THE USE OF COUNTER–INTELLIGENCE OPERATION STRATEGY IN COPING WITH CYBER THREATS

Yosua Praditya Suratman[1]

Secretariat Council of Strategic Analyst
(ypsuratman@gmail.com)

Abstract - The increasing number of cyberattacks that occur today indicates that Indonesia is an easy target for crime actors in the cyber world. Cyberattacks are selected because they are far more effective than conventional attacks - the military, and the actors are also invisible. Not to mention, the capacity of cyber handling, both infrastructure, funds, and human resources in Indonesia is inversely proportional compared to the number of cyberattacks in the last decade. Intelligence strategies, primarily counter-intelligence, is the answer to deter and detect the attacks, while the government fixing the regulations and policies of national cyber threats.

Keywords: cyber, counter intelligence, security

Preface

The increasingly complex presence of threats in Indonesia demonstrates that the dynamics of non-military threats continue to evolve with the development of time and technology. Cyber threat is one form of non-military threat whose growth rate has increased very rapidly in the last decade. It is undeniable that the advancement of cyber technology with its innovation of infrastructure further eliminates the boundaries between countries. The world seems to be more narrow and even convenience and ease into two keywords in a job both in government and private organizations. Analysis and computerization of data in the government sector, financial transactions in the banking sector, the benefits of military technology on defense equipment, and various jobs commonly done by the public as cannot be separated from the existence of cyberspace media, including the internet. By 2016, approximately 47 percent of the world's population is already using internet facilities, which is up from 43 percent earlier in 2015.[2] This figure is clearly predicted to

[1] The author is an alumnus of Defense Studies Department of Defense Management Cohort 4 and currently works as a Secretariat Staff of Strategic Analysis Council since 2015 until now.

[2] "47 percent of the world's population now use the Internet, study says" http://www.washingtonpost.com, 22 November 2016, accessed on 5 June 2017.

continue to increase as the relationship between technology and time is linear.

It is commonplace for the current Indonesian government to pay very high attention to cyber threats in recent times. In 2016, Indonesia recorded about 1.2 million more cyber threats, and Indonesia it is expected to be in the 26th position globally most vulnerable to cyberattacks.[3] The attacks are generally in the form of increasingly growing malware, the mode of data theft of bank accounts, savings accounts demand, credit cards, ransomware, and important data from every agency/government agencies and private. This means that all sectors are vulnerable to cyber threats at the moment. Some of these facts also show that Indonesia is an easy target for cyber-criminal world. The intelligence approach seems to be the primary choice in warding off cyberattacks that have progressed phenomenally over the past decade. The use of counter-intelligence strategy is one of the necessary efforts to prevent and detect early on any potential cyber threats. Therefore, in this paper, we will discuss three issues related to governance of cyber threats, namely, first, the increasing trend of cyber threats in recent times; Second, the type of cyberthreat facing Indonesia; And third, the counter-intelligence analysis looks at the development of national cyber threats.

Trend of Increasing Cyber Threats in the Past One Decade

According to Smith, the threat of cyber has been the source of various threats that not only attack the state / government, but also see organizations, companies, and individuals being the object. This is done in order to gain profit for their group, both financially, militarily, and his political interests.[4] Can be likened to a double-edged sword, on the one hand cyberspace offers great benefits but security uncertainty is also a given, whether intentionally or not. According to Setyawan and Sumari, cyber threats are used because its scope is able to steal information, propagate destructive ideas, as well as attacks on information systems in various fields, such as banking

[3] "Ancaman siber di Indonesia Kian Mengkhawatirkan", http://www.cnnindonesia.com, 8 September 2016, accessed on 5 June 2017.

[4] Michael Smith, Research Handbook on International Law and Cyberspace, (Cheltenham UK: Edward Elgar Publishing Limited, 2015), p. 2.

data and military networks and defense systems country. Even a survey conducted by the Ponemon Institute in 2015 of about 1000 senior leaders of Information Technology (IT) and IT Security in various companies and government agencies in America, Europe, Middle East and Africa said there was an ongoing increase in attacks on increasingly sophisticated countries followed by cyber threats and cyber terrorism and high data breakage.[5]

The increasing rate of cyber-threats also occurred in the Asia Pacific region, including Indonesia, where in 2015 there was an increase of 61 malicious sites active hosts, which rose from 41 million in 2014[6]. In recent years, the methods of cyber-attack actors have changed dramatically, where in the past attacks were still visible and opportunistic, targeting individual and non-state objects. But now the coverage of cyber threats is wider with targets already recorded from hidden actors[7]. This can be seen in Figure 1.

Based on the picture, the 1980 - 1990 cyberattacks are more inclined to the opportunist goal of benefiting the group. Call it like password guessing, self-replacing code, and bulgaries whose original purpose is to attack the company and get the funds. However, the trend of threats is increasingly changing from 2005 to 2015, where the characteristics of threats are already very stealthy and the use of the system is already more advanced in attacking the defense of a country. What is more dangerous is that cyberattacks do not require sophisticated equipment to attack, but enough with a reliable HR behind the screen of his laptop (tools). Cyber-threat terrorists are currently more diverse and numerous.[8]

Types of Threat Currently Developing

The Budapest Convention at the EU Convention on Cybercrime November 23th

[5] David Setyawan and Arwin Sumari, "Diplomasi Pertahanan Indonesia Dalam Pencapaian Cybersecurity Melalui ASEAN Regional Forum on Cybersecurity Initiatives", Jurnal Penelitian Politik,Vol. 13, No. 1, June 2016, Jakarta: Lembaga Ilmu Pengetahuan Indonesia, p.3.

[6] "Catatan Trend Micro Tentang Ancaman Siber di Asia Pasifik", Antara News, 17 June 2015, accessed on 7 June 2017.

[7] Eric Cole, "Detect, Contain, and Control Cyberthreats", SANS Institute, June 2015, in https://www.sans.org/.../detect-controlcyberthreats-36187, accessed on 7 June 2017, p. 4.

[8] *Ibid.*

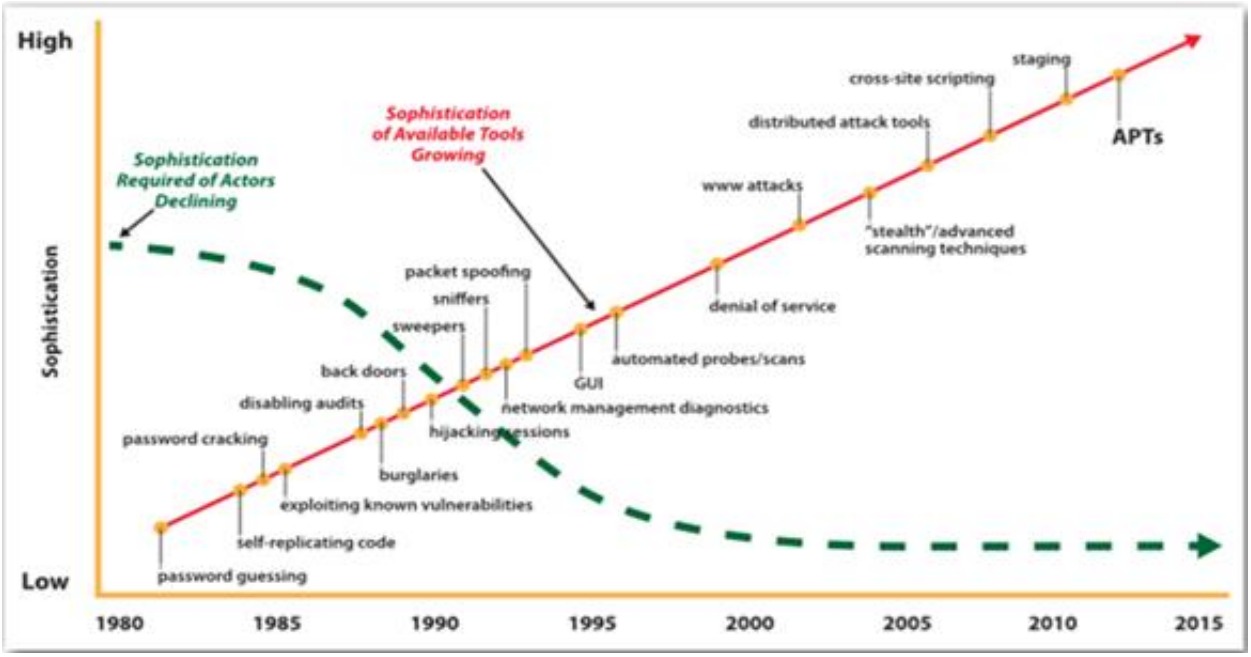

Figure 1. Cyber Threat Evolution since 1980 – 2015

Source: Eric Cole, "*Detect, Contain, and Control Cyberthreats*", SANS Institute, June 2015, on https://www.sans.org/.../detect-control-cyberthreats-36187, accessed on 7 June 2017

2001 in Hungary was established in order to recall the characteristic cybercrime threats that are borderless and use high technology as a medium. Therefore, this convention also sees criminalization policy in information technology that must pay attention to the development of cybercrime prevention both regionally and internationally in order to harmonize and uniformity of cybercrime arrangement.[9] From this Budapest convention there are three types of cyber-threat categories that are described as follows:[10]

1. *First Category*

   Cyber threats are a collection of types of attacks where information and communication technologies are the primary means or weapons to commit crimes. Examples are computers and

[9] Amirulloh, Muhammad et al., "Laporan Kajian EU Conventional on Cybercrime Dikaitkan Dengan Upaya Regulasi Tindak Pidana Teknologi Informasi",(Jakarta: Laporan Puslitbang Badan Pembinaan Hukum Nasional Departemen Hukum dan Hak Asasi Manusia Republik Indonesia, 2009), p. 4.

[10] Prof. Richardus Eko Indrajit, "Enam Aspek Menjaga dan Melindungi Dunia Maya", IDSIRTI (Internet and Infrastructure/Coordination Center) Indonesia, in http://www.idsirtii.or.id/doc/IDSIRTII-Artikel6_aspek_menjaga_dan_melindungi_dunia_maya.pdf, pp.5, accessed on 7 June 2017.

the Internet are used as tools and mediums to spread heretical sect; A mobile phone used to send messages or text messages to deceive potential victims; And electronic mail is used as a means to transmit images or video nuances of pornography.

2. *Second Category*

   Cyber threats are a collection of where computers or information technologies are subjected to a center of attack from criminals, such as, firstly, conducting fictitious financial transactions in an internet-based banking system (e-banking); Second, shut down or dismantle the work of a remote internet network; And third, spreading viruses to interfere with the performance of certain computers.

3. *Third Category*

   This cyber threat is aimed at events intended to destroying (including modifying and fabricating) data or information stored in the media of information technology devices. Attacks in this category include: first, changing the content of a site without the owner's knowledge; second, take a collection of passwords or complete credit card information of a group of individuals for misuse or sale; and third, damage the main database system so that the information in it becomes unreadable or accessed normally and so forth.

The three types of threats above show that the subject of cyber threats is not only directed to the government, but including individuals, community groups, and companies. The impact is obviously great although there is no dose calculating the loss conversion caused by cyberspace, but certainly this type of threat and threat trend will certainly increase steadily along with the development of technology. According to Brenner & Clarke, there are three reasons why this type of cyber threat is currently preferred over conventional attacks, like the military in general.

Firstly, developing a cyber-siege capacity costs less than developing the capacity of military wars in the 21st century. The cost of cyberwarfare includes training and financing of hardware and software cost less than conventional warfare. Second, the use of actors is much less than the military war, and the implementation can be done from a distance. That is, cyber

war no longer sees distance, time, and number of personnel, but as long as the system can be attacked then a country can easily perform cyberattacks. The actor is not limited whether state or non-state, as long as they are able to attack the intended system, whether it is state property or company or group. Thirdly, cyberattacks are very easy to sponsor without knowing who the real actors are, whether it's A country, country B, organization A, organization B, or even just a handful of groups / individuals.[11]

Cyber Threats Challenges in Indonesia and Its Current Policy

It cannot be denied that the urgent condition of cyber threat in Indonesia can be said in critical condition. With a population of 132 million internet users in 2016 it is not impossible that Indonesia becomes an easy target for cyberattacks from state and non-state actors. The description of internet users in Indonesia can be seen as follows:[12] (1) 67.2 million people or 50.7 percent access through handheld devices and computers; (2) 63.1 million people or 47.6 percent access from smartphones; and (3) 2.2 million people or 1.7 percent access only from computers. In addition, from a survey presented by APJII (Association of Indonesian Internet Network Providers), it was noted that approximately 86.3 million people or 65 percent of the total number of internet users this year are in Java. While the rest are as follows; (1) 20.7 million or 15.7 percent in Sumatra; (2) 8.4 million or 6.3 percent in Sulawesi; (3) 7.6 million or 5.8 percent in Kalimantan; (4) 6.1 million or 4.7 percent in Bali and NTB; And (5) 3.3 million or 2.5 percent in Maluku and Papua.

Looking at the data above and compared with the government's readiness in regulating national cyber security, it is not surprising if there is still a lot of criticism from most community groups. According to Adriyanti (2016) there are five cyber-security policies in Indonesia at this time that get full attention, namely:[13]

a. Legal Certainty

[11] Susan Brenner dan Leo Clarke, "Civilians in Cyberwarfare: Conscripts, *Vanderbilt Journal of Transnational Law,* Vol. 43, pp. 1011, 2011, University of Dayton School of Law, 2011, pp. 3-4.

[12] "2016, Internet Users in Indonesia Reach 132 Million", in http://tekno.kompas.com/read/2016/10/24/15064727/2016.pengguna.internet.di.indonesia.capai.132.juta, accessed at kompas.com, in July 18th 2017, issue 24 October 2016.

[13] Handrini Andriyanti. "Cyber Security dan Tantangan Pengembangannya di Indonesia", *Jurnal Politica* Vol. 5 No.1 June 2014, pp. 99 - 101

The legality of criminal handling in the cyber world is still weak because despite the existing laws and regulations that prohibit the form of attack or destruction of electronic systems in the Act of Information and Electronic Transactions No.11 of 2008, there is no legislation regulating specifically cybercrime and cybercrime handling while on the other hand the form of crime of cyber world is increasing and the pattern of occurrence so fast that it is difficult to be handled by law enforcement officers.

b. Technical and Procedural Measures

Cybercrime handling is still partial and scattered and there is no standard coordination in handling cybersecurity issues. The low awareness of the cyber threat attacks that impactfully cripple vital infrastructure. An example is the flight radar system at Soekarno-Hatta international airport which has been interrupted several times.

c. Organizational Structure

Cyber-security handling in the state defense framework is still sectoral and uncoiled and unified. Although in the end, the government succeeded in forming the State Cyber and Code Agency through Presidential Regulation Number: 53 of 2017 on Cyber and State Codes.

d. Capacity Building

Human resource development is needed on the importance of cyber-security in order to increase understanding of preventive measures in preventing all cybercrime.

e. International Collaboration

Strengthening international cooperation with regional and international organizations in the context of cybercrime prevention. Cooperation in order to overcome cybercrime that Indonesia has done on a regional scale and global.

Based on the description above , it can be seen how the current conditions and approaches that have been done by the Government. Based on a journal written by Handrini[14], the existing approach is still not maximum when compared to the threat intensity level and its variation. Moreover, internet users in Indonesia are numerous. Therefore, the strengthening of counter-intelligence approach becomes one of the

[14] *Ibid.*

scopes of discussion that should be done by intelligence agencies together with other relevant stakeholders.

Approach to Counter Cyber Intelligence in Facing Threats

Previously it should be understood in advance the function of intelligence based on applicable law in Indonesia. Referring to Law no. 17 of 2011 About State Intelligence, then the interpretation of the intelligence function is the function of investigation, security, and promoting. Where the counter-intelligence activities themselves fall into the category of promoting functions within the written Intelligence Act "a series of activities conducted in a planned and directed manner to prevent and/or combat attempts, work, activities of Intelligence, and or Opponents that harms national interests and security."[15] There are four main aspects of intelligence activities, namely counter intelligence, espionage, propaganda, and sabotage. According Soeripto in Praditya, counter-intelligence itself is a preemptive activity that is confidential. The goal is to narrow the space, ward off, thwart, and destroy opponent's intelligence operations. The operation of counter-intelligence is divided into two, namely passive and active, as described below:[16]

1. *Passive Counter Intelligence*

   Includes four things. *First*, secret restriction by limiting the number of people who know the secret, where the fewer people who know the secret then the chances of success will be greater. *Second*, information security by all means to prevent the opponent from knowing the information. *Third*, it filters out all sorts of activities and relationships in enemy movements. *Fourth*, do camouflage by changing the shape of something or give wrong info to the enemy. *Fifth*, concealment of the intelligence movement to be unknown to the enemy.

2. *Active Counter Intelligence*

   Active counter-intelligence leads to empowerment of intelligence activities to gain information from opponents by eliminating threats, challenges, obstacles, and distractions. Active counter-intelligence acts as a counter

[15] See Law No. 17 of 2011 about State Intelligence Chapter 6 Article 3.

[16] Yosua Praditya, *Keamanan di Indonesia*, (Jakarta: Nadi Pustaka, 2016), pp. 246–247.

penetration, counter infiltration, counter espionage, counter sabotage maker, and the use of special camouflage in opponent, enemy, or enemy territory. For example, counter-espionage counters must be actively observing constantly any symptoms that arise, until the case is revealed. Meanwhile, counter-surveillance is an attempt to conduct surveillance against the opposing party. Reconnaissance in this case focuses on securing, defending, and protecting any intelligence activities of the enemy. The main differentiator in active counter-intelligence is its more attacking activity, rather than persisting. Furthermore, according to Rahardjo, the above counter-intelligence division can be subdivided into vertical and horizontal sections as shown in the Chart 1[17].

Chart 1. Counter Intelligence Matix

Defensive Mode Blocks opposing access and gather information about opponents	
Passive Defense Block Opposing Access to Information	**Active Defense** Investigate opponent's action using surveillance, feed, double agent, spy, or electronic tapping
Offensive Mode Aim to manipulate, control, and thwart opponent's action	
Passive Offence Allowing the opponent see false information (seeing something that is not there, or something false, camouflage)	**Active Offence** Directly sends false information through secretive actions

Source: Beer and Basie on Elsa Vinietta, http://budi.rahardjo.id/files/courses/2016/EL6115-2016-23215130-Report.pdf, accessed on 7 June 2017, p. 5.

[17] Budi Rahardjo, "Strategi Operasi Kontra Inteijen Cyber Sebagai Upaya Peningkatan Ketahanan Negara Indonesia", on http://budi.rahardjo.id, accessed on 7 June 2017, p. 5.

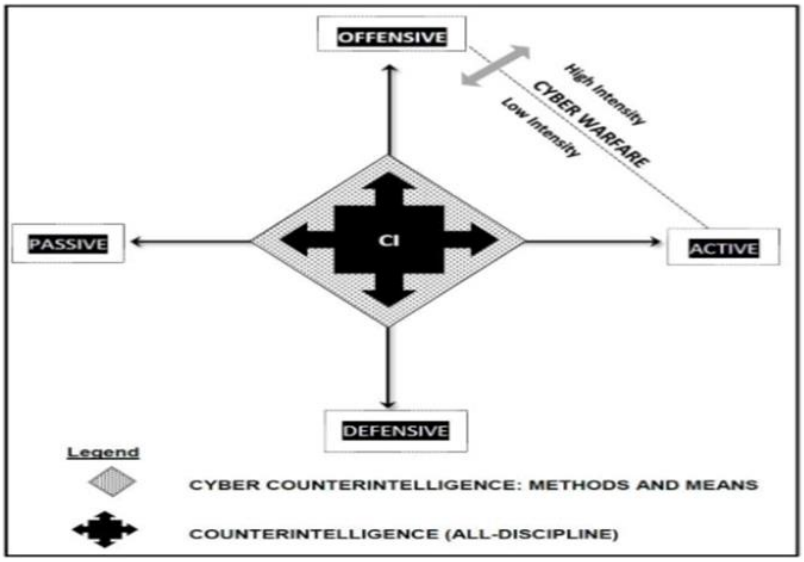

Figure 2. Integrated Counter Cyber Intelligence

Source: Beer and Basie in Elsa Vinietta, http://budi.rahardjo.id/files/courses/2016/EL6115-2016-23215130-Report.pdf, accessed on 7 June 2017.

Based on the Chart 1, both passive and active intelligence counter, ideally inseparable because the implementation should be done synergistically. What makes the difference is each mission, both offensive and defensive, which shows each action to ward off the enemy. Meanwhile, the vertical division distinguishes counter-intelligence operations from being active or passive based on the intensity of the given response. Passive action is done by protecting while waiting or allowing opponent operations but with minimal response, while active action is made by performing certain responses according to the circumstances.[18] Furthermore, if in seeing the linkage of cyber threat with counter cyber intelligence then can be seen in the Figure 2.

In the Figure 2, the intensity of cyberattacks is categorized as low and high intensity. With reference to the method of integrated counter-intelligence then the interpretation can be seen in the Table 1[19].

Based on the Table 1, it can be seen how each counter cyber intelligence approach are integrated against cyber threat. By using Table 1 we can analyze resources, including human, financial, and tools can be used effectively and efficiently.

[18] Elsa Vinietta, "Strategi Operasi Kontra Intelijen Cyber Sebagai Upaya Peningkatan Ketahanan Negara Indonesia", on http://budi.rahardjo.id/files/courses/2016/EL6115-2016-23215130-Report.pdf, accessed on 7 June 2017, p. 6.

[19] *Ibid,* p.10.

Keep in mind in dealing with cyber threats, resources have to be tailored to the shape and extent of the threat intensity, so the government does not incur excessive costs compared to reality. Cost to handle cyber threats does not need to be abundant provided that the human resources used given the right tools.

Table 1. Integrated Counter Cyber Intelligence Explanation

No	Method	Flow of Operation Mechanism
1	First Strategy- *Active* Counter Intelligence *Offensive High Intensity*	Objective-> Attacking; Opponent-> Identified; Priority -> High;
2	Second Strategy- *Passive* Counter Intelligence *Offensive High Intensity*	Objective -> Attacking; Opponent-> Identified; Priority -> Low;
3	Third Strategy - *Active* Offensive Counter Intelligence *Low* Intensity	Objective-> Attacking; Opponent -> Unknown; Strategy -> Offensive
4	Fourth Strategy - *Passive* Counter Intelligence *Offensive Low Intensity*	Objective -> Attacking; Opponent -> Identified; Strategy -> *Passive*
5	Fifth Strategy – *Active Defense* Counter Intelligence *High Intensity*	Objective -> Defense; Information -> Crucial; Security Threat -> Exist (High).
6	Sixth Strategy – *Active Defense* Counter Intelligence *Low Intensity*	Objective-> defense; Information -> Crucial; Security Threat -> Low
7	Seventh Strategy – *Passive Defense* Counter Intelligence *High Intensity*	Objective-> Defense; Information -> Crucial; Security Threat -> exist (high)

8	Eighth Strategy – *Passive Defense* Counter Intelligence *Low Intensity*	Objective-> Defense; Information -> Not Crucial; Threat Risk -> Low

Source: Substracted by Author from Elsa Vinietta, "Strategi Operasi Kontra Inteijen Cyber sebagai Upaya Peningkatan Ketahanan Negara Indonesia", on http://budi.rahardjo.id/files/courses/2016/EL6115-2016-23215130-Report.pdf, accessed on 7 June 2017.

Analysis of Cyber Counter Intelligence in Engaging National Cyber Threat

From the description of the table above, then the author has an analysis to see how the cyber threat are handled accordingly with the method. Here is the explanation:

1. *Active Offense Counter Intelligence High Intensity*

   The approach can be done with two things, namely cyber war and the use of virtual agents. Indonesia itself is considered still lagging behind the cyber war between countries, because Indonesia is actually a market or "easy target" of other countries. Usually other countries do so by offering free services to the people of Indonesia in order to volunteer and be happy to provide personal information through the medial social. Yet these ways are categorized as cyber war (active offense) by a country to Indonesia. Both civil servants (PNS), military-security apparatuses, including civilians must provide detailed information to email and social media.[20] As for the availability of virtual agents in Indonesia, the spread is still scattered and actually sometimes even attack government agencies, Police, and state-owned companies. Though such hackers can be used by officials to be empowered to help national cyber resistance from the threat of the hackers. While in big countries, like the US and Russia, it is commonplace that hackers are empowered to attack other countries' security-defense systems. In essence this counter-intelligence strategy is attacking, the object is known (usually

[20] The statement of Chief of Communication and Information System Security Research Centre/CISSReC (Lembaga Riset Cyber dan Komunikasi) Pratama D Persada, "Perang Siber Sudah Menjadi Ancaman Serius", on http://www.republika.co.id, 17 September 2016, accessed on 8 June 2017.

the IT system of other countries), and it is something that is prioritized.

2. *Passive Offense Counter Intelligence High Intensity*

   This strategy is Passive (not attack) because the main purpose is to collect information in detecting cyber threats / enemies. In Indonesia it finally endorsed the State Cyber and Codes (BSSN) based on Presidential Regulation no. 53 of 2017 by President Joko Widodo. The task of BSSN is to implement cyber security effectively and efficiently by utilizing, developing, and consolidating all elements related to cybersecurity. In performing these tasks, BSSN performs the functions of: preparation, implementation, monitoring and evaluation of technical policies in the areas of identification, detection, protection, control, recovery, monitoring, evaluation, control of ecommerce protection, coding, screening, cyber diplomacy, Mitigation support, recovery of countermeasures, vulnerabilities, incidents and / or cyberattacks[21]. The presence of BSSN will greatly assist the government to collect all forms of important and confidential information, and is expected to assist the defense and intelligence apparatus in counter-espionage in cyber world.

3. *Active Offense Counter Intelligence High Intensity*

   This strategy is done with the attacking system even though the enemy (object) is not yet known because of the very high threat intensity. For example, the threats of ransomware that attack public facilities are generally unknown to who the actors are, but this does not make the government behave Passive. Recently Indonesia was shocked by the wannacry ransomware attack, which according to M. Salahuddin, Chairman of the Indonesia Security Incident Response Team on Internet Infrastructure (Id-SIRTII) revealed the potential for wannacry's ransomware distribution will still be open in Indonesia as Indonesia is a very vulnerable market. Ransomeware of this type will later ask for ransom of Rp 4 million in the form of virtual currency (cryptocurrency) Bitcoin sent to the

[21] See Presidential Decree Number 53 of 2017 about BSSN on Chapter 1 Article 3.

address of the digital wallet of cyber criminals[22]. This ransomeware virus is suspected to use cyber weapons owned by the US intelligence service, the NSA, which in April was stolen and leaked by a group of hackers named Shadow Broker. The tool named "EnternalBlue" takes advantage of security holes in the Windows operating system via remote code execution SMBv1[23]. Although the government has difficulty knowing the details of Broken Shadow in spreading the virus, the government has learned that the virus is leaking from the NSA. Therefore, the government's strategy is how to deal with a virus or weapon potentially leaking from the NSA and misused by hacker groups.

4. *Passive Offense Counter Intelligence Low Intensity*

   The attack strategy is done passively considering the target / object is known and the goal is still focused to gather information. What makes the difference is its low intensity. Government, in this case coordination between the Ministry of Information with BSSN and security-intelligence apparatus need to map the potential of the threat that is not too high. The goal is that in the future the government will not be bothered by the threat that has been transformed into a threat that has a big impact. For example, 10 years ago, the government was not yet aware of the immense social impacts of the use of social media and the internet by the public, whereby anyone can now voice his political opinions as long as they do not violate the rules. But the fact is, the spread of hate speech, provocative messages, and hoax news are hard to stem, and the fact that this tendency becomes a proxy war of other countries to bring Indonesia down. Taxonomic conflicts that occur are closely related to the proxy war and its spread is greatly helped by the internet / social world. That is, the government 10 years ago failed to counter passive offensive intelligence to the threat of low intensity (social media / internet), but in fact, now the threat is already transformed and has a very

[22] "Intel AS di Balik 'Ransomware' yang menyerang rumah sakit Indonesia," 13 May 2015, http://www.kompas.com, accessed on 8 June 2017.

[23] "Begini Cara Menangkal 'ransomware' wannacray", http//www.kompas.com, 13 May 2017, accessed on 8 June 2017.

destructive power for the Indonesian social environment.

5. *Active Defense Counter Intelligence High Intensity*

   This strategy combines two things, namely hardware and software. On the hardware side, clearly Indonesia needs to be supported by the presence of adequate caliber infrastructure. Currently, Indonesia is estimated to lose trillions of rupiah each year, one of them because it does not pay attention to the security of communication systems, including the infrastructure. For example, in the case of illegal logging and illegal fishing that always happens because of a well-coordinated communication system and low technology infrastructure. In addition, the lack of infrastructure can affect the vulnerability of data breaches of Indonesian people using e-ID card (estimated as many as 180 million inhabitants).[24] While on the software, the government through the presence of BSSN able to upgrade the IT security system in each institution / agency that exists. The implementation of electronic-based government system (E-Government) is an object that needs to be improved, because Indonesia is still feared to be an easy target for cyber criminals.

6. *Active Defense Counter Intelligence Low Intensity*

   This strategy is actually the same as the previous strategy, which combines two things, namely hardware and software. But its implementation is directed to threats of low intensity. In this case the government should no longer underestimate the small impact of cyber threats, because this type of threat will certainly transform in a relatively short time. Low risk level threats do not make the Government stop thinking about the hardware and software installation strategy needed as a preventive step in the future. An example can be taken, when the CISSReC (Communication and Information System Security Research) agency advises the government to build an integrated passport database system, so that it can check online passport

[24] Republika Newspaper's interview with the Chief of CISSReC, on the subject of "Indonesia Butuh Lembaga Pertahanan Siber", on http://www.republika.co.id, accessed on 8 June 2017.

exclusively against multiple passports in Indonesia or elsewhere.[25] While this type of threat to dual passport ownership has not been so much intensified over double IDs, it does not mean the government is doing nothing.

7. *Passive Defense Counter Intelligence High Intensity*

   This strategy which puts forward its physical defense, be it for security system of IT security and intelligence apparatus, and other Ministry facilities. The goal is to maintain the system facilities from the threat of data theft, both hardware and software, or any malware attacks that can shut down government-owned IT hardware. In addition, this strategy focuses on routine IT personnel checks, in terms of personnel usage and measurement, and leaves no vital chain of management within the IT sector itself. The ultimate goal is to get the security expected. An example can be taken from the air force defense, for example, to strengthen the ADIZ (Air Defense Identification Zone) Air Force requires the addition of 12 air radar.[26] Where the addition of radar is certainly followed by the addition of the number of personnel and training. Radar is the equipment that is the physical infrastructure required by ADIZ which is no longer only partial in the form of small circle of archipelago (Java, Sumatera, Kalimantan, etc.) but has a large circle including air space from Sabang to Merauke.

8. *Passive Defense Counter Intelligence High Intensity*

   This strategy is the same as the previous one (No. 7), namely emphasis on the construction of physical facilities and human resources and maintenance. But what distinguishes it is this strategy is addressed to the types of threats with low intensity. In the past decade, there are still many countries that have not yet thought about building an information storage database in the cloud, where the US is the only country that has thought about it. They think the data is safer stored in the cloud with the help of

[25] "Indonesia diusulkan Segera Bangun Sistem Paspor Terintegrasi," on https://www.cissrec.org/, 14 September 2016, accessed on 9 June 2017.

[26] "TNI AU Perkuat Zona Identifikasi Pertahanan Udara," on http://nasional.kompas.com/, 7 April 2017, accessed on 9 June 2017.

satellite technology than it is stored on hardware which is prone to be stolen, especially for their military and intelligence purposes.

Conclusion

The increasing trend of cyber threat has increased very rapidly, where the criminals can be done by anyone. Meanwhile, Indonesia is categorized as the most vulnerable country and the tenderest target in the Asian environment. Penetration of cyber threats so powerful has occurred, whether it is data theft or the destruction of government and private information systems. The cyber threat becomes an option for the criminals because it is not costly, does not require a lot of personnel, is not visible, and they are able to control it from a great distance, even across countries and continents. Therefore, the government, in this case the security-intelligence apparatus needs to carry out the appropriate counter-intelligence operations strategy in dealing with the growing cyber threat. Counter-intelligence strategy becomes one of the main options because it is confidential and able to narrow the space of cyber threat from various lines. Intelligence measures and strategies are at the forefront of cyberattacks that are predicted to increase in the future.

References

Book

Praditya, Yosua. 2016. *Keamanan di Indonesia*. Jakarta: Nadi Pustaka.

Smith, Michael. 2015. Research Handbook on International Law and Cyberspace. Cheltenham UK: Edward Elgar Publishing Limited.

Journal

Ardiyanti, Handrini. 2014. "Cyber Security dan Tantangan Pengembangannya di Indonesia". *Jurnal Politica*. Vol. 5. No.1. June.

Brenner, Susan and Clarke Leo. 2011. "Civilians in Cyberwarfare: Conscripts, Vanderbilt". *Journal of Transnational Law*. Vol. 43. University of Dayton School of Law.

Setyawan, David and Sumari, Arwin. 2016. "Diplomasi Pertahanan Indonesia Dalam Pencapaian Cybersecurity Melalui ASEAN Regional Forum on Cybersecurity Initiatives". *Jurnal Penelitian Politik*. Vol. 13. No. 1. June. Jakarta: Lembaga Ilmu Pengetahuan Indonesia.

Report

Amirulloh, Muhammad et al. 2009. "Laporan Kajian EU Conventional on Cybercrime Dikaitkan Dengan Upaya Regulasi Tindak Pidana Teknologi Informasi". Jakarta: Laporan Puslitbang Badan Pembinaan Hukum Nasional Departemen Hukum dan Hak Asasi Manusia Republik Indonesia.

Law and Governmental Regulation

Law Number 17 of 2011 about State Intelligence Chapter 6 Article 3.

Governmental Regulation Number 53 of 2017 about BSSN Chapter 1 Article 3.

Website

"Ancaman siber di Indonesia Kian Mengkhawatirkan", http://www.cnnindonesia.com, 8 September 2016, accessed on 5 June 2017.

"Begini Cara Menangkal 'ransomware' wannacray", http//www.kompas.com, 13 May 2017, accessed on 8 June 2017.

Cole, Eric, "Detect, Contain, and Control Cyberthreats", SANS Institute, June 2015, in https://www.sans.org/.../detect-control-cyberthreats-36187, accessed on 7 June 2017.

"Catatan Trend Micro Tentang Ancaman Siber di Asia Pasifik", http://www.antaranews.com, 17 June 2015, accessed on 7 June 2017.

Indrajit, Richardus Eko, "Enam Aspek Menjaga dan Melindungi Dunia Maya", from IDSIRTI (Internet and Infrastructure/Coordination Center) Indonesia, http://www.idsirtii.or.id/doc/IDSIRTIIArtikel6_aspek_menjaga_dan_melindungi_dunia_maya.pdf, accessed on 7 June 2017.

"Intel AS di Balik 'Ransomware' yang menyerang rumah sakit Indonesia," 13 May 2015, http://www.kompas.com, accessed on 8 June 2017.

"Indonesia Butuh Lembaga Pertahanan Siber", in http://www.republika.co.id, accessed on 8 June 2017.

"Indonesia diusulkan Segera Bangun Sistem Paspor Terintegrasi," in https://www.cissrec.org/, 14 September 2016, accessed on 9 June 2017.

Persada, Pratama D, "Perang Siber Sudah Menjadi Ancaman Serius", dalam http://www.republika.co.id, 17 September 2016, accessed on 8 June 2017.

"TNI AU Perkuat Zona Identifikasi Pertahanan Udara," in http://nasional.kompas.com/, 7 April 2017, accessed on 9 June 2017.

Vinietta, Elsa, "Strategi Operasi Kontra Inteijen Cyber Sebagai Upaya Peningkatan Ketahanan Negara Indonesia", in http://budi.rahardjo.id/files/courses/2016/EL6115-2016-23215130-Report.pdf, accessed on 7 June 2017.

"47 percent of the world's population now use the Internet, study says," http://www.washingtonpost.com, 22 November 2016, accessed on 5 June 2017.

"2016, Pengguna Internet di Indonesia Capai 132 Juta", in http://tekno.kompas.com/read/2016/10/24/15064727/2016.pengguna.internet.di.indonesia.capai.132.juta, 24 Oktober 2016, accessed on 18 July 2017.