Journal of Strategic and Global Studies

Volume 4
Number 2 *July 2021*

Article 4

7-1-2021

Cyber Intelligence in National Security

Dwi Rezki Sri Astarini
National Resilience, School of Strategic and Global Studies- Universitas Indonesia, dwi.rezki81@ui.ac.id

Muhammad Syaroni Rofii
National Resilience, School of Strategic and Global Studies- Universitas Indonesia, roffi_daun@yahoo.com

Recommended Citation
Rezki, Dwi Sri Astarini and Syaroni Rofii, Muhammad (2021) "Cyber Intelligence in National Security," *Journal of Strategic and Global Studies*: Vol. 4 : No. 2 , Article 4.
DOI: 10.7454/jsgs.v4i2.1044
Available at: https://scholarhub.ui.ac.id/jsgs/vol4/iss2/4

Cyber Intelligence in National Security

Dwi Rezki Sri Astarini[*1] **and Muhammad Syaroni Rofii**[2]

[1,2] National Resilience, School of Strategic and Global Studies, Universitas Indonesia

ABSTRACT

This study discusses cyber intelligence for national security. A country is demanded to be able to master information and communication technology properly and appropriately and appropriately, because the cyber world can be a potential threat and the implementation of cyber security that has not been integrated can have an impact on state sovereignty and national security. Intelligence is used as a tool for early detection of cyber threats that come from within or outside the country. This research is included in the type of descriptive research using a qualitative approach and data collection methods through observation, literature study, interviews and documentation. This study aims to: (1) Determine the position of cyber intelligence in the intelligence field; (2) Cyber intelligence in the management of state intelligence. The results of this study are the role of cyber intelligence as a "new" form in the management of state intelligence can be clearer and avoid problems that may arise. In this case, attention to these issues must be accompanied by a solution in preparing qualified human resources, infrastructure, funds and technology to be able to make cyber intelligence an asset for the interests of national and state security.

Keywords**:** Cyber; Intelligence; Information; National Security.

1. Introduction

In the current era of technology and information development, threats to security are also becoming increasingly complex. Although infrastructure has become increasingly sophisticated to accommodate rapid changes, its existence has placed it in a critical position. Graham (2010) states that this sophisticated infrastructure that was built in modern times is actually vulnerable because it saves the potential for failure which can be fatal because human beings are increasingly dependent on technology that is responsible for the livelihoods of many people. With the increasingly integrated data centers and important infrastructure both physical and non-physical into the technology and global network, in addition to providing easy access and control, it also places new security risks. Among these risks stem from the presence of intrusion threats launched from cyberspace which are able to penetrate the data and information security network systems of these important centers and infrastructures.

At the country level, the existence of cyber threats to security is important to consider. At present, cyber attacks / cyber warfare are considered as very effective media to shake the

[*] Corresponding author : Dwi Rezki Sri Astarini
E-mail : dwi.rezki81@ui.ac.id

stability of the country's security because they have characteristics that are cheap, easy to run, and effectively achieve the expected results (Caplan, 2013). Meanwhile, efforts to create resilience to cyber attacks are more difficult to do due to the interconnection between complex networks which also gives the freedom for actors to hide and carry out attacks from various places on this earth.

The threat of cyberspace is becoming increasingly widespread in terms of the techniques used, the intended targets, and the resulting impacts, thus there is a possibility that one day the country will experience unsafe conditions. A country is in a safe condition as long as the nation cannot be forced to sacrifice the values it deems important (vital). ICT security is a crucial issue that must be fought seriously as a component of national defense, because the main problem facing every country is to build strength to ward off or defeat an attack. The program to improve education and awareness of cyber security is prepared with well-defined targets, but several government organizations carry out programs without any well-integrated coordination, such as the Directorate of Information Security, the Directorate General of Informatics Applications, the Ministry of Communication and Information (Ditkaminfo, Ditjen Aptika, Kominfo), The Indonesia Security Incident Response Team on Internet Infrastructure (ID-SIRTII), and the State Code Institute (Lemsaneg). There is no central connected online portal that is useful for raising cyber security awareness, limited national cyber security awareness campaigns and publicly available materials related to cyber security.

At this time, a number of countries have raised the issue of cyber security as a subject in the national security strategy. For example, since 9/11, the United States government has anticipated this cyber threat by establishing the National Cyber Security Division (NCSD) under the Department of Homeland and Security (DHS) in 2003. In 2015, the United States in its release was related The National Security Strategy also calls for the increasing need for increased cooperation between institutions in order to create resilience against cyber attacks (Bisson, 2015). The same attention is also increasing in European countries. Spain in 2013 issued a National Cyber Security Strategy to anticipate cyber threats which are expected to continue to increase in the future.

Meanwhile, Britain even has a special authority for cyber security, the National Cyber Security Center (NCSC). However, this phenomenon has not been a major focus especially in Asian countries except China. Countries in the Asian region are the target of 80% of cyber attacks from various parts of the world (BBC, 2016; Zheng, 2015). At the same time, although China is one of the major powers in Asia in enhancing cyber security capabilities and its role in cyber attacks, the country is currently experiencing obstacles and constraints that stem from the slow and uncoordinated overall policies related to cyber security (Lindsay, 2015).

Indonesia is one of the countries that are members of the Association of Southeast Asian Nations (ASEAN) faced with the condition of the digital economy in the ASEAN region that has the potential to increase the value of Gross Domestic Product (GDP) in the next few years. However, cyber threats can hamper trust and resilience of the digital economy and prevent ASEAN from realizing digital potential optimally. Countries in the ASEAN region are used as targets of cyber attacks by utilizing vulnerable points of insecure infrastructure. The strategic economic relevance that develops in the region makes ASEAN the main target of cyber attacks, in general because of cyber resilience and the low level of cyber readiness. Specifically, there is no strategic mindset, policy readiness, and institutional oversight related to cyber security. In addition, cyber threats are only considered as an Information and Communication Technology problem rather than a business problem, regional businesses do not have a comprehensive approach in terms of cyber security.
Cyber security governance and policies have not yet been developed in the ASEAN region. The national cyber security strategy has been established by Singapore, Malaysia, Thailand and the Philippines. Several ASEAN countries have formed national bodies tasked with consolidating and coordinating cyber security agendas including Singapore (Cyber Security Agency of Singapore), Malaysia (The National Cyber Security Agency) and the Philippines (Department of Information and Communications Technology). Even though other ASEAN countries do not have a special body, currently the Computer Emergency Response Teams (CERT) or Computer Security Incident Response Teams (CSIRT) play the role of cyber security institutions in several ASEAN countries.

Cyber security has an important role in maintaining information security because it is crucial to safeguard data in the storage media and ensure information sent is safe and to protect information systems against cyber threats. Enhanced protection of information and systems against unauthorized access through confidentiality, integrity, availability of information, non-repudiation, and authentication to avoid cyber attacks. Including providing information system recovery by combining the ability to detect, protect and respond. Cyber security governance in Indonesia is still partial and sectoral so that the handling of cyber security problems has not been integrated or integrated yet. This makes cyber threats even more real, especially when linked to cyber security and resilience threats to the government as a public service provider of the IIKN sector, digital economy actors. Therefore, management of cyber security is absolutely necessary to be integrated to prevent cyber threats in all aspects of national and state life. There are several government organizations dealing with the cyber security component, such as the Coordinating Ministry for Politics, Law and Security (Kemenko Polhukam), the Ministry of Communication and Information Technology (Kominfo), the Ministry of Defense (Kemhan), the State Intelligence Agency (BIN), the Indonesian Armed Forces (TNI), and the Indonesian National Police (POLRI), and the National Code Institute (Lemsaneg) which transformed into BSSN. However, various programs related to cyber security that have been developed and implemented are still at the level of each government agency and there is no formal focal point as the holder of the coordination and development of cyber security in Indonesia.

1.1. National Security Theory

National Security Theory is a general and asymmetrical war theory and communication theory will be used in deeper discussion. Theory of National Security according to Alan Collins (2003) is "*National security is the requirement to maintain the survival of the nation-state through the use of economic, military and political power and the exercise of diplomacy.*"

National security is a need to maintain the resilience of a nation through economic, military and political power and diplomatic expertise. Because of the competitive nature of nations, national security and countries that have significant resource values are based on technical measures and operational processes. This ranged from protecting information relating to State secrets for weapons to the military to strategies for negotiating with other nation states. Therefore, steps must be taken to ensure that state security is maintained.

1.2. Intelligence Theory

Michael Warner (2006) Office of the Director of National Intelligence, in his presentation on Intelligence said that intelligence has many meanings for some people. Interpreting Intelligence into 1 (one) definition will be very difficult to do, there are 2 (two) definitions that are often used in general namely "Intelligence for Decision Makers" and other definitions "Intelligence is the secret activity of a State to understand and influence foreign entities". Quoting Sun Tzu's thought (1963), which added the term "Espionage" in Intelligence, which is a translation of information and action, further there is a doctrine said by Sun Tzu, Intelligence must work in secret "When this type of agent works simultaneously and not some know the method of surgery, they are called "The Devine Skein" and are a treasure for sovereignty.

Hank Prunckun (2010), one of the authors of Intelligence in his book made 4 (four) definitions of Intelligence:

1. Action
2. Knowledge production
3. Organizations that handle knowledge
4. Reports generated from the process or organization

Hank Prunckun also explained in more depth 2 (two) other definitions of intelligence, namely as knowledge and as a process:

a) Intelligence as knowledge: is a body of knowledge, intelligence dealing with enemies, or those who have hostile potentials or operational areas make it possible for knowledge managers to plan and assume organizational direction;

b) Intelligence as Process: is a series of procedures and / or steps, then forms an intelligence cycle / cycle, the cycle runs initially from the emergence of requests for answers to a question and / or requests for suggestions for a problem by the taker decision.

   Intelligence in practical and academic terms is divided into 3 (three) terms:

   1. Knowledge
   2. Activity
   3. Organization

The three things above are input for policies and strategies so that decision makers can determine good attitudes in the form of prevention, deterrence, and mitigation of all existing threats, on the basis of intelligence products in the form of early detection and warning (output) produced. So that what is called Knowledge is the final product of Intelligence in the form of early detection and warning, and hereinafter referred to as Activity is an activity carried out by Intelligence with reference to the cycle process (Intelligence Cycle) both openly and closedly and carried out by an Intelligence Organization.

1.3. Cyber threat

Threats can be conceptualized as any business and activity, both from within the country and abroad that are considered endangering the country's sovereignty, the territorial integrity of the country, and the safety of the whole nation. The concept of threat covers a very broad matter in the form of challenges, disturbances, and obstacles as well as a spectrum that is constantly changing from time to time. The threat to state sovereignty which was originally conventional (physical) develops into multidimensional (physical and non-physical), both from abroad and from within the country. These multidimensional threats can originate from ideological, political, economic, social, cultural and security issues related to international crime, including terrorism, illegal immigrants, narcotics hazards, theft of natural resources, pirates and environmental destruction. Threats can be divided into two, namely military threats and non-military threats. Threats consist of two main components, namely ability and intention. Ability consists of two derivative components namely knowledge and resources, while intention can be measured from two things namely desires and expectations.

Cyberspace is a very dynamic and complex place where personal interests and actions and unintentionality broadly affect a relationship. Cyber as a condition whose main existence in the virtual world is created by the interaction of communication machines, or which is well known as the world wide web (www). Siber is a collection of information and communication technology infrastructure, applications, and equipment on which an organization, company, or mission depends, usually added support in the form of the internet, telecommunications networks, computer systems, personal equipment, and when connected to information technology, sensors, processors, and embedded microcontroller.

Threats are every condition and situation as well as the ability that are considered capable of carrying out actions or disruptions or attacks that are capable of damaging or anything detrimental, thereby threatening the confidentiality, integrity and availability of the system and information. These threats can be intentional because they are planned and / or unintentional such as disasters and threats that emerge from the cyber world. Threats that arise from the cyber world are known as cyber threats. Cyber threats are potential cyber events that can cause undesired results, which result in damage to the system or organization. Threats may come from outside or internal and may come from individuals or organizations. Basically, cyber threats can come from anywhere, in any form, can cause different disturbances to different objects. The threat of cyber is basically a condition in the cyber world whether intentional or not that can cause damage, disruption, loss, and instability in information and communication technology infrastructure

Cyber threats can basically be divided into two groups, namely unintentional and intentional cyber threats. One example of unintentional cyber threats is when updating software or managing procedures that unintentionally damage the system, whereas intentional cyber threats consist of two types, namely targeted attacks (attacks that occur when a group or individual specifically attacks a cyber asset) and the attack is not targeted (the object of the attack is not set or random).

2. Research Methodology

This research uses a qualitative method with a descriptive analysis approach. Qualitative research is researching whose data are expressed in verbal form and analyzed without using statistical techniques. The focus of research is in qualitative methods and that is researched to see the extent to which planned attitudes and policies are able to jellify national security. Research is focused on security vulnerability factors, attitudes and policies.

The process carried out in this study requires time and conditions to change, so the definition of this research will have an impact on the research design and ways of doing it which are also changing or flexible. So, the research conducted is qualitative research with the aim of descriptive research. The qualitative approach chosen by the researchers obtained data derived from literature studies (library research) or literature studies and interviews with informants. This research is analytical descriptive through the collection of detailed data from various sources of information, especially from various sources related to the object of study in this study.

2.1 Data collection technique

As with qualitative research data acquisition procedures, the research data of this research object were obtained from literature studies and interviews. Literature study is intended to obtain data from various references related to the object of study by researchers. While the interview aims to obtain input data from various informants as sources from the academy (including intelligence observers) and practitioners (who have worked and have worked in intelligence services) related to the object of research.

2.2 Position of Cyber Intelligence in the Field of Intelligence

In the world of intelligence, attention to cyber security and the threats posed by cyberspace also need to be prioritized. There are several important conditions that need to be considered in addressing the issue of cyber security in the world of intelligence, is:

1. There is a need for the use of the internet network in obtaining, processing, and storing information and intelligence data so that it requires high security.
2. The need for special abilities in anticipating and detecting cyber attacks (cyber attacks) for the benefit of national security.
3. The need to anticipate new types of threats to state / national security arising from advances in cyber technology such as cyber terrorism

In the field of intelligence, the issue of cyber security also concerns the existence of cyber espionage. The existence of cyber espionage is often difficult to detect because it includes the insertion of viruses, malware, and Trojan horses that cannot be recognized directly (Zheng, 2015). However, this can be anticipated through strengthening cyber intelligence, especially for authorized intelligence agents / agencies. Although the illustration of cyber security shows the vulnerability of the state and society to threats from cyberspace, intelligence can be a media that is not only defensive but also offensive (Brantly, 2013). In this case, the use of cyber intelligence must take a leading role in controlling cyber information that can be utilized for security strategies. Thus, cyber intelligence has the ability to provide input for futuristic decision making and is not always passive for protective purposes.

Cyber intelligence is a form of intelligence activity carried out through computer networks in cyberspace (Andress and Winterfeld, 2014). With the increasing use of information media through this virtual world, Uthoff (2015) states that cyber intelligence must now be an integral part of the intelligence field. Therefore, cyber intelligence naturally occupies a strategic position because of its ability to collect information and data comprehensively from public sources (opensource intelligence / OSINT), social media (social media intelligence / SOCMINT), geospatial (geospatial intelligence / GEOINT), signal (signal intelligence / SIGMINT), and human (human intelligence / HUMINT).

In relation to national intelligence, explicitly in Law NO. 17 of 2011 concerning State Intelligence, it has been stated that state intelligence is the first line in the national security system that carries the role and function of preventing, deterring, and overcoming any threat to national interests and security. This large role and function require extensive and comprehensive intelligence activities including the use of cyber intelligence capacity. On the other hand, the existence of threats to national security from cyberspace activities also requires a high ability of cyber intelligence to ward off attacks through information networks in cyberspace.

But until now, the regulation of security management and resistance to potential hazards from cyberspace has not been the main priority priority. Whereas the level of cyber attacks in Indonesia increased 40% in 2017 and placed Indonesia as one of the countries with a high level of threat of cyber attacks after China (Antaranews, 2018). In observing Indonesia's vulnerability to cyber attacks that can threaten national security, it is necessary to arrange and manage cyber intelligence that has an adequate legal.

2.3 Cyber Intelligence in Governance of State Intelligence

Cyber security governance in Indonesia is still partial and sectoral so that the handling of cyber security problems has not been integrated or integrated yet. This makes cyber threats even more real, especially when linked to cyber security and resilience threats to the government as a public service provider of the IIKN sector, digital economy actors. Therefore, management of cyber security is absolutely necessary to be integrated to prevent cyber threats in all aspects of national and state life. There are several government organizations dealing with the cyber security component, such as the Coordinating Ministry for Politics, Law and Security (Kemenko Polhukam), the Ministry of Communication and Information Technology (Kominfo), the Ministry of Defense (Kemhan), the State Intelligence Agency (BIN), the Indonesian National Army (BIN) TNI), and the Indonesian National Police (POLRI), as well as the State Code Institute (Lemsaneg) which transformed into BSSN. However, various programs related to cyber security that have been prepared and implemented are still at the level of each government agency and there is no formal focal point as the holder of the coordination and development of cyber security in Indonesia. At present there has been an initiative from the government to plan the formation of a national cyber agency that accommodates the need for formal cyber intelligence. However, an important thing that also needs to be discussed is placing the context of cyber intelligence in the management of national intelligence. This is important because it is related to a number of issues.

First, the use of cyber intelligence must produce accurate and quality intelligence information. For this purpose, adequate human and technological resources are needed in collecting and processing intelligence data from cyber media sources. Accuracy is important because, with fast and dense information traffic in cyberspace, careful attention is needed in analyzing existing information. Meanwhile, defensively, this ability is becoming increasingly important in line with the increasing capacity and development of technology used in cyber attacks.

Second, the management of cyber intelligence in the state intelligence agencies in charge must have clear connections and coordination in order to be effectively utilized. The problem of overlapping intelligence information obtained through cyberspace from various institutions must be treated as a triangulation medium to assess the accuracy of intelligence data obtained. In addition, cross-country cooperation in the exchange and distribution of cyber intelligence also needs to be strengthened by taking into account the effectiveness and respecting agreed principles or limits without being trapped in the exchange of intelligence assets that can harm state security.

Third, the use of cyber intelligence needs to avoid conflicts and threats to cyber freedom for individuals and groups that can create an atmosphere that is not conducive to security. The pretext of state security is not the basis for limiting freedom in cyberspace as long as there are clear, democratic, and in accordance with the principles of the right to convey and store information.

Fourth, cyber intelligence activities also need to involve the cyber intelligence community which is driven by non-governmental actors because the government's ability to embrace this community can be a great resource in providing intelligence information. This community has a broad and global informal network and can be utilized for the sake of national security. Conversely, taking a counter position against the community can be a potential threat to the government.

Fifth, adequate use and management of cyber intelligence requires a significant amount of funding. Research reported by Subrahmanian et al (2015) shows that countries with low levels of gross domestic product (GDP) per capita and human development index (HDI) have a higher vulnerability to cyber attacks. Thus, the allocation of funds for the benefit of cyber intelligence must receive important attention as well. Surely this has become a challenge for the government considering the lack of budget for national security needs, especially in the field of intelligence.

To overcome this, it is necessary to examine the level and priority of the main cyber threats as well as the needs of offensive cyber intelligence activities so that funding sources can be allocated to these priority aspects. In the future this need will certainly need to be evaluated given that cyberspace is becoming an increasingly effective and productive battleground with the development of existing technology.

3. Conclusion

Based on the above writing, it can be concluded that the cyber media has vulnerabilities that can be manipulated to threaten national security. So the government needs to take reasonable steps to circumvent cyberspace as a threat to national security. By considering (Andress, 2014) a number of these issues, the role of cyber intelligence as a "new" form in the management of state intelligence can become clearer and avoid problems that may arise. In this case, attention to these issues must be accompanied by a solution in preparing qualified human resources, infrastructure, funds and technology to be able to make cyber intelligence an asset for the interests of national and state security.

Reference

Andress, J. dan Winterfeld, S. (2014). Cyber Warfare: Techniques, Tactics and Tools for Security Practicioners. Waltham: Esevier.

Bisson, D. (2015). A “Cyber” Study of the U.S. national Security Strategy Reports. Diakses Dari https://www.tripwire.com/state-of-security/government/a-cyber-study-of-the-us-national-security-strategy-reports/.

Brahmanian, V.S., Ovelgonne, M., Dumitras, T., dan Prakash. A. (2015). The Global Cyber-Vulnerability Report. Switzerland: Springer International Publishing.

Brantly, A. (2013). Defining the role of intelligence in cyber: A hybrid push and pull. Dalam Mark Phytian (Ed.). Understanding the Intelligence Cycle, pp. 76 - 98. Oxon: Routledge.

Caplan, N. (2013). Cyber War: the Challenge to National Security. Global Security Studies, 4 (1), 93 -115.

Graham, S. (2010). When Infrastructures Fail. Dalam Stephen Graham (Ed). Disrupted Cities: When Infrastructure Fails, pp. 1- 26. New York: Routledge.

Irawan Sukarno, 2011, Aku Tiada Aku Niscaya, Menyingkap Lapis Kabut Intelijen, Buku Obor, Jakarta

Lindsay, J.R. (2015). China and cybersecurity: Contoversy and context. Dalam Jon. R. Lindsay, Tai Ming Cheung, dan Derek S. Reveron (Eds). China and Cybersecurity: Espionage, Strategy, and Politics in the Digital Domain, pp. 1 - 28. New York : Oxford University Press.

Supono Soegirman, April 2013, Etika Praktis Intelijen, Dari Sungai Tambak Beras Hingga Perang Cyber, Media Bangsa, Jakarta.

Undang-Undang No.17 tahun 2011 tentang Intelijen Negara.

Uthoff, C. (2015). Strategic Cyber Intelligence: An examination of Practices across Industry, Government, and Military. Dalam Frederic Lemieux (Ed.). Current and Emerging Trends in Cyber Operations: Policy, Strategy and Practice. Hampshire: Palgrave Macmillan.

Zheng, Y. (2015). From Cyberwarfare to Cybersecurity in the Asia-Pacific and Beyond. Dalam Jon. R. Lindsay, Tai Ming Cheung, dan Derek S. Reveron (Eds). China and Cybersecurity: Espionage, Strategy, and Politics in the Digital Domain, pp. 123 - 128. New York : Oxford University Press.