International Journal Of Engineering Research And Development
e- ISSN: 2278-067X, p-ISSN: 2278-800X, www.ijerd.com
Volume 16, Issue 12 (December 2020), PP. 01-05

Defense Science Philosophy in the Perspective of Technological Risk: The Rising of Cyber Dependency in the Era of Industrial Revolution 4.0

Richardus Eko Indrajit[1], Lilly Wasitova[2,] Marsetio[3,] Pujo Widodo[4,] and Rudy Agus Gemilang Gultom[5*]

[1]*Faculty of Defense Strategy, Indonesia Defense University, Indonesia*
[2]*Faculty of Defense Strategy, Indonesia Defense University, Indonesia*
[3]*Faculty of Defense Strategy, Indonesia Defense University, Indonesia*
[4]*Faculty of Defense Strategy, Indonesia Defense University, Indonesia*
[5]*Faculty of Defense Strategy, Indonesia Defense University, Indonesia*

Abstract: *Dependence on cyberspace is a phenomenon of necessity that occurs in the modern era. The rapid development of information and communication technology has changed various sectors in social life. Regardless of the benefits it provides, the existence of such technology presents its own risks in the world of national defense. The industrial revolution 4.0 which presents various types of technology can endanger the condition of the country if it is developed by the wrong party. The concept of national defense and national resilience must be sensitive to the risks arising from these technological advances. This article briefly describes how defense science needs to take into account the risk of cyber-based technology in the era of the 4.0 industrial revolution that is currently sweeping the world. The content of this article is the result of research using a phenomenological approach to a number of recent global events in the cyber domain.*

Keywords: Cyberspace, defense science, cyber dependency, technological risk, industrial revolution 4.0

Date of Submission: 01-12-2020 Date of Acceptance: 15-12-2020

I. INTRODUCTION

The rapid advancement of technology and information has changed the behavior of human life in various sectors of life. Its ability to break down the boundaries of time and space has resulted in various revolutions in the manufacturing, finance, telecommunications, trade, transportation, education, health and other sectors - including the defense and security sectors [1, 2].

The existence of Indonesia as a country is largely determined by its ability to manage and defend its sovereignty - especially in terms of anticipating and overcoming various threats and at- tacks from within and outside the country. Considering the condition of Indonesia as an archipelago with a geographically dispersed condition, the challenges in managing this sovereign territory can only be answered by the implementation of reliable, robust and high quality technology [3, 4].

In the conventional paradigm of defense of countries in the world, land, sea, and air entities become the focus domain for safeguarding a country's sovereignty. For this reason, there are three major dimensions in the implementation of its doctrinal concepts, namely the Army, Navy and Air Force. Each of these generations has a clear cut scope and parameters in determining the territory of its guardianship - considering that the three domains are mutually exclusive (mutually exclusive) [5].

The various phenomena that occurred after the discovery and application of computer technology presented a new type of arena and warfare model that had never happened before. This invisible war has unique characteristics, so that it cannot only be anticipated or handled using the three-dimensional approach above. This phenomenon, which is often termed cyber war, has a great variety of variances, according to the posture, characteristics and complexity of the features it presents [6].

Asymmetric war or asymmetric war is one such variant. In this war, the two warring sides did not have equal physical strength. Even at the extreme point of an asymmetric war, a country can be overwhelmed when faced with only one per- son. This individual innovatively succeeded in destroying the defense of a country only by using computing devices as his main weapon. The paradigm of attacking without armed forces is the principle used as a philosophical approach in modern warfare [7, 8].

[*] Rudy AG Gultom

Another example is a proxy war or what is often referred to as a proxy war. A fighting model in which the two warring par- ties do not face-to-head but instead use a third party (proxy) as the main stepping stone for their attack strategy [9,10]. The principles of doing politics of fighting against each other, slander, and disinformation are a number of philosophical strategies adopted to win a war.

In line with the increasingly rapid development of internet technology, so many other cyber arena-based war models were born, such as: hoax wars, influence wars, perceptions wars, slander wars, social media wars, infrastructure wars, network wars, and so on. So it is not an exaggeration if some discourses begin to talk about "cyber" as a new dimension that should be considered and given attention to cyber [11].

Indonesia's experience as a nation and a sovereign state that has been around for about 75 years shows that this cyber war phenomenon is not a mere figment, but has come and poses a separate threat to the integrity of the Unitary State of the Republic of Indonesia. In the existing records, there have been several cyber war events between the Indonesian community and the people of other countries such as Malaysia, Australia, America, Israel, China, Russia, and so on. The triggers for the wars that occurred were very diverse, ranging from very fundamental reasons based on idealism, ideology, and fanaticism - to those that were so simple as because of competition in sports, arts, trade, and other humanities matters. So many cyber wars occur between components of the nation in the country, such as:

Several studies and analysis results show that the impact or damage resulting from these invisible wars is very significant. In a number of incidents it even shows the potential that can divide the integrity of the nation and state [12].

II. CYBER DEPENDENCY IN IR 4.0

The rapid development of information and information technology has given birth to a cyber arena that is formed because of the connection between millions of computing resources around the world. Even the placement of sensors on physical objects connected to the internet (read: internet-of-things) has given birth to a new revolutionary era called the Cyber Physical System which colored the birth of the 4.0 Industrial Revolution era [13]. The implementation and use of internet technology in all sectors of public life such as education, health, trade, finance, transportation, distribution, manufacturing, government, and so on (including military and defense) have increased the level of human dependence on the cyber world (read: cyber dependency). The internet is a giant network that is formed from the connection of thousands of computing resource systems on this earth. The virtual arena formed by the existence of this internet network is termed a "cyber world". This cyber has very unique characteristics, namely [14, 15]:

- Social, a place where various diverse individuals meet to communicate, interact, and collaborate;
- Interactive, the occurrence of active multi-way communication between those who are connected to each other virtually;
- Vulnerable, vulnerable or prone to various disturbances due to the gathering of parties with different interests;
- Unregulated, there are no standard rules or regulatory authorities that have the authority to regulate data traffic and communications that occur;
- Anonymous, the tendency to not know the identities of the various parties that interact in the internet ecosystem;
- Global, open freely for all individuals on planet earth to interact without any obstacles;
- Dependent, highly dependent on the availability and reliability of transmission and computing technologies that form the internet ecosystem;
- Insecure, a feeling of insecurity due to virtual interactions with unknown parties;
- Uncontrollable, impossible to control because architecturally built by nodes and networks (paths) that are plural connected (mash);
- Dynamic, growing rapidly because more and more parties are joining and the services offered; and
- Ubiquitous, can be accessed with various digital devices from anywhere and anytime.

In line with the increasing benefits of the internet for human life, there are also high risks associated with it [16, 17]. The value or value of the internet is considered to be getting higher and higher due to the following phenomena:

- The flow of important data and information via the inter- net, such as: credit card numbers, important passwords or passwords, value of money transfers, confidential documents, transaction information, event log files, and so on;
- The proliferation of application platforms in which there are millions of members with detailed data regarding their profiles, identities, preferences, and interaction track records;
- Increasing the number of trading sites and applications (e- commerce) that have high volume and frequency of trans- actions;

- The flood of social media sites connecting thousands of communities and millions of individuals from various parts of the world;
- Allows the internet to be used as a medium for controlling various digital systems or sub-systems, especially those related to internet-of-things technology;
- The explosion of structured and unstructured data (big data) stored in various computing facilities; and so forth.

Of course the high value of the internet and cyber world at- tracts the attention of criminals and cyber criminals [18, 19].

For them, committing crimes on cyber has a number of advantages over the physical world, including:

- It does not require high costs;
- The amount of potential profit or proceeds from crime;
- Relatively easy to implement;
- Rapid execution; and
- The extent of the impact or exposure.

III. CYBER THREATS AND NATIONAL DEFENSE

The biggest risk facing cyberspace is disruption [20]. In principle, the thousands of types of attacks that exist can be classified into 4 (four) groups, based on their modus operandi and goals to be achieved:

- Interception: in the form of attempts to obtain confidential data or information using various wiretapping techniques. Techniques such as spyware, sniffing, man-in-the-middle attacks, etc. are often used as instruments in carrying out this type of attack.
- Interruptions: disruption of service or operation of a sys- tem due to a number of physical or virtual attacks, such as: fiber optic network disconnection, botnet attacks, malware, worms, and so on.
- Modification: the activity of changing the data or content of a message so that the phenomenon of disinformation or misinformation occurs. Examples of this type of attack include: web defacement, SQL injection, trojans, and so on.
- Fabrication: techniques to trick a person or party by impersonating an official institution, for example by means of phishing, social engineering, and so on.

The role or existence of computers or the internet itself can vary in the context of attacks such as:

- The internet is used as a medium for attack, by exploiting it as a giant and massive transmission infrastructure;
- The internet is used as a tool to attack, by using the existing computing resources as a powerful weapon to paralyze various systems and / or steal data;
- The internet is the target of an attack, because then the system or sub-system in it will be disrupted;
- The Internet as an arena where "battles" occur, because this virtual area can bring together various parties who have different interests; and
- Internet as a hiding place or interaction of criminals, especially with the darknet and deep web perimeter.

By considering the various phenomena above, it can be concluded that every institution or industrial sector that has a digital or internet-based system will face a variety of risks, such as: operational risk, organizational risk, reputation risk, and so on. Of all the potential unwanted events, the most feared is if the disturbance has the potential to cause a crisis. Examples of incidents of cyberattacks in other countries that trigger a national crisis in the defense sector are:

- Attacks on the electricity generation and distribution sys- tem which resulted in power outages in the nation’s capital for a long time (total blackout);
- Attacks on nuclear installations that are controlled by digital systems that endanger the surrounding community;
- Attacks on reversible military weaponry programmed to paralyze the owner country;
- Attacks on radar systems of commercial aircraft, which, if occurred, could endanger the lives of thousands of people; and so forth.

Attacks on this system or sub-system clearly have the potential to trigger a national crisis, in the sense that a situation occurs that can endanger the safety, integrity and sovereignty of the nation [21].

IV. CHALLENGES FACING INDONESIA

Moving on from a number of events that occurred in the past, it can be seen that there is a "stuttering" of the state and all components of its entity in dealing with this cyber war phenomenon - especially if the "warring" parties are groups originating from within their own country. This confusion is very understand- able considering the absence of a special doctrine that has been prepared and understood by all components of the nation and government in dealing with this phenomenon [5]. The absence of the same frame of mind in the context of cyber war is evident in the following phenomena:

- It is unclear who should be the main leader or coordinator responsible in case of various variations of cyber warfare at the local and national levels, especially if the "battles" that occur are parallel or simultaneous;
- The absence of standard mechanisms and procedures that must be obeyed by various parties in the event of a war in the cyber world;
- Absence of the same parties and opinion in identifying, detecting, and declaring a cyberwar going on;
- Incomplete instruments and legal instruments which are effective to be used as a basis for preventing and overcoming cyber warfare;
- Lack of solid references as a guide in carrying out strategic processes such as: risk mitigation, impact analysis, potential damage, and so on; and
- The number of parties who "clash with each other" or "shift responsibility" when a cyberwar occurs, especially when it comes to meeting emergency needs such as sharing re- sources, access to special data / information facilities, deployment of institutional professionals, and so on.

In short, the handling of events related to cyber warfare in Indonesia is still incidental and sporadic in nature, far from implementing a structured and systematic process mechanism. If this situation and condition is allowed to be very dangerous to national defense, because it will be exploited by criminals and not responsible for continuing to initiate destructive cyber war- fare [3, 18, 22].

V. DEFENSE PHILOSOPHY AND TECHNOLOGY RISK

State behavior-based ontology of defense always uses a state or nation approach as an object of study. Meanwhile in cyberspace, state boundaries in the context of space and time have collapsed - thus creating the concept of stateless or borderless as its characteristics. In other words, it becomes irrelevant to see defense science as a field of study based on the ability of a country to maintain its existence. The phenomenon of the formation of cross-geographic "new countries" based on ideology, race, class, interest, history, economy, etc. is a new phenomenon that must be studied using a new paradigm [23].

The epistemology of defense science which produces various concepts and theories related to national defense also needs to be reexamined. Recent incidents in the modern war era show how the element of art is more dominant than the scientific aspect - so that the pressure of the concept of defense which was previously oriented to military, management, government and warfare, is now turning to social sciences such as psychology, culture, history, education, and so on [24].

The axiology of defense science has experienced a significant shift. Initially, the principle of the benefits of defense science was emphasized more on determining the right strategy for a country to maintain its existence in the form of sovereignty and the safety of its nation [25]. However, with the emergence of various new phenomena and paradigms, the essence of defense science philosophically has entered into a deeper level, which is to provide an essential explanation to a country regarding its reason for being. Because only then can every individual who is in the social ties of a country be willing to maintain the existence of the country along with the various values and characteristics that exist in it.

ACKNOWLEDGMENTS

The authors would like to thank to the Rector of the Indonesia Defense University, Indonesia for his valuable support to the submission of this paper.

REFERENCES

[1]. Muhammed Zekeriya Gunduz and Resul Das. Cyber- security on smart grid: Threats and potential solutions. Computer Networks, 169:107094–107094, 2020.

[2]. Marina Dobrota, Veljko Jeremic, and Aleksandar Markovic. A new perspective on the ICT Develop- ment Index. Information Development, 28(4):271–280, 2012.

[3]. N K Sa'diyah and R T Vinata. Rekonstruksi Pembentukan National Cyber Defense Sebagai Upaya Mempertahankan Kedaulatan Negara. Perspektif, 21(3):168–168, 2016.

[4]. Anang Setiyawan. The Urgency of Defining Indonesias National Critical Infrastructure. UNIFIKASI : Jurnal Ilmu Hukum, 6(2):164–164, 2019.

[5]. P Campbell. Generals in Cyberspace: Military Insights for Defending Cyberspace. Orbis, 62(2), 2018.

[6]. Jan Rymarczyk. Technologies, Opportunities and Challenges of the Industrial Revolution 4.0: Theoretical Considerations. Entrepreneurial Business and Economics Review, 8(1):185–198, 2020.

[7]. Michael J. Mazarr. The Folly of 'Asymmetric War'. The Washington Quarterly, 31(3):33–53, 2008.

[8]. Peter Hammerstein and Geoffrey A. Parker. The asymmetric war of attrition. Journal of Theoretical Biology, 96(4):647–682, 1982.

[9]. Aniruddha Bagchi, João Ricardo Faria, and Timothy Mathews. A model of a multilateral proxy war with spillovers. Public Choice, 179(3-4):229–248, 2019.

[10]. A Marshall. From civil war to proxy war: past history and current dilemmas. Small Wars Insur, 27(2), 2016.

[11]. Andrew Colarik and Lech Janczewski. Establishing Cyber Warfare Doctrine. Journal of Strategic Security, 5(1):31– 48, 2012.

[12]. S Watts. The notion of combatancy in cyber warfare. Cyber Conflict, CYCON 2012 - Proc, 2012:4–4, 2009.

[13]. J M Riola, C H Fajardo-Toro, J D Reina, O M Torres, and M A G López. Defense 4.0: Internet of battlefield things (IoBT) in naval defense. RISTI - Rev. Iber. Sist. e Tecnol. Inf, 2020(E29), 2020.

[14]. M Lehto. Phenomena in the cyber world. Intell. Syst. Control Autom. Sci. Eng, 78, 2015.

[15]. Milton L Mueller. Against Sovereignty in Cyberspace. International Studies Review, 2019.

[16]. Ahmed Ibrahim, Craig Valli, Ian McAteer, and Junaid Chaudhry. A security review of local government using NIST CSF: a case study. The Journal of Supercomputing, 74(10):5171–5186, 2018.

[17]. Daniel DiMase, Zachary A. Collier, Kenneth Heffner, and Igor Linkov. Systems engineering framework for cyber physical security and resilience. Environment Systems and Decisions, 35(2):291–300, 2015.

[18]. A Subagyo. Sinergi Dalam Menghadapi Ancaman Cyber Warfare. J. Pertahanan Bela Negara, 5(1):89–108, 2018.

[19]. Cyber war: the next threat to national security and what to do about it. Choice Rev. Online, 48(05), 2011.

[20]. S L Hupp, Richard A Clarke, K Robert, and Knake. Cyber- War: The Next Threat to National Security and What To Do About It. Libr. J. VO, 139(8), 2014.

[21]. Yoonyoung Cho and Jongpil Chung. Bring the State Back In: Conflict and Cooperation Among States in Cybersecu- rity. Pacific Focus, 32(2):290–314, 2017.

[22]. R Setiawan. Indonesia Cyber Security : Urgency To Estab- lish Cyber Army In The Middle Of Global Terrorist Threat.

[23]. J. Islam. World Polit, 2(1), 2018.

[24]. Worku Gedefa Urgessa. Multilateral cybersecurity gover- nance: Divergent conceptualizations and its origin. Com- puter Law & Security Review, 36:105368–105368, 2020.

[25]. T Kuusisto and R Kuusisto. Cyber world as a social system.

[26]. Intell. Syst. Control Autom. Sci. Eng, 78, 2015.

[27]. I Mikolic-Torreira. A Framework for Exploring Cyberse- curity Policy Options, 2017.

Richardus Eko Indrajit, et. al. “Defense Science Philosophy in the Perspective of Technological Risk: The Rising of Cyber Dependency in the Era of Industrial Revolution 4.0." *International Journal of Engineering Research And Development*, vol. 16(12), 2020, pp 01-05.