Indonesia Cyber Security: Urgency To Establish Cyber Army In The Middle Of Global Terrorist Threat

Rangga Setiawan
Indonesia International Studies Academic Utilization Community Email: ranggasetiawan13@gmail.com

Abstract

This research focused on how on the year of 2030 Indonesia will gain better governance in order to countermeasures terrorist threats, fairer human rights in terms of privacy and security in information and technology, also stronger Indonesia's national cyber security. Cases are taken firstly from nowadays Indonesia social conflict which started from the internet as society's first source of information regardless the validity of information and secondly from Indonesia's foreign policies towards private technology deals. By using the concept of cyber power and national security as paradigm, this research described how Indonesia going securely, equally, rapidly forward in line with globalization opportunities and technology dependencies. While minimizing invalid and provocative information as terrorist threat to Indonesia's sovereignty and integrity by improving the security of intellectual and on-field assets by integrating academia, military aspects and people's contribution to accelerate Indonesia's national potential in cyber security.

Keywords: *Cyber Security, National Security, Human Security*

1. INTRODUCTION

Cyberspace is the digital, the invisible, the intangible frontier between human and the greatest possibilities towards the transformation of the human way of life. Cyberspace provides unlimited space to constructed new world system along with its every single information network. Intellectual and financial assets, the map of land,

sea, and outer space, and human interaction transformed into data that interconnected one another around the world. The cyberspace provides major enhancement on the speed of information exchange, yet the security issues in the physical world also engaged the cyberspace.

Regarding the level of de-pendencies over cyberspace, each stakeholder (i.e. Individuals, Industries, governments) im- proves their cyber security in a different level. Most individuals as cybercitizen used free or paid antivirus to improve their security. On a wider network, industries which required protecting their databases decided to improve their main portal (e.g. satellites, servers, etc.) to ensure the access to their databases are visibly clear and highly controllable. Other than both actors, a government that wields the widest network in a cyberspace mostly concerning cyber security and cyber-attack capability to ensure national cyber security.

National cyberspace, it might be protected, but the question of "what to protect?" explained the value of cyber dependencies, which aligned with cyber security threat (Clarke & Knake, 2010). Indonesia in this regard possesses high rate in cyber dependencies by more than a half of Indonesia's populations (Asosiasi Penyelenggara Jasa Internet Indonesia, 2016) connected to the internet. The number of internet users comes along with the number of vulnerabilities; in this case, the 132.7 million internet users also brought the same number of the possibilities of threat source towards Indonesia cyberspace. The threats might in form of minor disruption such as malware up to exploitation by a hacker or foreign cyber army.

In order to protect Indonesia cyberspace, Ministry of Communi-cation and Informatics of the Republic of Indonesia protected Indonesia cyberspace by adding proxy called "internet positive" in national Internet Service Provider (ISP). The main function of internet positive is to 'move' the user who using internet access from Indonesia ISP and Domain Name System (DNS) who tried to access certain websites that blocked by internet positive into "internet- positif.org". However, there are also Indonesian ISP(s) owned by private or multi-national companies, even though the regulation to blocked several types of websites were directed to all Indonesia ISP(s), but the list and quantity of websites that blocked by each ISP(s) are different. The implementation differences between

private and government-owned ISP make the national interest regarding cyber security become ineffective.

On terms of direct cyber-attack analysis and protection, on 4th May 2007, Ministry of Communication and Informatics of Republic of Indonesia, established an agency called "Indonesia Security Incident Response Team on Internet Infrastructure / Coordination Centre" (ID - SIRTII/CC). The agency has its main role to educate public and strategic sectors and on how to utilize correctly the internet to prevent any 'incident' happens inside Indonesia cyberspace (ID-SIRTII/CC, 2013a). However, the agency's lack of functions to directly intervene Indonesia's cyberspace, and to directly control, manage and counter-attack towards incoming cyber-attack makes ID-SIRTII/ CC only cover small part to fully established strong Indonesia cyber defence system.

The lack of Indonesia's cyber defence also threatened the security of information that affected national security. In the end of 2016, Indonesia was faced one of crucial protest in Jakarta; the issues are mainly about the blasphemy (Budiari, 2016). The main point is the issue was not coming from the mass media; it started from the social media. Only by uploading the edited video in order to create propaganda, the suspect does not need to have a specific background to do so (The Jakarta Post News Desk, 2016). By that approach, it shows that Indonesia still required a lot of protection in cyberspace to filter and executed preventive and penetrative actions towards propaganda.

Therefore, Indonesia's National Cyber security Agency (NCA) initiative announced in 2015 (Parameswaran, Indonesia's Cyber Challenge Under Jokowi, 2015). A year after the announcement of the initiative of NCA, on September 2016 Indonesia announced its plan regarding NCA function to be established and expanded separately on ministries and industries that have cyber security function (Parameswaran, Does Indonesia Need a New Cyber Agency?, 2016). The 2016 announcement showed backwardness in the establishment of strong national cyber security, as when each institution and ministries has their own cyber security sections, each institution will only defending their sectors, but not Indonesia as a whole cyberspace. Though Indonesia faced the uncertainties in the past two years, on February 2017 Indonesia's government

reaffirmed the establishment of NCA along with readiness on infrastructures and human resources (Parameswaran, Is Indonesia Ready for New Cyber Agency?, 2017a) which had previously became the main obstacles to the NCA's establishment. In accordance with the issues of the establishment of NCA, This paper described how Indonesia reduced its vulnerabilities by the establishment of NCA.

2. RESULTS

2.1 Indonesia Cyberspace

The internet in Indonesia mainly used to broaden users' knowledge, proven by 132 million cybercitizens, 25.3% of them are using the internet by the reason to be up-to-date towards newest issues. However, differentiate between valid and invalid information has become ignored matter for the most of the users, proven by 129.2 million cybercitizen preferred social media as their main source to gather the information (Asosiasi Penyelenggara Jasa Internet Indonesia, 2016). To be noted that most social media are using crowdsourcing system, a system to ask and solve a problem using information gathered by public (Hsu, 2013). Indeed not all sources from social media and crowdsourcing system are invalid, yet the number of invalid information also cannot be underestimated.

Furthermore, social media becomes the information conflict zone, it may be regarded as 'psyops' or psychological operation, it has the role to shape an idea to construct preferred outcome through the spread of information (Clarke & Knake, 2010). E.g. crowdsourcing system that becomes the major information's source for Indonesian students; the Wikipedia (Asosiasi Penyelenggara Jasa Internet Indonesia, 2016). Anyone regardless the intention might use Wikipedia as the vessel to spread the information. Without strong cyber defence, Indonesia cannot prevent the spread of invalid information that possibly contains propaganda content that might threaten Indonesia's national security.

By the number of cyber-attack happened in Indonesia cyberspace, in 2013 Indonesia has been attacked by 42 million intrusions (ID-SIRTII, 2013b) that make Indonesia marked by The Diplomat News as "one of the world's most vulnerable countries to cyber-attacks" (Parameswaran, What Will a New Indonesia Cyber Agency Mean?, 2017b). While the

Indonesia's cyber security is still close to zero in minimizing the number of cyber-attack, the number of Internet user in Indonesia grows rapidly from the number of telecommunication devices, which 'easily' enter Indonesia's market (Widiartanto, 2016).

In the beginning of the establishment of NCA, Indonesia will begin to enter the realm of the cyber warfare. Nation's cyberwar strength might be regarded from three sectors; cyber offensive, cyber dependence, and cyber defence (Clarke & Knake, 2010). Indonesia cyber offensive capability ranked close to zero as the capability and capacity to deliver coordinated nation-based cyber-attack will only available with the establishment of NCA. Indonesia cyber dependence with 132 million users who are depending on cyberspace makes Indonesia assigned in the lowest mark in the middle of South-east Asia countries (Kemp, 2017). Indonesia cyber defence marked with a middle score as the high number of cyber-attack addressed to Indonesia cyberspace (Parameswaran, Does Indonesia Need a New Cyber Agency?, 2016) should provide Indonesia's NCA with various framework to improved Indonesia cyber defence system. Yet, to obtain a higher mark on cyber defence, Indonesia's NCA should able to 'control' (Clarke & Knake, 2010) all internet network across Indonesia cyberspace under government authorization.

2.2 Indonesia's Cyberspace Threat

Cyberspace not only has the capability to create more space than physical world, but also have the capability to 'renew' the relation between government, organization, and individual regarding the security dilemma. The traditional concept of security dilemma by Robert Jervis (Jervis, 1978) shows the dominance of state-level relation in a security dilemma. On his writing, Jervis showed a clear border between state and non-state actor regarding their role in national security. However, the border become blurry when the concept of security dilemma applied to observed security dilemma in cyberspace. Figure 1 shows the possibilities of threat just from two Domain Name Systems (DNS) which one domain normally represent one state's cyberspace, each actor might carry the threat to any other actors, and the limitation to carrying any threats only limited by the capability of the actor itself.

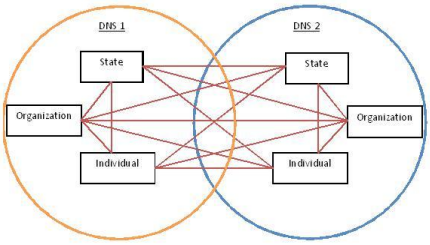

Figure 1: Threats possibilities that delivered and possessed by each actor

The complexity of security dilemma in cyberspace also affected by new security's dispositions that exclusively appear in cyberspace:

1. the smaller actor might have the same or more cyber power than the bigger actor (Nye, 2010).
2. The actor who brings the threat might not appear in the physical world. 3. Threat level also might be kept hidden until the software has been delivered and activated (Clarke & Knake, 2010). 4. The attackers also able to use other actor internet protocol (IP) address to deceive their native address (Lee, 2013). 5. Each actor may use other actors' infrastructures willingly or by force, a single unit or multiple units simultaneously in order to deliver the threat (Syverson, 2013).
6. Physical infrastructure that have the possibility to be control from cyberspace, possess the same threat level as the insecurity of databases.
7. The complexity will increase in corresponding to the appearance of new IP address in a DNS.

One of the major threats to current Indonesia's cyberspace is the global terrorist organization, which utilizes internet to attack Indonesia's cyberspace. In cyberspace, terrorism might be in the form of information and or system disruption. Despite the fact that terrorist organization already constructed a strong digital network, their network and capability improve as the computing, information, and communication technologies improved (Hsu, 2013). The improvement of cyberspace's infrastructure will affect every actor in it who able to access the facilities both legally and illegally.

In facing terrorist group that grows in a cyberspace, a country without cyber security sector will gain disadvantages. The integration between a terrorist group, high economy capacity, and cyberspace capability cannot be underestimated. In some cases, terrorist groups might have lack in infrastructures and capabilities regarding networking, information and communication technologies (NICT) (Hsu, 2013); however, as long as they have high economy capacity, they might rent hacker or a team of hacker as mercenaries to deliver cyber-attack (Clarke &

Knake, 2010).

A year before the announcement of the NCA initiative; in 2014, Indonesia's cyberspace already become the 'nest' of global Islamic-State (IS) terrorist network, led by Santoso, the terrorist's recruitment, and threats were spread through Indonesia's cyberspace via video and terrorist's websites (Sangadji, 2016). A year after the first video, Santoso sent another threat via a voice-record file which spread through Indonesia's cyberspace (Hawley, 2015). That insecurity provide clear overview over how global terrorist threat disrupt national security through cyberspace, also shows the lack of cyber security might decreasing national security.

As the capability to deliver the cyber-attack come into consideration, Indonesia requires more than a secure cyberspace to claim strong cyber security. The function to penetrate suspected attack sources and the function to counter- attack the source of threat become the crucial functions of NCA. Yet, regardless the cyber offensive capability, Indonesia's NCA expected to be able to deliver effectively what so called cyber power (Nye, 2010).

2.3 *Cyber Power and Authorizations*

Cyber power defined as the ability to obtain preferred outcomes through cyber domain. The capability of cyber power rest upon a set of resources that relate to the creation, control, and communication of infrastructure, network, software and human skill, yet the behaviour of the implementation of cyber power rest upon the government's policy and NCA's functions. Through cyberspace, NCA expected to be able to produce preferred outcomes within cyberspace and other domains (Nye, 2010), while interconnected with the physical instrument.

By the aim and range of protections, there are three objectives to implemented cyber power: 1. to change the outcome of an action, 2. to change the action, 3. to construct ideas to produce the preferred outcome (Nye, 2010). For example of the first objective, when Indonesia disrupted by provocative information, Indonesia's NCA able to make a decision to penetrate the source and implemented new cyberspace restriction. For the second objective, Indonesia's NCA must able to deliver system disruption and physiological operation to the suspected websites

and or network with the objective to minimize and or eliminate the threat. For the third objective; Indonesia's NCA able to used cyberspace to trigger an idea to raise nationalism in order to lower the idea that might threaten national security.

As mentioned before, one of the factors that affected cyber power implementation is the human skill (Nye, 2010) which also becoming one of the obstacles in the establishment of Indonesia's NCA (Parameswaran, Does Indonesia Need a New Cyber Agency?, 2016). By the fact that the cyber power capacity cannot make up for a bad intellectual (Clarke & Knake, 2010), therefore, understanding regarding cyber security become necessities for every actors.

Furthermore, the construction in behaviour and characteristic of Indonesia's NCA in terms of cyber offensive and defence become crucial. The cyber defence policy might decide either to restrict Indonesia's cyberspace to protect their cybercitizen like China and it's "Great Fire Wall of China" (Clarke & Knake, 2010) or to set cyber security and defence as the main sector to be developed like U.K and it's National Cyber Security Centre (NCSC) (Corera, 2017). In terms of cyber offensive policy, it might decide either to fully assigned cyber power into a military sector like U.S. and their cyber warriors, or to utilize hacker and cybercrime network like Russia and it is every single nongovernmental and cybercrime enterprises (Clarke & Knake, 2010). Yet, to decide the best behaviour for Indonesia's NCA might come from the combination thereof.

To obtain what so called "optimum security" (Baldwin, 1997), the establishment of NCA should form by every single stakeholder which have a correlation with Indonesia's cyber security. This paper merged the stakeholders into several sector classifications: scholars, military, intelligence service, law, government and public sector.

Scholars have the main role as offense system programmer and defence system developer, to make a system for "zero-day-exploit" and "zero-day-update" (Clarke & Knake, 2010). The military has the main role to consider the strategic plan to implemented NCA's cyber power. Under military's command and their cyber army, the team of field operation should able to operate any smart weapon and used it as a whole interconnected operation between cyber and field operation.

Intelligence services needed to analyse and provide information in any physical and physiological threats towards Indonesia's national security. Law hereby expected to provide the diplomatic act to cover the need of each cyber operation both domestically and internationally. The widest role assigned to the Government and public sector, which expected to provide clear and quick access related to vertical authorization while providing cooperative response horizontally.

As explained in figure 1, the range of protection and cyber operation of Indonesia's NCA covered domestic DNS and foreign DNS as the area of response to cyber threats. The figure 2 shows how the Indonesia's NCA expected to response towards cyber- attack and implementing hack-back command (Clarke & Knake, 2010).

Start from the attacker attributes; the actor-level might be any and the origins of DNS and its actual position might be set to hidden. Cyber-attack lines of commands are standing still, planted (Clarke & Knake, 2010) in Indonesia cyberspace. The type of intrusion itself depends on the capability of the attacker, most of the foreign cyber warriors are targeting Supervisory Control and Data Acquisition (SCADA) system; a program to control infrastructure such as power plant (Clarke & Knake, 2010). NCA's active function started from the diagnostic stage, as the cyber-attack forensic provides several visible data from current incident. Less than a day, cyber army expected to be able to update cyber defence system to be 'immune' to set of command that used in current cyber-attack. In the other hand, strategic command consists of military and its cyber army are executing cyber operation and field operation. Cyber operation naturally carried by cyber army using the hack-back command to trace the attacker's actual IP address from the intrusion that left by the attacker. Field operation team under military will form a strong coordination between cyber and field army. By the data gathered from the diagnostic stage, the field operation might be executed either domestically or internationally depends on the result of diagnostic. Other than domestic operation, the international operation must through international law and affairs (Sefriani, 2011) which might hamper the operation.

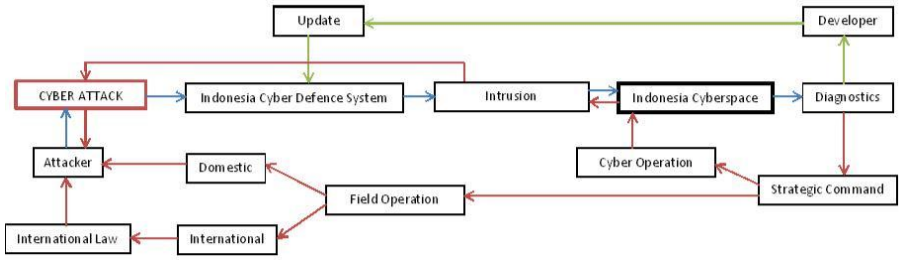

Figure 2: The flow of national cyber security agency's response

Cyber- attack does not only bring out the insecurity and disruption in cyberspace, with a good system management and development in each of NCA's functions, it might become the prime source to prepare strong cyber defence system. The actual implementation of Indonesia's NCA will require a strong communication and fast decision-making process between the related government agencies and NCA to authorize such wide range of operation. By the actualization of NCA functions, Indonesia expected to shape better governance in terms of domestic bureaucracy and national security.

2.4 Indonesia and National Cyber Security Agency

In summary, the establishment of Indonesia's NCA is greatly enhancing Indonesia's national security in the cyberspace domain. The full capacity of cyber security might only obtained by establishing both cyber offensive and defence. In order to obtain such wide range protection, Indonesia's government expected to be able to utilize infrastructures that have established to support NCA's functions.

On the early stage, the contra-movement towards NCA is the side effect that has to be expected. The most crucial might come from the Indonesian or foreign hackers. The government websites and system information might become the primary early target, yet, to prevent such movement happened; Indonesia should start building the positive image of NCA towards Indonesia hacker and programmer communities. Need to be noted that the capacity of Indonesian hackers was already sufficient to deliver major disturbance in 2008's Ambalat cyber war (Madu, 2008). By empowering Indonesia's programmer especially hacker communities, NCA might rapidly meet the requirement of human resource and smart intelligence

(Clarke & Knake, 2010). ID-SIRTII/CC might become the first-line agency in the recruitment of future Indonesia's cyber army, as one of their agenda is to initiate the competition of hacking, cyber forensics analysis, and computer network defence, called "*Cyber Jawara*" (ID-SIRTII/CC, 2016).

Other than empowering the society towards Indonesia's secure cyberspace, NCA also expect to be able to contribute to the enhancement of communication towards Indonesia's archipelago. By covering most of Indonesia's cyberspace, the lack of com- munication considered as the main issues in the enhancement of Indonesia's information technology (IT) (Wibisono, 2015) might obtain a great leap. Not only by the communication that covered Indonesia entirely, but also to control and utilize the number of internet user not to become the disadvantage but to become an advantage towards Indonesia's cyber security.

The advantage might also come from the way Indonesia utilize NCA in order to enhance military and intelligence sectors. Therefore, by the establishment of NCA, both sectors expected to gain more secure communication and working environment. In addition, both sectors have similar role which is preventing and penetrating threat towards national security (Kertopati, 2013), which broaden and strengthen Indonesia's security scope.

There is a major difference between cyber warfare and physical warfare in terms of attack and defence; by obtaining a sword in physical warfare zone, a warrior might defence their territory while having the capability to attack. However, in cyber warfare zone a cyber-army who only developing cyber-attack capability does not make it able to defence their territory (Clarke & Knake, 2010). Therefore, in order to obtain the optimal cyber security, NCA expected to possess a balance cyber capability in defence and offensive.

3. DISCUSSION

3.1 Cyber Attack and Law Enforcement

One of several issues of cyberspace following the establish-ment of cyber security agency is the law enforcement that might face several new cases regarding cybercrime and human rights. In some states that already established the cyber security agency commonly faced those issues i.e. United States (Keck, 2013) and China (Austin,

2014). The issues about law enforcement regarding cyberspace are not only questioning cybercrime, but also the improvement of cyber security which affecting cybercitizen's privacy rights.

The law enforcement issue in cyberspace might appear from the intellectual and monetary assets thievery. In the physical world to enforce a law regarding thievery might done clearly and easily. Yet, the terms of thievery in cyberspace might become more complicated issues, as to steal in cyberspace is only by making an identical copy of the assets without taking the original one from the first place (Clarke & Knake, 2010). Therefore, the national's assets and or confidential information might have stolen without any alarm ringing; in this case, without any proves that something is missing inside the databases, the law enforcement will found difficulties in the advocacy process.

Other than direct cybercrime issues, the law enforcement also faced the difficulty on international-level cybercrime. The international-level cybercrime will required a precise attacker's IP address. Yet, even a country's cyber army able to track down the suspected foreign IP address, the denial towards cybercrime accusation might become the most common statement to directly hid the action (BBC, 2017). Which mean the cybercrime law enforcement in the international-level will found a 'dead end' in terms of direct problem solving.

Despite the issues of law enforcement in cyberspace, the needs to establish Indonesia's NCA become urgently necessary regarding it produces much stronger and independent cyber security environment. However, the establishment of NCA makes Indonesia's cyberspace closely watched by the authorities, which aligned with the reduction of digital privacy of Indonesia's cybercitizen. Yet, it required securing cybercitizen's intellectual and monetary assets from the exploitation of foreign cybercriminal and cyber army.

3.2 Indonesia Collaboration Challenge

In the process of the establishment of Indonesia's NCA, the government should take into account the value of national interest and the cooperation between the institutions and agencies. Remembering tight cyber security regulations must enforced towards communication companies in order

to completely protecting Indonesia's cyberspace.

The establishment of Indonesia's cyber army might bring major development in strengthening national security, yet few major changes in infrastructure, military aspects, and national budget are required in order to establish Indonesia's cyber army. Firstly, the infrastructure, the establishment of new agency somehow required the cooperation of other agencies and industries both private and public. It seems easy to formed cooperation between stakeholders, however, to 'let' NCA inspected their cyber databases will require more than trust and higher authorization. Secondly, the military aspect, Indonesian national army, and police required to start securing and put the cyberspace as the fifth domain of defence and warfare (Hsu, 2013) to the national security main agenda. Thirdly, the national budget stability, like the other countries with cyber army capability (i.e. China and United States), Indonesia also expected to encounter national budget issues in the early day of establishment of national cyber security agency (Subcommittee on Intelligence, Emerging Threat and Capabilities, 2014).

In terms of collaboration, the issues occurred on how to increase cyber security while minimally decreases the digital privacy. The question is left with the options of "which risk to take" as when digital privacy rights sharply increase, that will make cyberspace more vulnerable to the hidden terrorist threat like mentioned before. Yet, when cyber security highly increased, the digital privacy might be disturbed due to the deep intervention from the cyber army in order to track down a suspect or to investigate emerging threats.

By crucial early obstacles mentioned above, the solution might come from the cooperation between higher authorities such as ministries, industries and NCA itself. Learning from initiatives of United States' Department of Defence (DOD), which established a specific cyber environment, called Joint Information Environment (JIE) (Subcommittee on Intelligence, Emerging Threat and Capabilities, 2014), JIE are mainly about reducing data centres that regarded as blind spot of cyber security. By merging connection-pipe in a DNS, it expected to sharpen the NCA's role in filtering information (Clarke & Knake, 2010). In this case, JIE is the initiative which carried by U.S.

which in a condition of owning several data centres. Indonesia in the other hand, have the opportunity to not encounter the same problem, by paying close attention to the number of data centres owned by a private or public company or even by ministerial departments.

4. CONCLUSIONS

The establishment of Indonesia's National Cyber Security Agency (NCA) might encounter major issues in terms of resources both human and budget, and the adjustment of Indonesia's cyberspace by the presence of NCA. Yet, the urgent condition of global terrorist threat cannot be underestimated; therefore, the establishment of a cyber-army under NCA become urgently needed. The establishment of NCA expected to cover the function of protection and penetration by producing unique cyber defence system and by providing a necessary cyber-attack capability in order to achieve Indonesia's national interest through cyberspace.

Following the establishment of Indonesia's NCA, to put cyber security, as one of the state's major agenda might become a strategic policy, it is because a decision to improve cyber security will indirectly improve other sectors. As in order to provide NCA with the future cyber-army, it might begin from basic and higher education to start concerning computerization as a major subject. In addition, to improve Indonesia's cyber defence it might approached from the development of infrastructures (e.g. CCTV, satellites, communication tower, etc.).

In terms of synergy between NCA and military, by establishing NCA close with the military sector will enhance the manoeuvre of NCA both physically and digitally. By then, NCA possess the capabilities to response to current cyber-attack, to prevent the upcoming cyber-attack and to eliminate the threat before it delivered major cyber-attack into Indonesia's cyberspace.

By fully integrate diverse expertise and support from cybercitizens; NCA expected to obtain great momentum in its future development to be able to produce balance in the cyber environment both cyber security and security of digital privacy. Indeed to make a flawless synergy and perfect outcome in cyberspace is impossible by regarding the enclave possibilities in each of it. Yet, if Indonesia does not takes major changes or hold any longer regarding the establishment of NCA, the technology gap between

Indonesia and other countries, and between the internet users and cyber defence system will get wider which align with the increase of threats from the cyber domain.

REFERENCES

Asosiasi Penyelenggara Jasa Internet Indonesia. (2016). *Penetrasi & Perilaku Pengguna Internet Indonesia.* Polling Indonesia. Jakarta: Asosiasi Penyelenggara Jasa Internet Indonesia.

Austin, G. (2014). *Cyber Policy in China*. Cambridge: Polity Press.

Baldwin, D. A. (1997, January). The Concept of Security. *Review of International Studies, 23*(1), 5-26.

BBC. (2017). *Russia's Putin calls leaked Trump memos 'utter nonsense'.* Retrieved 04 09, 2017, from BBC News: http://www.bbc.com/news/world-us-canada-38649169

Budiari, I. (2016). *Anti-Ahok rally ends peacefully.* Retrieved 04 02, 2017, from The Jakarta Post: http://www.thejakartapost.com/news/2016/12/02/anti-ahok-rally-ends-peacefully.html

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

Corera, G. (2017). *Cybersecurity: Queen opens centre to protect against attacks.* Retrieved 04 05, 2017, from BBC News: http://www.bbc.com/news/uk-38964996

Hawley, S. (2015). *Jakarta on high alert after video threat from Islamic State.* Retrieved 04 04, 2017, from ABC: http://www.abc.net.au/am/content/2015/s4360874.htm

Hsu, D. F. (2013). Building a Secure and Sustainable Cyberspace Ecosystem. In D. F. Hsu, & D. Marinucci (Eds.), *Advances in Cyber Security* (pp. 1-33). New York: Fordham University Press.

ID-SIRTII. (2013b). *Laporan 2013.* ID-SIRTII. Jakarta: Direktorat Jendral Penyelenggaraan Pos dan Informatika Kementrian Komunikasi dan Informatika Republik Indonesia.

ID-SIRTII/CC. (2013a). *Sejarah Id-SIRTII/CC*. Retrieved 04 02, 2017, from http://www.idsirtii.or.id/halaman/tentang/sejarah-id-sirtii-cc.html

ID-SIRTII/CC. (2016). *Cyber Jawara*. Retrieved 04 02, 2017, from http://jawara.idsirtii.or.id/

Jervis, R. (1978). Cooperation Under the Security Dilemma. *Robert Jervis, 30*(2), 167-214.

Keck, Z. (2013). *Yes, Edward Snowden Is a Traitor.* Retrieved 04 09, 2017, from The Diplomat: http://thediplomat.com/2013/12/yes-edward-snowden-is-a-traitor/

Kemp, S. (2017). *Digital in 2017: Global Overview.* Retrieved 04 03, 2017, from we are social: http://wearesocial.com/blog/2017/01/digital-in-2017-global-overview

Kertopati, S. N. (2013). *Komunikasi Dalam Kinerja Intelijen Keamanan.* Jakarta: PT. Gramedia Pustaka Utama.

Lee, R. B. (2013). Improving Cyber Security. In D. F. Hsu, & D. Marinucci (Eds.), *Advances in Cyber Security* (pp. 37-59). New York: Fordham University Press.

Madu, L. (2008). Ambalat Netwar antara Indonesia - Malaysia, 2005: Refleksi Teoritis Mengenai Hubungan Internasional di Era Internet. In *Global & Strategis* (Vol. II). Yogyakarta: UPN Veteran.

Nye, J. J. (2010). *Cyber Power*. Cambridge: Belfer Center for Science and International Affairs.

Parameswaran, P. (2015). *Indonesia's Cyber Challenge Under Jokowi.* Retrieved 04 02, 2017, from The Diplomat: http://thediplomat.com/2015/01/indonesias-cyber-challenge-under-jokowi/

Parameswaran, P. (2016). *Does Indonesia Need a New Cyber Agency?* Retrieved 04 02, 2017, from The Diplomiat: http://thediplomat.com/2016/09/does-indonesia-need-a-new-cyber-agency/

Parameswaran, P. (2017a). *Is Indonesia Ready for New Cyber Agency?* Retrieved 04 02, 2017, from The Diplomat: http://thediplomat.com/2017/02/ is-indonesia-ready-for-new-cyber-agency/

Parameswaran, P. (2017b). *What Will a New Indonesia Cyber Agency Mean?* Retrieved 04 03, 2017, from The Diplomat: http://thediplomat.com/2017/01/ what-will-a-new-indonesia-cyber-agency-mean/

Sangadji, R. (2016). *Terrorist Santoso only obedient to IS, video reveals.* Retrieved 04 04, 2017, from The Jakarta Post: https://translate.google.com/#id/en/dipimpin

Sefriani. (2011). *Hukum Internasional Suatu Pengantar.* Jakarta: Rajawali Pers.

Subcommittee on Intelligence, Emerging Threat and Capabilities. (2014). *Information Technology and Cyber Operations: Modernization and Policy Issues In A Changing National Security Environment.* Committee On Armed Services House of Representative. Washington: U.S. Government Printing Office.

Syverson, P. (2013). Practical Vulnerabilities of the Tor Anonymity Network. In D. F. Hsu, & D. Marinucci (Eds.), *Advances in Cyber Security* (pp. 60-73). New York: Fordham University Press.

The Jakarta Post News Desk. (2016) . *Buni Yani, uploader of Ahok's blasphemy video, named suspect.* Retrieved 04 02, 2017, from The Jakarta Post: http:// www. thejakartapost.com/ news/2016/11/23/buni-yani-uploader-of-ahoks-blashpemy-video-named-suspect.html

Wibisono, M. (2015). *Tantangan Diplomasi Multilateral.* (M. Keliat, & M. Mas'oed, Eds.) Jakarta: LP3ES.

Widiartanto, Y. H. (2016). *2016, Pengguna Internet di Indonesia Capai 132 Juta.* Retrieved 04 03, 2017, from Kompas.com: http://tekno.kompas.com/ read/2016/10/24/15064727 /2016.pengguna.internet. di.indonesia.capai.132.juta.