang diidentifikasi harus bisa menghasilkan strategi pertahanan negara dalam menghadapi ancaman kejahatan siber.

Kata kunci: kejahatan siber, manajemen risiko, strategi, pertahanan negara

Abstract – *Increasing technology and information caused new threat in cyberspace called cyber crime. Cyber crime is a crime that emerge as a negative impact of applications development on the internet. In analyzing the impact of cyber crime towards a state defense, it is necessary to identify risk management that can know how big the probability and consequences caused by cyber crime. The risks faced in overcoming the threat of cyber crime is not inferior to conventional wars. This causes the identified risks has to be able to produce a state defense strategy in the face of cyber crime threat.*

Keywords: *cyber crime, risk management, strategy, state defense*

[1] Penulis merupakan alumni Manajemen Pertahanan Cohort 7, Universitas Pertahanan.

Preface

The development of globalization and information technology has brought great changes in human life. Information Technology makes the communication between people and between nations more easily and quickly without being influenced by space and time. Globalization is a process of changing the dynamics of the global environment as a continuation of a pre-existing situation characterized by technological and information advancement features, creating interdependence, borderless. The impact of technological developments and information changes the course of war which is happening today.

The era of globalization encourages some countries no longer use traditional and conventional warfare. As a result, the power of the state is no longer seen in the power of weaponry, but also on the cultural, economic, political and technological aspects. This makes the competition and war increasingly invisible. Wars and conflicts that occur in a country are not only dominated by military forces, but nirmiliter forces are also carried out by non-state actors.

A form of war that no longer uses traditional warfare poses a new threat in the cyber space. Threats that evolve into cyber attacks are not just concepts. The vulnerability of information exchange in the cyberspace is driven by a country to build a security system that can overcome the threat. The events of Estonia in 2007 and Georgia in 2008 are examples of cyber crime attacks with the use of Distributed Denial of Service (DdoS), thus crippling state activity as many of the critical sectors are attacked. The attack which is quite worrying is the attack towards Stuxnet. Stuxnet is a very sophisticated example of malware that successfully paralyzes one-fifth of the nuclear enrichment control system of Iran's nuclear power plant.[2]

The threat of cyberspace is dominated by non-state actors such as hacker individuals, hacker groups, hacker activities, non-government organizations (NGOs), terrorism, organized criminal groups and the private sector (Such as internet companies and carries, security companies) can also threaten national

[2] Michael B. Kelly, "The Stuxnet Attack on Iran's Nuclear Plant Was Far More Dangerous than Previously Thought", dalam http://www.businessinsidercim/stuxnet-was-far-more-dangerous-than-prevoius-thought-2013-11?IR=T&, diakses pada 8 Juni 2017.

defense and sovereignty.[3] The target of cybercrime threats has occurred in the case of private interception of Indonesian President and some of Australia's top officials based on a document leaked by Edward Snowden, a former National Security Agency (NSA) contractor from America.[4] In addition, one of the official sites of the Ministry of Defense of the Republic of Indonesia (Defense Ministry) was burglarized by a hacker, the website of the Directorate General of Defense Potential (Ditjen Pothan) who experienced a page change called defacing. The site was broken into by CVT (Cyber Vampire Team) by writing the website page "Oops Myanmar Hacker was here". Then write the sentence in English, that is:

> *Hello Indonesia Government, you should be proud with uneducated Indo script kiddies. Coz they believe (defacing/Ddosing) to other country website is the best solution for them. If you would sympathize the white programmers/developers of your country and how they are feeling. You can catch such script kiddies. Coz CVT are ready to provide those kiddies information.*[5]

The global threat, technological advances and information are not only aimed at attacking government and military agencies. But it can also threaten all aspects of human life, such as economy, politics, culture, and security of a country. Recently, cyber-attacks also occurred on the government's telecom industry website. The threat of cyber crime can occur because of the interests of various individuals or groups. This threat in the aspect of public life raises various physical threats either real or not real by using computer codes (software) to make the theft of information and data that can threaten a country.

Increasing the threat of cyber crime committed by either state or non state actors which has an impact on the occurrence of cyber warfare or cyber violence. The state's dependence on the communications network brings its own challenges and threats. Therefore, risk management analysis is needed in the face of cyber crime attacks with the aim

[3] Pearlman, W. and Cunningham, K.G., “Non State Actors, Fragmentation, and Conflict Processes”, *Journal of Conflict Resolution*, Vol.2 No. 56, 2012.

[4] “Snowden: Ponsel SBY Disadap Australia”, dalam http://news.liputan6.com/read/748895/snowden-ponsel-sby-disadap-australia, diakses pada 8 Juni 2017.

[5] “Situs Dirjen Kementerian Pertahanan RI Di-Hack”, dalam https://news.detik.com/berita/2243078/situs-dirjen-kementerian-pertahanan-ri-di-hack?9911012, diakses pada 12 Mei 2017.

of maintaining the defense and sovereignty of the Unitary Republic of Indonesia in realizing national goals. Risk management can be defined as a set of procedures and methodologies used to identify, measure, monitor and control the risks arising from the activities of the organization.[6] Risk management made in the field of information and communications related to the lives of many citizens or scretive in nature, is done to reduce the level of vulnerability of misuse of information and data in the cyberspace.

Risks that occur in facing the threat of cyber crime comes from within and outside the country by utilizing social conditions, politics, culture, ideology, and technological developments. Many ways are done by various parties to obtain information contained in the State Defense Information System (Sisfohanneg). Some attacks have even been carried out, such as hacking action by defacing the directorate general's site of defense potential of the ministry of defense. Leaking information related to national defense contained within Sisfohanneg may threaten the sovereignty of the state, especially the sovereignty of information. The concept of risk management in defense is an important element for analyzing how much threat impacts the country's defense.

In the context of facing the threat of cyber crime, it can not be solved by using only the strength of the weapon. But it requires the integration of all national forces under the command and control (Kodal) of the Ministry of Defense (Kemhan).[7] Risks faced in overcoming the threat of cyber crime (cyber crime) is not inferior to conventional wars. The use of cyber technology is widespread because it can cover various aspects of public and state life, including ideological, political, economic, socio-cultural, and security fields. Cyber crime is increasingly used by certain parties either individually or in groups or countries with a specific purpose to be able to weaken the opponent. This condition needs to be watched because it is not impossible to cripple or destroy a state by tech war or through cyber.[8]

[6] Rini Lestari, " Manajemen Risiko Terhadap Kinerja Organisasi", *Jurnal Riset Akuntansi dan Bisnis*, Vol.13, No.2, 2013.

[7] *Ibid.*

[8] Sugeng Brantas, "Defence Cyber dalam Konteks Pandangan Bangsa Indonesia tentang Perang dan Damai", Jurnal Pertahanan, Vol.2, No.2, 2014, hlm.55.

As a sovereign and civilized nation certainly needs an effort to defend the integrity of a country by building a strong state defense in order to achieve the goals of national interest. The above conditions illustrate how important the identification of risk management in the face of the threat of cyber crime in the management of state defense.

Cyber Crime Definition

Technology is an activity born by humans by planning and creating material objects of practical value, such as cars, planes, television is the result of technology development. Judging from the function and importance of technology, all societies and government institutions are very dependent on technology both for positive and negative purposes. The word cyber and technology is described from the origin of the word technique, from the Greek word Technikos which means artistry or skill in and logos is the limo or the main principles on cyber (software). Increased utilization of cyberspace throughout the lifetime of society in the current era of globalization in parallel, will connect to the utilization of a network of internet technology on a particular object or sector in accordance with the purpose of it's existance.

Cyber space is a space where communities connect to each other using a network (eg intenet) to perform various daily activities.[9] *Cyber is defined as another term, ie cyberspace taken from cybermetics data. At first the term cyberspace is not intended to describe the interactions that occur through computer networks. John Perry Barlow in 1990 applied the term cyber (cyber) that is connected to the Internet network. In its development, cyber can bring positive and negative impact that can lead to a crime in the development of cyber world. Crime born as a negative impact of the development of applications on the internet is called cyber crime (cyber crime) which includes all types of crime and its modus operandi is done as a negative impact of internet applications*.

In the opinion of McDonnell and Sayers, there are three types of cyber threats,[10] which are:

a. *Hardware threat*

This threat is a threat caused by the installation of certain devices that serve to perform certain activities within a system, so the equipment is a

[9] Kementerian Pertahanan Indonesia, *Pedoman Pertahanan Siber*, (Jakarta: Kemhan RI, 2014), hlm.5.

[10] *Ibid.*

disruption to network systems and other hardware.

b. *Software threat*

This threat is a threat caused by the entry of certain software that serves to conduct activities of theft, destruction, and manipulation of information.

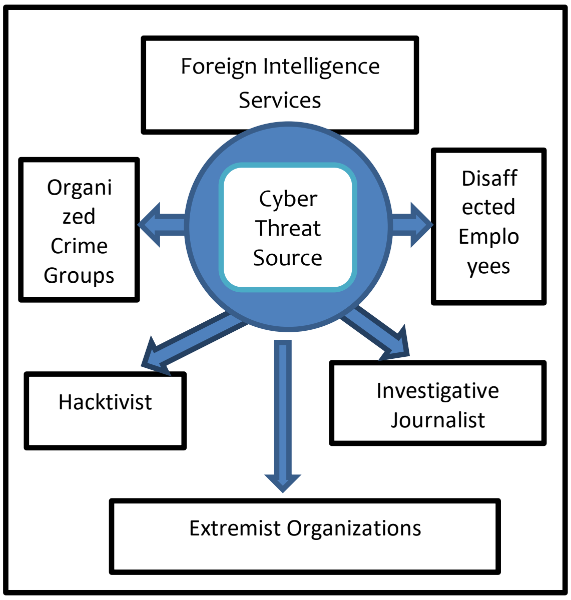
c. *Data/information threat*

This threat is a threat caused by the dissemination of certain data / information that is intended for a particular interest.

In the National Cyber Security Strategic Assessment, defining the threat of cyber crime as any condition and situation as well as the ability to be judged capable of undertaking acts or harassment or attack capable of damaging or detrimental, thus threatening the confidentiality, integrity, And availability of systems and information.[11] Cyber threats can occur because the interests of certain individuals or groups in the life aspects of society can pose a variety of physical threats, both real and unreal, using computer codes to carry out information theft, system destruction), information manipulation (information corruption) or hardware to interfere with the system (network instruction) or dissemination of data and certain information to conduct propaganda activities.[12]

Sources of cyber threats can come from various sources, such as foreign intelligence services, disaffected employees, investigative journalists, extremist organizations, hacktivist activities, and criminal groups organized (organized crime groups).

Fig 1. Sources of Cyber Threats



Source: Dr. Federick Wamala, CISSP International Telecommunication Unit (ITU) National Cybersecurity Strategy Guide, 2012

Cyber crime risks have the potential to lose data information systems, military activities and other disruptions using computer networks and the Internet. In looking at the sources of the above threats, the government through the

[11] Iwan, dkk, *Kajian Strategi Keamanan Cyber Nasional: Dalam Rangka Meningkatkan Ketahanan Nasional di Bidang Keamanan Cyber,* (Jakarta: Tesis Universitas Pertahanan Indonesia, 2012).

[12] *Ibid.*

Ministry of Defense (Kemhan) needs to prepare themselves in the face of this cyber threat. Kemhan need to provide reliable Human Resources in mastering technology, reliable infrastructure system, and supported by legislation or policy in carrying out cyber warfare operation.

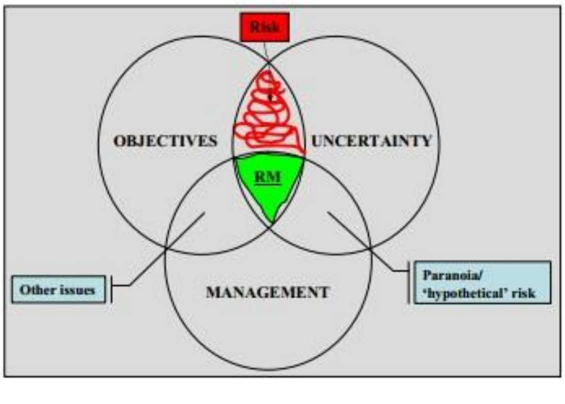
Discussion

Indonesia belongs to the five largest countries that use social media and is perceived as a positive potential (strength) or negative potential (vulnerability / weakness) if it is associated with potential cyber war. The use of social media among the public could potentially threaten the sovereignty of the state. But on the other hand, social media can also be a source of knowledge about the world of information technology, communication and digital, so that people can literate the digital world. The activities of Indonesians using digital technology will eventually become a potential for cyber warfare. The use of information technology will be easily tapped or hacked by hackers and crackers from foreign countries, so it will create vulnerabilities, especially intelligence information that uses the virtual world as a means of transmission. Fast-forward tapping technology for hacking social media users will be very harmful in this era of cyber warfare.

Risk management is defined as "*process of understanding and managing the risk that organization is inevitability subject to attempting to achieve its corporate objectives*".[13] Risk Management is also defined as "*the essence of risk management lies in maximizing the areas where we have some control over the outcome while minimizing the areas where we have absolutely no control over the outcome, and the linkage between effect and cause is hidden from us*".[14]

Referring to the above two definitions, risk management is a continuous process, carried out during defense management activities in the

Figure 2. Risk Management



Source: Steve Gibson, cranfield.ac.uk

[13] Collier, P.M. Agyei S. dan Ampomah, *CIMA's Official Learning System: Management Accpunting – Risk and Control Strategy, First Edition*, (Oxford: Elsevier, Ltd, 2006).

[14] Bernstein, Peter L. Against the Gods: The Remarkable Story of Risk. (Canada: John Wiley&Sons Inc, 1998)

face of the threat of cyber crime. Risk management is a management (planning) that plans advanced plans in the face of risk and uncertainty in order to maximize the achievement of objectives.

Elements of risk management according to the Institute of Risk Management include Risk Assessment, a process of identifying, describing and estimating; Risk Evaluation, decision making on significant risks that should be treated depends on risk appetite; risk treatment, risk appetite is a response or treatment that is the process of selection and implementation. The several stages in the risk management process that can be implemented in facing the threat of cyber crime are described as follows:[15]

a. *Identify*

In this stage, the identification of the risk of cyber crime should be done periodically against the triggers of cyber crime. In this process, all potentially harmful aspects are carefully identified. All identified risks are then measured. The measure of risk to this threat refers to two measures, namely Probability and Impact Probability.

b. *Assess*

At this stage, the assessment or judgment basically assesses the level of risk posed by cyber crime that affects all aspects of life, especially national defense. Assessment of cybercrime can not be measured directly but can use matrix tables in measuring the risks posed by cybercrimes.

c. *Treat*

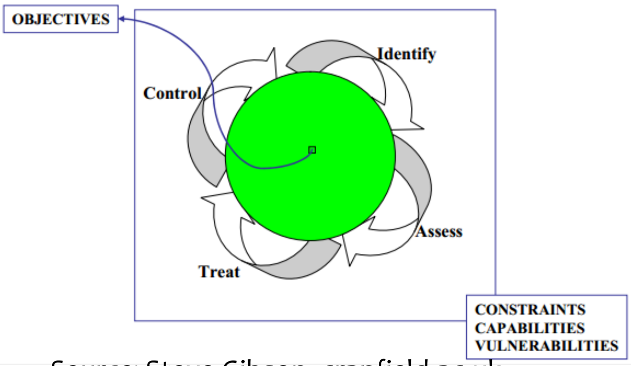
After identifying and measuring risks, it is then used as a basis for determining risk treatment and response, whether the risk will be accepted, transferred, minimized or avoided. In this case, it is necessary to minimize theft of information and data that often occur either individually or by institution.

d. *Control*

Monitoring and adjustment should be continuously made to assess the success of risk management. In the monitoring process, there should be an early warning mechanism for the security controller such as the Ministry of Defense of the Republic of Indonesia, so that the controlling party may take the necessary actions in order to anticipate the existence of cyber crime.

[15] Ibid

Fig 3. Risk Management Process



Source: Steve Gibson, cranfield.ac.uk

Risk Matrix

The potential threat of cyber crime leads to cyber warfare. The potential threat of cyber crime in Indonesia as follows.

1. *Hacking*

Hacking cases occurred several times in Indonesia. The causes vary from fraudulently hacking security to the rejection of government discourse. Examples of cases in 2014 presidential election and leakage of the news that the site of the General Elections Commission (KPU) was hacked hacked. The indication is that the KPU website could not be accessed.[16]

Not only in the government sector, but the private sector is often hacked by hackers. Recently Telkomsel Company hacked by hackers. In the page, the hacker was protesting the price of Telkomsel data packets are considered too expensive. His description also contains harsh words complaining about it.[17]

2. *Cracking*

Cracking cases occur in Indonesia by way of "carder" who just peek credit card then cracker peep savings of customers in various banks or other sensitive data centers for personal gain. Experienced crackers create their own scripts or programs for cracking, which targets credit cards, bank account databases, customer information databases, and purchases of goods with counterfeit credit cards[18].

3. *Cyber Sabotage*

Cyber Sabotage is done by making interference, destruction or destruction of a data, computer network system connected to the internet. Cyber sabotage is the most feared mudus by almost all the major industries in the world. At least the 'beautiful' modes that are played vary from malicious network posts and social slander, all the

[16] Trentech. "Kasus Hackting Terbesar di Indonesia", dalam https://www.trentech.id/5-kasus-hacking-terbesar-di-indonesia/, diakses pada 10 Juli 2017

[17] Tekno Kompas, " Situs Telkomsel Diretas Berisi Keluhan Internet Mahal", dalam http://tekno.kompas.com/read/2017/04/28/08042477/situs.telkomsel.diretas.berisi.keluhan.internet.mahal, diakses pada 10 Juli 2017

[18] Arifah, Dista Amalia. "Kasus Cybercrime Indonesia", *Jurnal Bisnis dan Ekonomi (JBE)*, Vol.18. No.2. September 2011

way to consumer information, hacking, and leaked systems from companies like card numbers or industry secrets.[19]

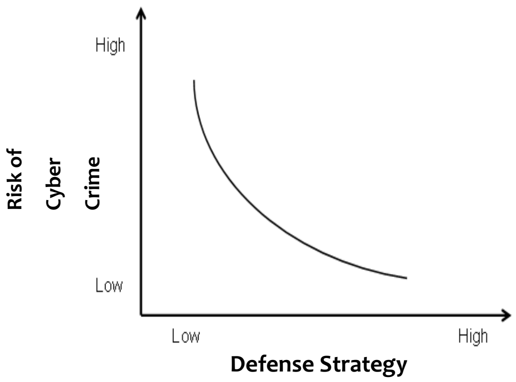
4. Spyware

Spyware is a program that can record secretly any user's online activities, such as recording cookies or registry. Recorded data will be sent or sold to companies or individuals who will send advertisements or spread the virus.[20] Malware cases occur in Indonesian society online bank users. The perpetrator spread malware to deceive the victim. Malware is distributed to customers' phones through fake internet banking software advertisements that often appear on a number of internet pages.

When the client downloads the fake software, the malware automatically enters the phone and manipulates the look of the internet banking page as if the page is really coming from the perpetrator spreading the malware to deceive the victim. Internet banking malware as if the page really came from a bank.

The key to understanding risk involves two elements, namely probability and consequence. This is done because the risk is also something that can not be avoided. Therefore, an understanding of risk management is essential in determining a strategy. The Risk Matrix arising from cyber crime when viewed in terms of probabilities and consequences as follows.

Figure 4. Risk Matrix



Source: Deduced by Author

In the risk matrix can be seen that the higher the risk of cyber crime then the defense strategy made should be improved.

Risk management is a fundamental element of a strategy. From risk management we can make a calculation of a budget cost required. In the handling of cyber crime, no small cost incurred in securing the confidentiality of information and data of a country. Therefore, risk management can make a

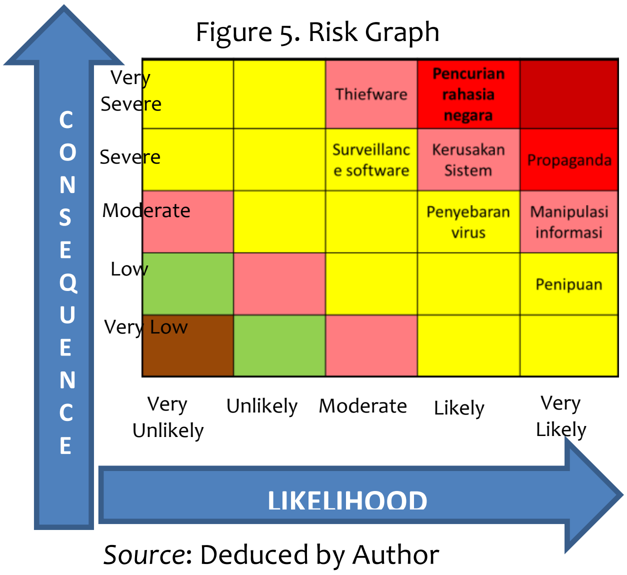
[19] Detik, "Meminimalisir Kejahatan Cyber Crime dan Cyver Sabotage di Indonesia, dalam http://news.detik.com/kolom/2610228/meminimalisir-kejahatan-cyber-crime-dan-cyber-sabotage-di-indonesia, diakses pada 10 Juli 2017

[20] Ibid

more affordable strategy in dealing with cyber crime threats.

Risk is an integrative metric to evaluate alternatives and prioritize resources. The decision-making in risk management, the risks of the highest priority should be funded in advance compared to lower priorities. The important thing to do in risk management is the creation of graphics that define risks in terms of probabilities and their consequences. Risk is a combination of likelihood and consequence. This answers the question of how probable the probability is and how bad the consequences are. Here's a graphic example of a cyber crime threat.

Figure 5. Risk Graph



Source: Deduced by Author

Risks to cyber threats are increasing. Pusdatin Ministry of Defense of RI said that cold war of cyberwar is running in global context. Sooner or later the country of Indonesia will be involved in which this cyberwar can be done by nation-state actor.

Cyberwar happens to be viewed from a state where a country penetrates the computer or server of other country. Such circumstances must be directly related to the sovereignty of the state and the national interest of Indonesia. Therefore, Indonesia must prepare a good state defense system. If not addressed properly, the biggest risk that will be experienced is the theft of secret state data and geopolitical changes and geostrategis Indonesia with other countries.

The Nation’s Defense against *Cyber Crime*

In the military aspect, cyber is used as a tool to attack the opponent's strength or to know the weakness of the opponent and damage the defense network. In reaching a power, cyber depends on a country's strategy and policy to develop cyber security.

The formation of cyberarmy is part of the development of the Cyber Defense Center which includes defense of the Ministry of Defense's information and communication system. Cyberarmy consists of the military that is the Army, the Air Force, and the Navy as well as civilians who participate in the defense of the state in the field of Technology and Information. Cyberarmy is needed as a state defense that can deflect all attacks in cyberspace that at any time can disrupt the integrity of NKRI. Cyberarmy is also required to have the ability to attack that can balance the progress of technology and other countries' information.

In the defense of the state both military and non-military are very important to have a new system as a modern generation and future war, in the field of defense of technology and information. In addition to strong state defense, it also requires mutual legal support and interconnected in the face of cyber crime threats. Laws are needed to create order and justice in society.

Technology, law and society today become a unity that can not be separated. Along with technological advances, society is required to continue to grow and not infrequently lead to the emergence of new crimes in technology. Therefore, the law becomes the most important part to deal with criminality that can damage the country's defense.

Cyber crime in Indonesia is frequently happening either by individuals or groups. All criminal acts related to cyber are of various types, ranging from copyright, piracy, misuse of access to even defamation of individuals or institutions. But this is in stark contrast with the law that regulates cyber crime that is still very minimal limitations that can be used as a reference to ensnare perpetrators in committing a crime. This inequality makes law less powerful. Law enforcement in Indonesia about computer abuse is influenced by several factors namely the Act, the mentality of the officers, the behavior of society, the means and the culture.

The Ministry of Communication and Information noted that there are 21 laws and 25 bills that will be affected by the laws governing cybercrime. External harmonization consists of adjusting the formulation of cybercrime articles with similar provisions from other countries, especially with the Draft Convention on Cyber Crime and cybercrime arrangements from other countries. The world of internet technology has provided a revolution and innovation to human beings in communicating. Therefore, a harmonization between law and technology is required. This harmonization has been well implemented in the Bill, PTI, IETE Bill, the bill of ITE, the TPTI Bill and the Criminal Code Bill.[21]

Cybercrime issue is requires standardization and harmonization in one

[21] *Ibid.*

particular area, namely legislation, criminal enforcement, and judicial review in law enforcement and judicial efforts.[22]

The ITE Act is a law that specifically regulates cyber crime both criminal law and criminal procedure law. The newly born law is cyberlaw. Cyberlaw itself is used for law enforcement related to the utilization of information technology in anticipating the behavior of society on information technology, as the restriction to do the crime (Law of Information Technology) and cyber law.

IT HR Planning to Cope with Cyber Crime Threat

The preparation that Indonesia must have in dealing with cyber crime is the human resources and state security production facility. Competence-based human resources are expected to create a positive way of thinking to the dynamics of global environmental change so as to increase awareness of technological developments and information that cause various impacts in people's lives, especially related to cyber threat.

In order to anticipate the cyber crime requires technological experts who can support sophisticated and modern state defense system. Therefore, it is necessary to cooperate with Indonesian defense industry that can make information and communication system program that can compete with other countries. Increasing the role of the military in developing cyber defense system in Indonesia can not be denied. Cyber military defense sets up operations and resources to improve national cyber security.[23]

The development of cyber defense system in Indonesia is influenced by two factors. The first factor is regulation and the second is the existence of a cyber command center. The government needs to make a good and proper regulation related to the development of national cyber security. As a comparison material, regulations made by the US government are USA cyber attack convention, draft cyber warfare international law manual and council of Europe convention on cyber crime 2001.[24]

Another important thing is to build a cyber defense security command center. The Indonesian government will implement a cyber operation command aimed at becoming a cyber defense command center in Indonesia. When the

[22] Edmon Makari, “Informasi Hukum untuk Sistem Ketahanan Nasional Terhadap Penyelenggaraan Sistem dan Komunikasi Elektronik Global”, *Jurnal Ketahanan Nasional,* 2014, hlm. 77.

[23] *Ibid.*

[24] *Ibid.*

command center is operational, there is great hope for Indonesia that is ready to anticipate the non-traditional threat, namely cyber crime which increasingly influences the sovereignty of NKRI. This is a major step that needs to be continued in order to run optimally. The need for proper regulation and cooperation with all parties, both government and private can be key in facing the increasingly complex challenges of the cyber world.[25]

IT HR planning process is part and function of personnel development within Ministry of Defense and its staff.[26] This function is carried out by the Bureau of Personnel, in accordance with the Order of the Minister of Defense No. 16 of 2010, article 41, paragraph 2 that the Procurement of Civil Servants Kemhan, TNI Headquarters and Force and the development of employees Kemehan. The IT HR planning process is based on certain criteria, such as educational background, administration, physical, health, and HR psychology, should be considered. The procurement process of civil servants in Kemhan has several stages starting from the procurement process, education, use, care and separation.

Efforts to realize competency-based human resources, is the main capital in dealing with various changes in strategic environment and technological advances today. IT human resource planning is more concerned with quality than quantity to meet personnel needs. Understanding of the educational background of IT human resources both formal and informal education greatly helps the organization in producing quality IT human resources. Therefore, the preparation of IT human resources requires the ability of state defense systems, network systems, applications, and policies related to cyber.

Conclusion

1. The threat of cyber crime in the form of theft of confidential information and data is aimed at attacking individuals, government and military agencies that threaten the defense of a country. The government through the Ministry of Defense institutions needs to prepare themselves in the face of this cyber threat. Kemhan need to provide reliable Human Resources in mastering technology, reliable infrastructure system, and supported

[25] Mohammad Syahruddin, "Propaganda Malaysia terhadap Pertahanan Negara Indonesia melalui Cyber pada Kasus Blok Ambalat", Jakarta: Tesis Universitas Pertahanan, 2015.

[26] *Ibid.*

2. by legislation or policy in carrying out cyber warfare operation.
3. Risk management made in the field of information and communication related to the lives of many citizens or the secret is done to reduce the level of vulnerability to misuse of information and data in cyberspace. Risk management is a fundamental element of a strategy. Risk is a combination of likelihood and consequence. This answers the question of how probable the probability is and how bad the consequences are. Therefore, important risk management is made to prepare a good state defense system.
4. In achieving a cyber power depends on a country's strategy and policy to develop cyber security. In addition to strong state defense, also requires legal support that affect each other and interconnected in the face of cyber crime threats. The need for proper regulation and cooperation with all parties, both government and private can be key in facing the increasingly complex challenges of the cyber world.

Reference

Book

Bernstein, Peter L. 1998. Against the Gods: The Remarkable Story of Risk. Canada: John Wiley&Sons Inc.

Bessis, J. 2002. *Risk Management in Banking*. Willey: Chicester.

Collier, P.M. Agyei S. and Ampomah. 2006. *CIMA's Official Learning System: Management Accounting – Risk and Control Strategy, First Edition*. Oxford: Elsevier Ltd.

J.A. Scholte, 2000. *Globalization: A Critical Introduction*. London: Palgrave.

Kementerian Pertahanan Indonesia. 2014. *Pedoman Pertahanan Siber*. Jakarta: Kemnhan RI.

Scholte, J.A. 2000. *Globalization: A Critical Introduction*. London: Palgrave.

Journal

Arifah, Dista Amalia. 2011. "Kasus Cybercrime Indonesia", *Jurnal Bisnis dan Ekonomi (JBE),* Vol.18. No.2.

Andersen, T.J. 2008. "The Performance Relationship of Effective Risk Management: Exploring the Firm-Specific investment Retaionale". Long Range Planning. Vol. 41. No.2.

Brantas, Sugeng. 2014. "Defence Cyber dalam Konteks Pandangan Bangsa Indonesia tentang Perang dan Damai". Jurnal Pertahanan, Vol.2. No.2.

Lestari, Rini. 2013. "Pengaruh Manajemen Risiko Terhadap Kinerja Organisasi. Jurnal Riset Akuntansi dan Bisnis". Vol. 13. No.2.

Makari, Edmon. 2014. "Informasi Hukum untuk Sistem Ketahanan Nasional Terhadap Penyelenggaraan Sistem dan Komunikasi Elektronik Global". Jurnal Ketahanan Nasional, Vol.2. No.2.

Pearlman, W. and Cunningham, K.G. 2012. "Non State Actors, Fragmentation, and Conflict Processes". *Journal of Conflict Resolution*. Vol.2.No.56. 56.

Thesis

Kurnia N.M., Erwin. 2015. *Kesiapan Sumber Daya Manusia Teknologi Informasi (SDM-TI) Kementerian Pertahanan untuk Mengantisipasi Cyber Warefare*. Tesis Universitas Pertahanan.

Mohammad Syahruddin. 2015. Propaganda Malaysia terhadap Pertahanan Negara Indonesia melalui Cyber pada Kasus Blok Ambalat. Jakarta: Tesis Universitas Pertahanan.

Syahruddin, Mohammad. 2015. *Propaganda Malaysia terhadap Pertahanan Negara Indonesia melalui Cyber pada Kasus Blok Ambalat*. Jakarta: Universitas Pertahanan

Website

Anderson, Nate, "Massive DDoS Attack Targets Estonia, Russia Accused", dalam http://arstchnica.com/security/2007/05/massive-ddos-attacks-target-estonia-russia-accused/, diakses pada 8 Juni 2017.

Kelly, Michael B, "The Stuxnet Attack on Iran's Nuclear Plant Was Far More Dangerous Than Previously Thought", dalam http://www.businessinsidercim/stuxnet-was-far-more-dangerous-than-prevoius-thought-2013-11?IR=T&, diakses pada 8 Juni 2017.

Michael B. Kelly, "The Stuxnet Attack on Iran's Nuclear Plant Was Far More Dangerous than Previously Thought", dalam http://www.businessinsidercim/stuxnet-was-far-more-dangerous-than-prevoius-thought-2013-11?IR=T&, diakses pada 8 Juni 2017.

Nate Anderson, Massive DDoS Attack Targets Estonia, Russia Accused, dalam http://arstchnica.com/security/2007/05/massive-ddos-attacks-target-estonia-russia-accused/, diakses pada 8 Juni 2017.

Situs Dirjen Kementerian Pertahanan RI Di-Hack, dalam https://news.detik.com/berita/2243078/situs-dirjen-kementerian-pertahanan-ri-di-hack?9911012, diakses pada 12 Mei 2017.

Snowden: Ponsel SBY Disadap Australia", dalam http://news.liputan6.com/read/748895/snowden-ponsel-sby-disadap-australia, diakses pada 8 Juni 2017.

Tekno Kompas, "Situs Telkomsel Diretas Berisi Keluhan Internet Mahal", dalam http://tekno.kompas.com/read/2017/04/28/08042477/situs.telkomsel.diretas.berisi.keluhan.internet.mahal, diakses pada 10 Juli 2017

Trentech. "Kasus Hackting Terbesar di Indonesia", dalam https://www.trentech.id/5-kasus-hacking-terbesar-di-indonesia/, diakses pada 10 Juli 2017