Indonesia’s cyber diplomacy strategy as a deterrence means to face the threat in the Indo-Pacific region

A Fathan Taufik
Indonesia Defense University, Department of Defense Diplomacy, Bogor, Indonesia

Email: fathan.taufik@gmail.com

Abstract. This paper discusses Indonesia's cyber diplomacy strategy as a deterrence means to deal with the threat of cyberspace security in the Indo-Pacific region. Advances in information and communication technology in each country have driven new threats in cyberspace. Indonesia as one of the highest internet user countries in the world is inseparable from the threat of attacks in the cyberspace. The literature method is used to interpret the problem and to present more details in the cyber diplomacy efforts. This literature method approach is used to find perceptions and definitions from various references in relevant contexts and to carry out a process of identifying the defense forces possessed by cyber institutions in Indonesia and the challenges faced in the Indo-Pacific region. Following the circumstances, risk mitigation can be carried out as the basis for developing cyber diplomacy strategies and policies in Indonesia. However, this defense diplomacy strategy may not be effective if it is only carried out in dichotomic by one or two agencies only.

1. Introduction
Emerging in the era of information technology it is important for all aspects of life, let it be an individual, an organization, or even a country, makes the community a must to accept a kind of new world which is called the cyberspace. Unfortunately, the presence of the cyberspace is followed by some negativity that a country must build a cybersecurity capacity as an effort to provide safety and security in the cyberspace. Each country to day start their cybersecurity management system in maximum capacity (Midhio, Reksoprodjo, & Zaelani, 2018). With military activities today entering their fifth domain, the cyberspace, military cyber capabilities are developing rapidly. Those development capabilities is prepared for defensive, offensive, and intelligence operation purposes. Cyber capabilities will certainly become part and parcel of conventional military operations and conventional warfare (Ministerie van defensie, 2012).

Cyber espionage, cyber-attacks, hacktivism, internet censorship and even supposedly technical issues such as net neutrality are now making the headlines on a regular basis. Cyberspace has become a contested political space, shaped by diverging interests, norms and values. As a result of this politicization, diplomats are forced to enter the game. If cyberspace was once a domain for technical discussions among IT specialists only, that era is definitively over (Barrinha & Renard, 2017). The development of Information and Communication Technology (ICT) in the era of globalization has changed traditional warfare with conventional ways to never more used by most countries in the world (Rahman, Anwar, & Sumari, 2015). However, although today, many international community has accepted rules and regulations to govern conventional warfare, there is no common international
agreement as of yet of what constitutes cyber operations, or cyber warfare for that matter (Mueller, 2014).

The role of diplomacy in cyberspace is much less prominent in the media than stories of cyber incidents. A notable exception was the 2015 cybersecurity deal reached between the US and China, one of the most contentious issue in their bilateral relations. For years, both sides had accused each other of network infiltration and of stealing confidential information from companies and government agencies. The US had accused China of stealing or compromising a number of weapon systems, such as the F-35 and the PAC3 missile (Meyer, 2015). For the cases of Indonesia, digital diplomacy has shown a serious challenge following diplomacy practices in the era of President Joko Widodo. Although the idea of using social media for diplomacy can be traced back in early 2000s since its first usage of website, the Jokowi’s administration is the first to declare officially the importance of cyber diplomacy through the Ministry of Foreign Affairs (MOFA) in 2016 (Madu, 2018).

In the past few years the “Indo-Pacific” has increased in using the term in every strategic discussions circulating among the Australian, France, India, Indonesia, Japan and the United States. The term involves treating the Indian Ocean and Pacific Ocean as one maritime zone shaping appropriate foreign, defense, and economic policies (Scott, 2019). At the 2017 Shangri-la Dialogue, there were only five mentions of the ‘Indo-Pacific’ (Choong, 2019). While acknowledging China’s role in this process, I argue that, as a discursive construct, the ‘Indo-Pacific’ is designed primarily to enable the USA and its regional allies to ‘naturally’ strengthen and expand their existing regional alliance networks to hedge against a perceived China-centric regional order in Asia (Pan, 2014). In terms of geo-spatiality, the Indo-Pacific is broadly to be understood as an interconnected space between the Indian Ocean and the Pacific Ocean (Das, 2019). In this article, the focus of the discussion is to examine how cyber-diplomacy strategy needs to be applied by Indonesia in dealing with threats in the field of cyberspace security in the Indo-Pacific region.

2. Defining strategy, cyberspace security, regional security and cyber-diplomacy

2.1. Strategy

The concept of strategy has been adopted from the military to be used in business. In business, as in the military, strategy bridges the gap between policy and tactics. Together, strategy and tactics bridge the gap between ends and means (Nickols, 2016). The use of strategy has existed for many centuries although it has been used today in the management for more than 40 years. Strategy born out of military conflicts and the use of strategy enabled one warring party to defeat another. Von Clausewitz, writing in the nineteenth century, states that the decision to wage war ought to be rational, that is, based on estimates of what can be gained and the costs incurred by the war (Clausewitz, 1982).

Liddell Hart observes that Clausewitz later acknowledged these flaws and then points to what he views as a wiser definition of strategy set forth by Moltke: "the practical adaptation of the means placed at a general’s disposal to the attainment of the object in view (p.334)." In Moltke's formulation, military strategy is clearly a means to political ends (Hart, 1967). George Steiner, Strategic Planning, there, he notes that strategy entered the management literature as a way of referring to what one did to counter a competitor’s actual or predicted moves (p.348) (Steiner, 1979). Henry Mintzberg, in his 1994 book, The Rise and Fall of Strategic Planning, points out that people use "strategy" in several different ways, the most common being these four (pp.23-27): 1) Strategy is a plan, a "how," a means of getting from here to there; 2) Strategy is a pattern in actions over time; for example, a company that regularly markets very expensive products is using a "high end" strategy; 3) Strategy is position; that is, it reflects decisions to offer particular products or services in particular markets; 4) Strategy is perspective, that is, vision and direction (Mitzberg, 1994).

2.2. Cyberspace-security

The word cyber is generally believed to originate from the Greek verb κυβερνέω (kyberneo) to steer, to guide, to control. At the end of the 1940s, Norbert Wiener (1894–1964), an American mathematician,
began to use the word cybernetics to describe a computerized control systems. William Gibson, a science-fiction novelist, coined the term cyberspace in his novel Neuromancer (Gibson, 1984). Science-fiction literature and movies portray the Gibsonian cyberspace, or matrix, as a global, computerized information network in which the data are coded in a three-dimensional, multi-colored form. Users enter cyberspace via a computer interface, where after they can ‘fly’ through cyberspace as an avatars or explore urban areas by entering the buildings depicted by the data.

The word Cyber, as a concept, can be perceived through the following conceptual model (Kuusisto, 2012) : 1) Cyber world: The presence of human post-modern existence on earth; 2) Cyberspace: A dynamic artefactual state formed by bits (vs. static); 3) Cyber domain: A precisely delineated domain controlled by somebody; and 4) Cyber culture: The entirety of the mental and physical cyberspace-related achievements of a community or of all of humankind. Many countries are defining what they mean by cyber world or cyber security in their national strategy documents. The common theme from all of these varying definitions, however, is that cyber security is fundamental to both protecting government secrets and enabling national defense, in addition to protecting the critical infrastructures that permeate and drive the 21st century global economy (Lehto, 2013).

2.3. Regional security
First, regional security emerged as a significant issue in the agenda of superpower dialogue that led to the termination of the Cold War (p.93) (Buzan & Wæwer, 2004). Barry Buzan and Ole Wæwer, Regions and Power, notes that for a decade after the ending of the Cold War, both the remaining superpower and the other great powers (China, EU, Japan, Russia) had less incentive, and displayed less will, to intervene in security affairs outside their own regions (p.3). Because penetration from the global level was so strong, the indigenous regional security dynamics in Southeast Asia are difficult to differentiate, but nonetheless are present and significant (p.134).

Some clarification of our previous statements of RSCT and security theory in general is called for. The original definition of a security complex (Buzan 1983: 106) was: ‘a group of states whose primary security concerns link together sufficiently closely that their national securities cannot reasonably be considered apart from one another’. This story is told as a strong interregional linkage involving a great power and territorial rivalry though, as with the regional level, its dynamics were greatly affected by those of the Cold War (p.138). First, it created divisions within ASEAN about the meanings of the terms in relation to the trade and security links that individual members already had with outside powers (p.142). Using the levels-of-analysis scheme from RSCT to think about East Asian security dynamics during the Cold War produces the following picture. But at the regional level, South, Northeast, and Southeast Asian security dynamics were largely separate. In Northeast Asia an older conflict formation was heavily penetrated by superpower rivalry, though it remained visible in the local securitization rhetoric (p.142).

2.4. Cyber-diplomacy
Diplomacy, understood as “the attempt to adjust conflicting interests by negotiation and compromise” (Wight, 1979). Indeed, for Hedley Bull, diplomacy is “a custodian of the idea of international society, with a stake in preserving and strengthening it” (p.176) (Bull, 1977/2002). According to him, there are five main functions to the diplomatic practice: to facilitate communication in world politics, to negotiate agreements, together intelligence and information from other countries, to avoid or minimize “friction in an international relations” and, finally, to symbolize the existence of a society of states (p.165). It is not even just about relations between states. It now has to take into account “wider relationships and dialogues, involving such entities as regional and international organizations—be they intergovernmental (IGOs) or non-governmental (NGOs)—multinational firms, sub-national actors, advocacy networks, and influential individuals” (Jönsson & Langhorne, 2004).

Now, diplomacy has also progressively extended to new policy areas over the years, entering uncharted political territories such as climate negotiations or, lately, cyber issues. Cyber-diplomacy can be defined as diplomacy in the cyber domain or, in other words, the use of diplomatic resources
and the performance of diplomatic functions to secure national interests with regard to the cyberspace. Such interests are generally identified in national cyberspace or cybersecurity strategies, which often include references to the diplomatic agenda. Predominant issues on the cyber-diplomacy agenda include cybersecurity, cybercrime, confidence-building, internet freedom and internet governance (Barrinha & Renard, 2017). Cyber-diplomacy is therefore conducted in all or in part by diplomats, meeting in bilateral formats (such as the US-China dialogue) or in multilateral fora (such as in the UN). Beyond the traditional remit of diplomacy, diplomats also interact with various non-state actors, such as leaders of internet companies (such as Facebook or Google), technology entrepreneurs or civil society organizations (Barrinha & Renard, 2017).

Diplomacy can also involve empowering oppressed voices in other countries through technology (Owen, 2015). Following our definition, this article focuses exclusively on the latter, whereas the former fits within what could be labeled as “e-diplomacy”. “Digital diplomacy” refers to the use of new technologies and social media by diplomats, in the context of their traditional activities, including for consular purposes (Hocking & Melissen, 2015). According to Tom Fletcher, e-diplomacy was officially born on 4 February 1994 when the then Swedish Prime Minister Carl Bildt sent the first diplomatic email to US President Bill Clinton congratulating him for lifting the embargo against Vietnam (Fletcher, 2016). Much of the debate on new diplomacy has been based on this growing reliance on technology for the fulfillment of diplomatic duties (Copeland, 2015). Related to it, some see in the necessary adaptation to these technologies (and rationale behind them) the key factor in guaranteeing the predominance of state power in an increasingly networked world (Hocking & Melissen, 2015).

Cyber-diplomacy, as we define it in this article, is relatively a new concept. The term had been used before to describe “e-diplomacy” activities. In a 2002 book entitled Cyber diplomacy: Managing foreign policy in the twenty-first century, for instance, several scholars reflected already on the impact of the internet and new technologies on the objectives, tools and structures of diplomacy (Potter, 2002). The term has also been used to describe the evolution of public diplomacy activities in the digital age (Kleiner, 2008).

3. The emergence of cyber-diplomacy today, stakeholders and policies from the government

3.1. The emergence of cyber-diplomacy today

When considering the emergence of cyber-diplomacy, it is important to first understand the underlying logic of cooperation in this policy domain. Cyberspace cumulates a number of characteristics that frame diplomatic engagement among stakeholders. To begin with, it is a global domain connecting nations and citizens worldwide in a variety of manners, generating interactions and frictions between them. Furthermore, cyberspace is usually considered as a “global commons”, defined as a “resource domain to which all nations have legal access” (Buck, 1998). Unlike in other areas of international realm, it is problematic for a state to rely on deterrence by retaliation when it comes to cyberspace, due to problems such as with defining attribution notably, although other forms of deterrence are possible (Nye, 2017).

In World order, Henry Kissinger gives perhaps the clearest reasoning underpinning the rise of cyber-diplomacy, emphasizing that the absence of dialogue and diplomacy would be detrimental to the cyberspace, but also to the broader world order: “The road to a world order may be long and uncertain, but no meaningful progress can be made if one of the most pervasive elements of international life is excluded from serious dialogue. In the absent some articulation of limits and agreement on mutual rules of restraint, a crisis situation is likely to arise, unintentionally creates; the very concept of international order may be subject to mounting strains.” (pp. 345-346) (Kissinger, 2014).

The starting point of cyber-diplomacy is arguably to be found in the publication of the US International strategy for cyberspace in 2011, which is the first government document worldwide to focus entirely on the international aspects of cyber issues. The strategy identifies a number of priorities
(economy, network protection, law enforcement, military, internet governance, international development and internet freedom), while relying on three pillars to pursue these objectives: diplomacy, defence and development (3Ds) (White House, 2011).

3.2. Stakeholders and policies from the government

Various actors, both state and non-state, have the potential threat to disrupt the network because of the difficulty of identifying actors in cyberspace for certain actions and actions in a place that has an effect or impact in all parts of the world (Coucri & Goldsmith, 2012). Furthermore, when viewed from the aspect of crime in the realm of social media, Indonesia ranks 13th in the Asia Pacific region and Japan, and as much as 72.87 percent of fraud in the realm of social media, it turns out that it is spread by users unknowingly (mujalahic, 2018).

Meanwhile, a report from the National Radio News Agency/Kantor Berita Radio Nasional (KBRN) stated that in the second quarter of 2013, Indonesia was the first largest country as the origin of world hit by cyber-attack and, the country with the highest cyber risk (38%) which followed by China in the second place (33%) and the United States in third place (6.9%) (CATRA, 2016). In the case of cyber threats, based on the analysis of the ID-SIRTII (Indonesia Security Incident Response Team on Internet Infrastructure) traffic monitoring system it is noted that the incidence of attacks in cyberspace in Indonesia reaches one million incidents and will tend to increase every day due to system and application weaknesses the unknown. In this case, government institutions are also not immune from cyber-attacks where in the period 1998 - 2009 as many as 2,138 attacks have been addressed to government domain websites.

Distributed Denial of Service attacks on the CCTLD-ID Domain Name Service (DNS) system, ie; “id domain” especially the “.co.id”. Other cases also involved the spread of malwares and malicious codes inserted in files and web sites as well as phishing sites, industrial espionage and the seizure of critical information resources, as well as black campaigns of political parties or defamation of beliefs and spreading hoaxes for the purpose of political provocation and engineering the economy. Due to limited resources and access related to examinations by Indonesian law enforcement agencies to foreign service providers abroad, some of these cases have yet to be resolved even though the ITE Law has set them (Setiawan, 2011). While in a global context, the intensity of cyber-attacks is increasingly high, it can be seen from a series of cyber-attacks as reported by The Telegraph UK, where in May 2017 where there was a cyber-attack WanaCrypt0r 2.0 or commonly referred to as the WannaCry virus spread rapidly in scale massive throughout history at the global level. The virus was initially spread in Ukraine which then spread to 10 other countries within just under two hours, including to Indonesia (Burhanuddin, 2017).

If you look at the global trends, countries like Brazil, Russia, India, China have increased their cyber security. Even cyber war preparation has happened a lot as countries, including in this case Indonesia, also needs to maintain sovereignty in the realm of cyber given that confidentiality, communication between public officials is now entering the digital world (Gera, 2018). In order to respond to these events, Indonesia then formed the Badan Siber dan Sandi Negara (BSSN) as the model of the national cyber security institution. Considering today that Indonesia as one of the emerging country which has become one of world’s largest population country as well as one of the largest internet users in the world. The development of the number of internet users in Indonesia has increased rapidly where in the period June 2017 as many as 132,700,000 to 143,260,000 as of March 31, 2019. Indonesia internet users growth recorded from 2000-2019 is 7.063%.

4. Analyzing strategy

The world conditions faced in today fourth and fifth generation warfare eventually require a deterrence strategy that is different from the previous one. If, the concept of the previous generation warfare is more too conventional and involves more physical contact, then the concept of fourth generation warfare is more in a networked, cross border, and information-based society (Setyawan & Sumari, 2016). Following the situation in Indonesia, the Law No. 11 of 2008 concerning Information and
Electronic Transactions (ITE), rectified. It govern the how to operate in the electronic systems of by both private and government parties in order to protect the availability, integrity, authenticity, confidentiality, and accessibility of electronic information. In addition to the ITE Law, Indonesia cyber security has also been overseen by the Indonesia Security Incident Response Team on Internet Infrastructure (IDSIRTII), the Indonesian Computer Emergency Response Team (ID-CERT), and the Sub Direktorat Cyber Crime Direktorat Tingkat Pidana Ekonomi dan Khusus (Dittipideksus) Bareskrim Polri. Although the policy on cyber security has been regulated through the ITE Law, Indonesia also faces the problem of the distribution of the authority on the role and responsibility whom which to obliged to tackle the cyber-crime, cyber terrorism, cyber hacktivism and cyber warfare.

One of the laws oversees the Lembaga Sandi Negara as a forerunner to the formation of BSSN regulated in the Presidential Decree No. 103 of 2001 concerning the Position, Duties, Functions, Authority, Organizational Structure, and Work Procedures of Lembaga Pemerintah Non Departemen (LPND) with their duties are to carry out governmental tasks in the field of coding in accordance with the provisions of the legislation in force.

Before the formation of the Badan Siber Nasional /National Cyber Agency under the State Intelligence Agency/Badan Intielen Negara (BIN), through the Secretariat General of the National Defense Council/Sekretariat Jenderal Dewan Ketahanan Nasional (Wantannas) on 30 October 2013, the National Siber Security Desk (KSN Desk) was further studied by Wantannas General Secretariat Number K102/Sesjen/X/2013 the Anticipation and Solution of Threats to Cyber Security in order to strengthen national stability. The Coordinating Ministry for Politics, Law and Security of the Republic of Indonesia (Kemenko Polhukam), followed up with the establishment of the National Cyber Information Security and Security Desk/Desk Ketahanan dan Keamanan Informasi Cyber Nasional (DK2ICN) in 2014 based on the Decree of the Minister No. 24 of 2014 dated April 8, 2014 concerning the National Cyber Information Security and Security Desk of 2014.

The Indonesian Armed Forces/Tentara Nasional Indonesia (TNI) under the Indonesian Ministry of Defense, in 2016 also took the initiative to establish the TNI Cyber Agency to secure military assets such as securing missiles and monitoring foreign ships entering Indonesian territory without permission via satellite. The duties and functions of the TNI Cyber Agency are different from those to be formed by the police and law. In order to face the threat of defense that utilizes the development of information technology, the TNI inaugurated the formation of the Cyber TNI Unit/Satuan Siber TNI (Satsiber). Based on Presidential Regulation/Peraturan Presiden (Perpres) No.62 of 2016 concerning Amendments to Perpres No. 10 of 2010 concerning the Organizational Structure of the TNI, the Satsiber is led by the Commander of the TNI Satsiber who is domiciled and responsible to the TNI Commander.

With the existence of problems in handling cybersecurity in the framework of national defense which today is still manage by sectors and not yet well coordinated and not yet fully integrated, in the end, it encourages the government to form the National Cyber and Encryption Agency (BSSN) on May 19, 2017 through Presidential Regulation (Perpres) No. 53 of 2017 concerning the Badan Siber dan Sandi Negara (BSSN). Several other institutions that have interests in the area of national security and defense which include the cyber scope, are ordered to synergized under BSSN. The Ministry of Defense, TNI, Polri, BIN, Ministry of Communication and Information, the National Code Institute, and various related agencies affected (Chotimah, 2019).

Today in Indonesia besides the Ministry of Foreign Affairs that acts as the implementing agency for cyber diplomacy is BSSN. The function as the executor of cyber diplomacy at BSSN will be in the responsibility of the Deputy II of Protection which covers information security governance of equipment, support tools, key management, frequencies, intra networks, and information security audits are carried out as well as cyber diplomacy functions and focal points cooperation. Citing from Indra Rosandry, cyber diplomacy in Indonesia may become effective with the following aspects; first, the existence of cyber threats that have complexity and cross country, requires an international partnership or cooperation with other countries because Indonesia's strategic position as one of the largest internet user countries in the world is an attraction for major powers in the cyber field.
Secondly, cooperation may not only carried out with other countries, but it also needs to involve various elements at the national level both from the public and the private sector. Thirdly, in order to emphasize the orientation of Indonesia's foreign policy and diplomacy, the cyber strategy must have a very vital role. The establishment of BSSN as an executor of the functions of cyber diplomacy and cyber security is a positive move in the efforts to achieve cyber resilience, public service security, cyber law enforcement, cyber security culture, and cyber security in the digital economy. In addition, this is also an investment in addressing the 'power struggle' between major countries in the field of global cyber governance (Rosady, 2018).

5. Concluding remarks
The existence of BSSN as a new institution must be able to coordinate the tasks of various institutions, especially those that handle cyber incidents. Considering that the impact of cyber-attacks is so broad, it is not only a matter of economic loss, but also individual rights to the integrity and sovereignty of the state, the development of cyber defense and security is a necessity for maintaining national security in Indonesia. So, it must be able to form the strategy of Indonesian cyber diplomacy in the Indo-Pacific region.

However, the unclear division of role and responsibility including the working areas of various institutions and institutions relating to the function of the cyber defense and cyber diplomacy will hamper the performance and optimization of Indonesia's cyber diplomacy strategy in dealing with cyber threats in the Indo-Pacific region. The needs of a good integration, synergy, rule of law, and limitations within every institutions including the private sectors in dividing and distributing its role and responsibility to support cyber diplomacy, particularly among related stakeholders is a must.

6. Acknowledgements
Authors wishing to acknowledge assistance or encouragement from the Department of Defense Diplomacy of Indonesia Defense University. The author would like to thank the parties who have helped in this writing activity.

References

[1] Barrinha A and Renard T 2017 Cyber-diplomacy: the making of an international society in the digital age Global Affairs
[2] Buck S 1998 The global commons: An introduction (Washington, DC: Island Press)
[3] Bull H 1977/2002 The anarchical society: A study of order in world politics (3rd ed) (Basingstoke: Palgrave)
[4] Burhanuddin S 2017 Membangun Strategi Pertahanan Cyber di ASEAN. Majalah Masyarakat ASEAN, Edisi 16 34
[5] Buzan B and Waever O 2004 Regions and Power: The Structure of International Security (Cambridge: Cambridge University Press)
[6] CATRA 2016 Dari Desk Cyberspace Nasional Menuju Badan Cyber Nasional. Majalah Setjen Wantannas Edisi VI 16
[7] Choong W 2019 Australian Journal of International Affairs 1-17
[8] Chotimah H C 2019 Cyber Security Governance and Indonesian Cyber Diplomacyby National Cyber and Encryption Agency Politica 10 113-29
[9] Clausewitz v 1982 On War (ed. A. Rapaport) (Penguin: Harmondsworth)
[10] Copeland D 2015 Digital technology ( Oxford: OUP) pp 453-72
[11] Coucri N and Goldsmith D 2012 Bulletin of the Atomic Scientists 68 70
[12] Das U 2019 What Is the Indo-Pacific? Retrieved from thediplomat.com:https://thediplomat.com
[13] Fletcher T 2016 Naked diplomacy: Power and statecraft in the digital age (London: William Collins)

[14] Gera I 2018 LIPI: Dibutuhkan Badan Cyber Nasional Indonesia. Retrieved from Voa Indonesia: https://www.voaindonesia.com/a/lipi-dibutuhkan-badan-cyber-nasional-di-indonesia-2591870.html

[15] Gibson W 1984 Neuromancer (New York: The Barkley Publishing Group)

[16] Hart B L 1967 Strategy, 2nd Revised Edition. Basic Books

[17] Hocking B and Melissen J 2015 Diplomacy in the digital age (The Hague: Clingendael Institute)

[18] Jönsson C and Langhorne R 2004 Diplomacy: Volume III. Problems and issues in contemporary diplomacy (London: Sage Publications) pp 7-8

[19] Kissinge H 2014 World order (New York, NY: Penguin Press)

[20] Kleiner J 2008 The inertia of diplomacy Diplomacy & Statecraft 19 321-49

[21] Kuusisto R 2012 KYBER – miten se voitaisi-inkaan määritellä? lecture 10.10.2012. Helsinki.

[22] Lehto M 2013 International Journal of Cyber Warfare and Terrorism 3 1-18

[23] Madu L 2018 Journal of International Relations 7 11-19

[24] majalahict 2018 Indonesia Butuh Badan Cyber Nasional. Retrieved from www.majalahict.com: http://www.majalahict.com/indonesia-butch-badan-cyber-nasional/

[25] Meyer P 2015 The Washington Quarterly 2 47-61

[26] Midhio I W, Reksoprodjo Y and Zaelani H 2018 Journal of Asymmetric Warfare Study Program 4 77-92

[27] Ministerie van defensie 2012 Defensie cyber strategie. Retrieved from www.rijksoverheid.nl: https://www.rijksoverheid.nl/documenten/brochures/2012/06/27/brochure-defensie-cyber-strategie

[28] Mitzberg H 1994 The Rise and Fall of Strategic Planning. Basic Books

[29] Mueller B 2014 Why we need a cyberwar treaty. Retrieved from www.theguardian.com: http://www.theguardian.com/commentisfree/2014/jun/02/we-need-cyberwar-treaty

[30] Nickols F 2016 strategy: Definitions & Meanings

[31] Nye J J 2017 International Security 41 44-71

[32] Owen T 2015 Disruptive power: The crisis of the state in the digital age (Oxford: OUP)

[33] Pan C 2014 Australian Journal of International Affairs 68 453-69

[34] Potter E 2002 Cyber-diplomacy: Managing foreign policy in the twenty-first century (Montreal: McGill-Queen's University Press)

[35] Rahman A F , Anwar S and Sumari A W 2015 Journal of Defense 5 63-85

[36] Rosady I 2018 Merajut Diplomasi Siber Indonesia. Retrieved from mediaindonesia: https://mediaindonesia.com/read/detail/199360-merajut-diplomasi-siber-indonesia.

[37] Scott D 2019 Asia-Pacific Review 26 29-57

[38] Setiawan A B 2011 Jurnal Penelitian dan Pengembangan Komunikasi dan Informatika Indonesia 2 395-442

[39] Setyawan D P and Sumari A D 2016 Jurnal Penelitian Politik 13 2

[40] Steiner G 1979 Strategic Planning Free Press

[41] White House 2011 International strategy for cyberspace (Washington DC: The White House)

[42] Wight M. 1979 System of states (Leicester: Leicester University Press)