Logical Cyber Weapon in National Security: Threat or Requisite? In Indonesia and Australia

Rangga Setiawan
{ranggasetiawan13@gmail.com}

Universitas Pertahanan, Indonesia

Abstract. This research objective is to show the differences between two countries in facing logical cyber weapon in a form of policies differences which forming unique behaviour and impact towards both countries. The background of this paper is based on the emerging new type of weapon, the intangible weapon; cyber weapon. Many governments regarded this weapon as a non-lethal weapon; therefore, they put less or no effort in enhancing the defense architecture to face the threat; until there is a cyber-incident to be learned from. The term 'black swan event' used in this paper as the approach to reduce the gap stated in this paper which is the relation between the cyber incident and the government response. The government acknowledgement regarding 'black swan event' resulting the policy(s) to create a major change in the state's architecture by learning from the major incident that surge the state, in this case, cyber-attack incidents. This paper describes the pattern differences between Indonesia and Australia in responding to the cyber-attack incident as the 'black swan event' to strengthen cyber Defense architecture and/or establishing national agencies.

Keywords: Cyber Attack, National Defense, Black Swan Event.

1 Introduction

This paper is describing the perspective and policies of two neighboring countries; Indonesia and Australia as both countries are uniquely engaged in various cooperation and conflicts while both of them affiliated in the different region along with its organizations. Based on their differences and closeness, Australia and Indonesia construct a unique relation, this paper focusing on their policies in facing cyber challenges. Like any other neighbor, these two countries also had their domestic conflicts both conventional and asymmetric one, few, written in the history books, others, mentioned in the breaking news or even held back for the diplomatic purposes. Despite all conflicts that occurred between those two countries, from a broad perspective, they possess common threats regionally and globally; especially by the unrestrained behaviour of cyberspace and its technology development.

The development in cyberspace is indeed shifting the way people socializing and interacting with tools; while the principle function is still the same, however, "cyber" provides a new platform where everything can proceed in a split second through millions of line of computer codes. The shifting of human interaction with physical technology through digital–cyber–space often called as "digitalization" that formally called as 'digitize' [1]. The rapid development of this platform shift how most sectors works, the sector that creating the human society itself; including its governance and crime [2].

ICIPSE 2019, October 21-22, Semarang, Indonesia

DOI 10.4108/eai.21-10-2019.2294419

When we told a story about the bad and good person in a crime, conflict, or warfare, there is one thing in common for both of them, which is the possession of a weapon. This common perspective usually applied in cyber space to describe what happened with what so called the 'Cyber Warfare'. The relation of actors in a cyberspace who possesses a certain type of weapon forming an action-reaction relation that later shaping a conflict, depends on the size and impact, it might later be called as a warfare. Like other history of battle, there will always two perspectives; one perspective might see this phenomenon as a conflict that harming both systems, and the other might seeing this Cyber warfare as a phase for each system to be upgraded, as it learning from former vulnerabilities.

The technology that used in any form of conflict mostly called a weapon, in this cyber warfare, the weapon called a cyber-weapon; a set of technology that might be used to conduct an offensive operation or defensive one. Cyber weapon divided into three types: first, Logical Weapon that formed from a set of codes that directly harming cyber system or might indirectly harming physical infrastructure. Second, Physical Weapon that regarded as the platform to deliver the cyberattack or the supporting tools and infrastructure to do so. Third, Psychological Weapon regarded as a set of activities through cyber or physical space in a form of information that forms a set of an idea that harming the psychological aspect of the target [3].

Undoubtedly, by the types of cyber weapon mentioned above, it is already covering all aspects as a weapon; it can do harm, resilience itself, and to make a certain outcome in any level of conflict. Recalling the terms of 'struggle for survival' [4], any possession of weapon to ensure survival regarded as the natural behavior of a human, or in this case, a state. The possession of such capability means there is a higher degree of power accumulated in an actor to achieve certain interest. This cyber capability or weapon accumulation or possession called as cyber power. Just like the traditional concept of power, actors use it to achieved certain interest in both domestic and international sphere [5], cyber power, however, used to achieve actors' interests in cyber sphere [6].

The accumulation of power in the sector of cyber is not an agenda that can be prioritize immediately, especially in terms of national budget for cyber defense or development under military sector, while a state must still maintain the power in three military forces i.e. Army, Navy, and Air Force. One of the ways in finding out at military power is by observing the military expenditure. Development in enhancing cyber capacity regarded as an expensive one as there is no tangible prove that shows the result of cyber enhancement, unlike the budget allocation to strengthen conventional military power that bare eyes might see the increase of the weapon accumulation.

Australia and Indonesia in the graph have a contrast differences in terms of defense expenditure and cyber power capacity. Indonesia 2018 GDP compared to Australia is 37.42% lower shown in Figure 1 [7] along with having 72.16% lower military expenditure than Australia in Figure 2 [8]. One of approach to analyze the cause of this difference is by analyzing the urgency of defense sector from each government perspective; this might be approach by seeing the defense or military expenditure by GDP percentage, Indonesia allocated 0.716% while Australia allocated 1.892% that shown in Figure 3 [9]. In the last 10 years, by graph, Australia begin to rose their expenditure by year 2013, while, Indonesia is getting lower defense allocation in the same year Figure 3 [9]. The rise did not happen without any 'trigger', as in the year of 2013 Australia start to concerning their 'brand new' defense capability, which is cyber capability in national defense sectors, that commenced in 2014 [10].

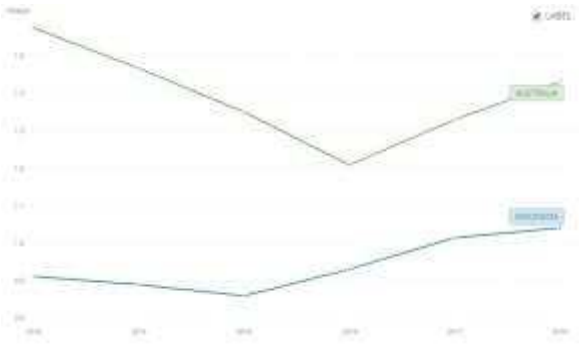

Fig. 1. Growth Domestic Product (GDP) in USD of Indonesia and Australia 2013-2018
Source: World Bank Data (2019).

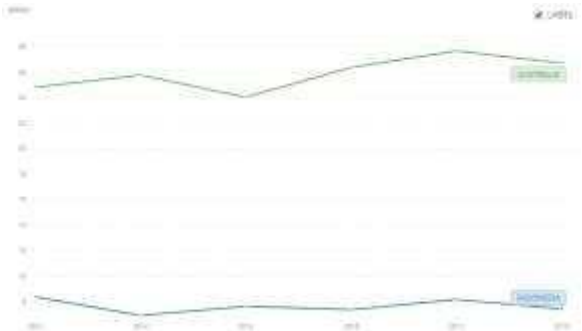

Fig. 2. Military Expenditure in USD of Indonesia and Australia 2013-2018
Source: World Bank Data (2019).

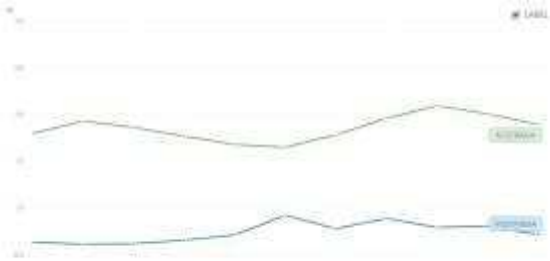

Fig. 3. Military Expenditure in USD of Indonesia and Australia 2008-2018
Source: World Bank Data (2019).

The main concern in above-mentioned statistics is the gap between GDP and military expenditure of both countries, the 37.42% GDP gap, while the military expenditure has a 72.16% gap; this might be the result of different response towards military and defense issues; cyber incident.

There are several cyber incidents in both countries in the last 5 years. Few of the incident is a global-scale incident, therefore both countries affected from the same attack e.g.

WannaCry, which is a ransomware-type malware that attacked both Australia and Indonesia in a minor scale compared to other region Figure 4 [11].

Fig. 4. WannaCry Attack Infection in a world map at 12:20pm, 12 May 2017 [11].

Despite the destructive global-scale cyber incident, the trigger to enhance domestic cyber capability is mainly from domestic cyberattacks. One of Australia wakeup call is the cyber incident of 2016 that attacked Australian Bureau of Statistics (ABS) that initiate the digitalization to do a census, the type of attack is a Distributed Denial of Service (DDOS) attack that causing the system to slow down [12]. The incident considered giving a major impact that internet dubbed it as 'Census Fail 2016' that rising the #censusfail all over social media platform. Indonesia in the other hand, not considered to have a major wakeup call yet; however, Indonesia is actively taking part in global cooperation and summit concerning cybersecurity and rising its concern in cybersecurity by establishing cyber-related agencies.

The different approach of both countries in decision making regarding cyber capability becomes an enigma once it faced with the number of cyberattacks targeted their local system. The data of cyberattack on June-July 2019 shows that Indonesia Figure 5 [13] and Australia Figure 6 [13] received a huge amount of cyberattack daily, except for weekend in both countries.

Fig. 5. Cyberattack with Type of Local Infection in Indonesia
Source: https://cybermap.kaspersky.com/stats/ (2019).

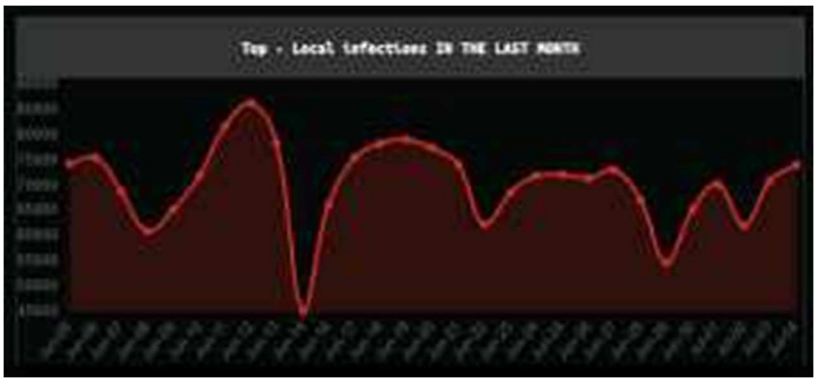

Fig. 6. Cyberattack with Type of Local Infection in Australia
Source: https://cybermap.kaspersky.com/stats/ (2019).

The point that considered as relative in this paper is the decision of a government of Australia and Indonesia in reckoning cyber incidents that emerge in both countries' cyberspace. The decision to consider it as an urgent matter might be affected by the number of attacks, the impact caused by several cyber incidents, or the echo of their people. Those hypothetical points regarded as the aim of finding in this paper.

2 Methods

Methods in this paper constructed from four parts; research methods, research design, analytic methods, and data gathering. These methods also serve as the scope that limited this research to sharpen the result and discussion. All four parts of methods in this research based on the perspective of two experts; Neuman, and Sugiyono.

First, the type of method to construct this paper is Qualitative-Descriptive research. Qualitative research explained as research that used a set of data in a form of words or picture [14]. Descriptive serves as the purpose of this research which trying to create set categories or classify types, and clarify the sequence of stages [14] that on this paper focused on the cyber issues and governance.

Furthermore, based on qualitative type, the design research of this paper is Case Studies that explained as in-depth exploration of a program, event, activity, process, or one or more individuals [15]. This research design is in line with the aim of this research, which is explaining the event that taking the form of policy in a specific activity, which is cyber, also, observing multiple individuals, or in this research seen as actors.

The analytical technique of this paper is an Analytical Comparison, which applying Methods of Difference. This technique explained as the technique of analysis that compares characteristics among cases that focus on the differences among cases [14]. This explanation is indeed in line with the discussion of this paper, which aiming to explore the policy and approach differences between Australia and Indonesia in facing cyberspace issues.

As for the data gathering method, this paper is using Unstructured Interview. Esterberg explains this type as an interview that not following or not using any arranged interview script, yet setting an outline as interview scope [15]. The use of Unstructured Interview is decided based on the process of this research, which going through National Security College (NSC)

short course, Australia National University, which attended by author in June 2019. The data gathering is directly inquiring NSC's experts – ranging from academia to military personnel regarding emerging cyber issues, especially in Australia and her regional.

3 Discussion

The discussion section in this paper – like many other ‘cyber-ish' paper – started with a brief overview of the well-known globalization, the term that having a wide range of meaning to outline the automation era and the information or digital era, which also put up the generation of "millennial". The importance to have a clear understanding of globalization in this paper will provide the fundamental perspective of the actual research locus, the cyberspace.

Just like understanding the physic of winds, therefore physicist can explain how aero plane aviate; the behaviour of globalization could explain how actors are interconnected. To observe the behaviour of globalization, this paper using the term of “borderless world” that seeing globalization as the fading state border [16]. The perspective of the borderless world has constructed based on the issues of global economic and its four characteristics called the four Cs, which are communication, capital, corporation, and consumer [16]. Economics and communication, these two aspects are indeed two of the few fundamental factors that shaping social phenomenon and pattern. Once the discussion goes to social science, therefore, the international relations science also take part in the perspective.

The international relations are truly gain the advantage in terms of technology evolution, especially in terms of diplomacy and the reduction of distance by the enhancement of transportation technology. On the early century of a nation-state, diplomacy did by a person who called a ‘messenger' (that have many terms depends on the kingdom or nation). Messenger has a role to deliver message between kings, or king to the commander in the battlefield; without any transportation, this messenger must travel miles by foot or mounts to deliver the message, whether it is a threat or an alliance request.

The importance of this communication in a time of conflict or peace mentioned in the ancient script of Sun Tzu [17] and ancient Greek [18]. From the beginning of its invention, it has a strong defense mechanism, many of this messenger will act, and protected like a king itself, as it is representing the words of the king or queen. However, with those high protection does not mean this role is threat-free. Many ways to intercept the message from the sender to receiver, either to kill the messenger on his way, replace him, force him to change the message, or even control the messenger from the beginning to gain full control of the relations between any user that employ this particular messenger [17].

The way to do communication has evolved likewise its security. Information security is closely related with algorithmic coding or as we called it as ‘encryption'. Although the first computer invented in 1823; Difference Engine [19], an electromagnetic one was invented by Alan Turning in 1937 [20]. Yet in the perspective of ‘security', this communication technology comes into something that needs to be hacked, one of the first hacking tools was in a World War II called Colossus [20] which have the main function to decrypt German code transmission in WW II. The development as I mentioned before did not merely develop in wartime, following the end of WW II, those technologies created a whole new interconnected network called World Wide Web in 1991 [20].

The historical background of state relation, communication, and electronic technology shows that there is a connection between computing technology and international relations.

Relating to the issues that occur in the process of communication in the ancient era, in a digital era – cyberspace – the issue persists, in fact in the same manners. The international relations issue in terms of cyberspace occurs in between the need for information and its security, this may be called the Digital Divide [21]. In many warfare, even the ancient one, the information availability and credibility have considered as the degree of power and or a powerful strategy [17].

The concept that seeing information as power also take place in cyberspace that called ‘networked power' [22], this new perspective of power will lead to the importance to put information in a form of data that accumulated. The networked power has three criteria, which shift the basic argument of Westphalian sovereignty. First, formless, the action in cyberspace is formless, it could facilitate anyone cyber-attack without any physical form. Second, unstable, this based on the fact that cyber technology is evolving at a fast pace, and one thing that makes it has a rapid evolution is the data. Third, collaborative, the only purpose that the internet was invented, with the rapid communication with a huge number of audience, an idea might become a common purpose, the one that needs bigger attention is the malicious intention [22]. With those three criteria, the threat is not occurring between states; as if Westphalian, yet, the threat towards state sovereignty might come from anyone, even individual level of the attacker, as long as he/she could gather enough data to be exploited.

The reason data considered as power are based on two reasons, first, without or with a ‘dubious' data, a company might fail to conduct calculation of market trend, which therefore suffers loses. Second, from an individual perspective, to have a big amount of data and the ability to process such data will give the user a faster and more accurate decision-making process [23]. The worth of data might explain from various perspectives, one of it is to see it as a set of information that has four characteristics [24]; first, Diverse, data that recorded in a form of number is collected from multiple sectors and covering many aspects. Second, Automatic, the collection of data generated automatically, and it is getting harder not to record our daily data. Third, Time, the usage of data is not static, one might keep raw data and use it in future needs. Fourth, Artificial Intelligence, this what makes automatic and actual data recording a reality, by using one or multiple Narrow Artificial Intelligence, which might become the ‘fuel' to the future Artificial General Intelligence.

Based on the above brief explanation, if data become that valuable and considered as a power, then, the behavior of human towards it might be observed from a perspective of ‘struggle of survival' by accumulating a set amount of power [4]. By this perspective, like any other form of power, the actor who able to accumulate the biggest amount of power dubbed as Super Power. In traditionally, the superpower is a state; is the cyber make this different? the answer is no. Because, once a state decides to have cyber sovereignty [25], then, every data collected by anyone in their grasp is its. For a state, become invincible or ‘secure' is its ultimate goal, based on accumulated power, the hierarchy is constructed, which always followed by ‘insecure perception' between each actor.

As secure is the condition that is pursued by states, therefore, anything degrades security stability must be eliminated. The relations come to power hegemony, where the weaker state cannot execute direct counterwork towards the stronger state, where the threat may come from. Here comes the ‘cyber proxy' as a way to resolve this issue. Cyber proxy considered as a way to ‘show' capabilities, it also means to conceal the attacker's genuine identity [26]. The cyber proxy only possible because of the rapid rise of quality and quantity of machines, internet, and user, as the proxy projected from those three (i.e. attacker might exploit the vulnerability in a machine that carried by specific device, this vulnerability most likely happened by the negligence of the user) [26].

To implement such nation-wide decision is indeed not as easy as write it down in this paper, yet, in order to 'jack-up' awareness of government about the urgency, this paper relates the escalation of user in Australia and Indonesia, by means the higher number of the user means higher number of vulnerable possibilities [27].

The rise of internet user in both countries indirectly suggest that both countries must enhance their cyber capacity, Indonesia have a rise up to 10.12% Figure 7 [28] while Australia have a rise up to 3.6% Figure 8 [29]. The rise is increasing that penetrate in a rate 64.8% out of total population in Indonesia [29]. This paper counts the growth of internet usage as the growth of cyber vulnerability as well. The principle to relate internet user growth and degradation of the state's cyber power is the concept of cyber dependency [27].

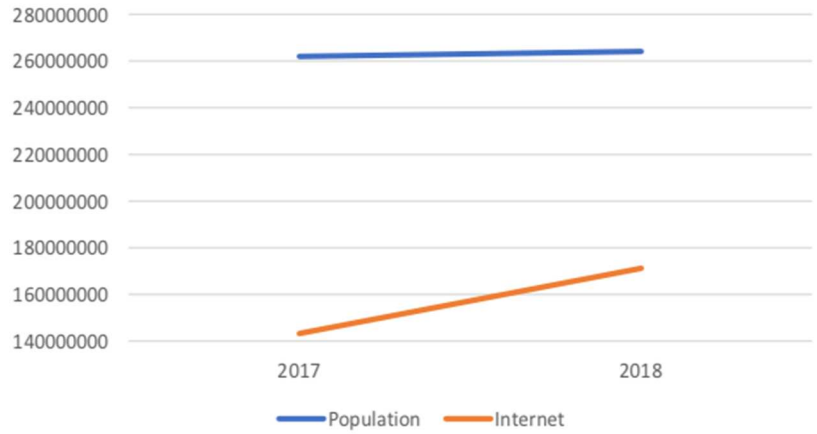

Fig. 7. Indonesia Internet User Population 2017-2018
Source: Indonesia Internet Service Provider Association Survey 2017 & 2018.

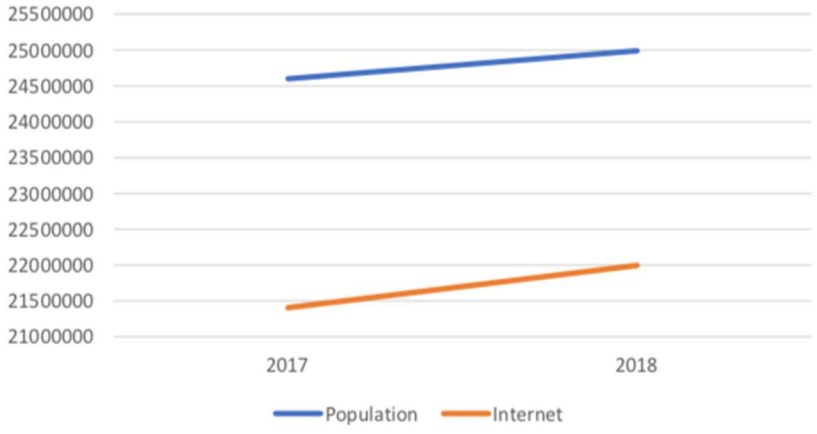

Fig. 8. Australia Internet User & Population 2017-2018
Source: World Bank Data & Christopher Hughes (2019).

The other perspective might not take those growths merely as the vulnerabilities; yet, as a weapon. Related to the usage of proxy by using the user itself, the conversion to gain this power required to give out the user's data, which is supposed to be their privacy – rights [30]. This is where the capacity of the state in keeping the balance between national security and human rights questioned; it might back to question the role of the state itself, to preserve the wellbeing of their people or its security *status quo* [30].

The dilemma between those two questions might stimulate the government to trigger a certain type of movement in cyberspace among their geek to protect the state which also by taking a certain amount of risk in rising "hacktivism". Hacktivism is the terminology for "hacker" and "activism", where the act of activism mostly in political issue delivered via cyberspace by hacking their specific state computer system [31]. Hacktivism might also have considered as the cyber civil disobedience.

The shift civil disobedience to hacktivism has started from 1989, by the spread of Worms Against Nuclear Killer (WANK) in US cyberspace, malware with a type of worm capable to infect a specific type of vulnerability in the random target [31]. For some people, cyber-attack might be considered as a "meh" issue or even a myth, yet, the New York Times dubbed the biggest hacktivism using DDoS (Distributed Denial of Services) in Estonia as the World Wide Web War I (WWWWI) [31]. The crisis caused by the attack successfully changed the Estonian government perspective regarding cyber power and security.

Based on the explained importance of cyber power for a state, it is clear enough that it is a requisite. A state cannot ignore the urgency of a cyber-issue any longer or the state will find it hard to control and catch up with it, even domestically, as the cyberspace and capability of actors in it is developing in the light-speed pace that no other technology is evolving as fast as computer technology. It will be a nightmare for a state when it needs to keep its pace – to gain control – with their own private sectors' technologies.

To awaken the awareness of the government, this paper has observed two different approaches, costly and risky, which serve as obligatory options. The costly one focused on the sector of Research and Development (RnD) e.g. RnD that did by the US that cost a fortune for Indonesia or Australia, to begin with. Therefore, the risky one becomes the only solution, as to put so much weight in the national budget, there must be a strong reason which the word ‘cyber’ is not considered as dangerous as terrorism just yet. To reduce the possibility to raise an excuse to ignore, the risky option might become the finale. The risky option might take a form of a hacktivism that created by a state itself or anyone who concern on it, e.g. by imitating the WWWWI.

The question of the effectiveness of cyberattack as awareness intensifier might be answered by putting the changes in Australia as a learning point for Indonesia. In this paper, the terms used to represent a major change in a country based on its experience in crisis called the "Black Swan Event". Recalling the rise of Australia's military expenditure shown in Figure 1 and the reason behind it. Australia cyber power development manifested in several agencies i.e. Australian Cyber Security Centre, Radicalization Awareness Network, Cyber Ambassador, etc. which in the beginning meant to deal with the domestic cyber threat – the WANK worm mentioned was created by Australian activist group.

Indonesia in the other hand, making its steps in international policies, yet, not much in domestic one, it proven by Indonesia active role in signing and building United Nation's resolution of A/68/98 in 2013 about the field of information and telecommunication in the context of international security that even mentioned in Australian cyber strategy [32]. In the regional scope, Indonesia’s role in establishing the Masterplan on ASEAN Connectivity [33]. The gap between domestic and international policies regarding cyber is the data shown by the

data of Cyber Power Index (CPI). CPI shows that Indonesia is in rank 19 for overall cyber power, yet, by recalling the international role of Indonesia in cyber issues, if domestic policy implemented in the same level, then, Indonesia supposed to have a better position in the index ranking; unfortunately, data shows it is not.

4 Conclusion

In this part of the paper is where the possibility of researching cyber going further, even in the small scope of Australia and Indonesia. The data shows that Australia and Indonesia has a similar growth in GDP, internet user, and the cyber-attack incident; yet, both countries have different conduct to respond to such growth.

This paper concludes that Indonesia required a bigger alarm, an alarm which has louder noise; not a low volume alarm even it beeps many times in many places, it won't woke up Indonesia government. This kind of big alarm might come from a neighboring state or designed by Indonesia itself. This "alarm" metaphor used as in writer perspective, to gain far stronger cyber power all Indonesia need is a total awareness of its government, by actual fear, perhaps.

In hope that there is research to construct a complete scenario of this alarm, this paper will be underlying that scenario as a "white-hat hacktivism" that required for Indonesia to gain so much change through "black swan event". The experience of attacked by the cyber weapon is not a threat; it is requisite for direct changes in national agendas.

With the suggestion of executing "cyber black swan event", this paper remains to have few questions: the calculation of how to control the spread of the malware, and importantly, how far Indonesia must suffer to be awakened. If somehow it is "safe" to sounding such alarm, then, it required the answers: who should take responsibility for such loud sound, which infrastructure to be awakened first, and in the end, is to determine how long and how much it takes to recover from such loud attack. Those inquiries also serve as this research limitation.

References

[1] S. Downing, D. A.; Covington, M. A.; Covington, M. M.; Barrett, C. A.; Covington, *Dictionary of Computer and Internet Terms*. New York: Barron's, 2017.

[2] C. Senker, *Cybercrime and The Darknet: Revealing the hidden underworld of the internet*. London: Sirius, 2017.

[3] J. Andress and S. Winterfeld, *Cyber warfare: techniques, tactics and tools for security practitioners*. Elsevier, 2013.

[4] J. H. Herz, *Political realism and political idealism, a study in theories and realities*. University of Chicago Press, 1951.

[5] H. J. Morgenthau and K. W. Thompson, *Politik antarbangsa*. Yayasan Pustaka Obor Indonesia, 2010.

[6] J. S. Nye Jr, "Cyber power," Harvard Univ Cambridge Ma Belfer Center For Science And International Affairs, 2010.

[7] The World Bank, "GDP (current US$) - Indonesia, Australia," *World Bank Group*, 2019. [Online]. Available: https://data.worldbank.org/indicator/NY.GDP.MKTP.CD?end=2018&locations=ID-AU&start=2013. [Accessed: 27-Sep-2019].

[8] The World Bank, "Military expenditure (current USD) - Indonesia, Australia," *World Bank Group*, 2019. [Online]. Available:

https://data.worldbank.org/indicator/MS.MIL.XPND.CD?end=2018&locations=ID-AU&start=2014. [Accessed: 27-Sep-2019].
[9] The World Bank, "Military expenditure (% of GDP) - Indonesia, Australia," *World Bank Group*, 2019. [Online]. Available: https://data.worldbank.org/indicator/MS.MIL.XPND.GD.ZS?locations=ID-AU. [Accessed: 27-Sep-2019].
[10] Commonwealth of Australia, "2016 Defense White Paper," *Canberra Aust. Gov. Dep. Def.*, 2016.
[11] J. Ashkenas, "Animated Map of How Tens of Thousands of Computers Were Infected With Ransomware," *The New York Times Company, 12 May 2017*, 2017. [Online]. Available: https://www.nytimes.com/interactive/2017/05/12/world/europe/wannacry-ransomware-map.html.
[12] H. Davidson, "The Guardian," 2016. [Online]. Available: https://www.theguardian.com/australia-news/2016/aug/09/the-great-australian-census-fail-of-2016-website-crashes-under-load.
[13] Kaspersky, "Cyberthreat Real-Time Map," *AO Kaspersky Lab.*, 2018. [Online]. Available: https://cybermap.kaspersky.com/stats/. [Accessed: 27-Sep-2019].
[14] W. L. Neuman, *Social Research Methods: Qualitative and Quantitative Approaches*, Fourth. USA: Allyn & Bacon, 2000.
[15] Sugiyono, "Metode Penelitian Kuantitatif, Kualitatif dan R&D," *Alf. Bandung*, 2014.
[16] K. Ohmae, "The Next Global Stage-Challenges and Opportunities in our Borderless World." SAGE Publications Sage India: New Delhi, India, 2008.
[17] L. Giles, *Sun Tzu's The Art of War*. Singapore: Tuttle Publishing, 2008.
[18] K. Hamilton and R. Langhorne, *The practice of diplomacy: its evolution, theory and administration*. Routledge, 2013.
[19] T. Jackson, *Physic: An Illustrated History of The Foundations of Science*. New York: Shelter Harbor Press, 2015.
[20] W. Isaacson, *The innovators: How a group of inventors, hackers, geniuses and geeks created the digital revolution*. Simon and Schuster, 2014.
[21] M. Wibisono, M. Keliat, and M. Mas'oed, *Tantangan diplomasi multilateral*. LP3ES, 2006.
[22] T. Owen, *Disruptive power: The crisis of the state in the digital age*. Oxford Studies in Digital Politics, 2015.
[23] Y. N. Harari, *Homo Deus*. New York: Harper Perennial, 2018.
[24] T. Harkness, *Big Data: Does Size Matter?* Bloomsbury Publishing, 2016.
[25] G. Austin, "Cyber Policy in China, Cambridge, UK, Malden, MA," *Polity*, vol. 26, 2014.
[26] T. Maurer, *Cyber mercenaries*. Cambridge University Press, 2018.
[27] R. K. Knake and R. A. Clark, *Cyber war: the next threat to national security and what to do about it*. The ECSSR, 2012.
[28] Australian Bureau of Statistics, "8153.0 - Internet Activity, Australia, June 2018," *Commonwealth of Australia, 2 October 2018*, 2018. [Online]. Available: https://www.abs.gov.au/AUSSTATS/abs@.nsf/Lookup/8153.0Main+Features1June 2018?OpenDocument.
[29] APJII, "Penetrasi & Profil Perilaku Pengguna Internet Indonesia," *Asos. Penyelenggara Jasa Internet Indones.*, 2018.
[30] H. Farrell and A. L. Newman, *Of privacy and power: The transatlantic struggle over freedom and security*. Princeton University Press, 2019.
[31] P. W. Singer and A. Friedman, *Cybersecurity: What everyone needs to know*. oup usa, 2014.
[32] Australian Government, *Australia's International Cyber Engagement Strategy*. Canberra: International Security & Cyberspace Resource, 2019.
[33] ASEAN Secretariat, "Master Plan on ASEAN Connectivity 2025," *ASEAN Secr. Jakarta*, 2016.