International Journal of Social Science Research and Review

http://ijssrr.com
editor@ijssrr.com
Volume 4, Issue 5
December, 2021
Pages: 18-25

Indonesian Defense Industry Development Strategy as Responses of Cyber Threat to Support State Defense

Rustandi Wiramanggala; Khaerudin; Aries Sudiarso

Indonesian Defense University, Indonesia

http://dx.doi.org/ 10.47814/ijssrr.v4i5.140

Abstract

The condition of the Indonesian defense industry still has many shortcomings, but with the passage of time and a very dynamic strategic environment, the spectrum of threats is rapidly changing. Currently, where the development of information and communication technology is accelerating, cyber threats are the most dangerous threat, as well as for the Indonesian defense industry. Thus, Indonesia must determine attitudes and strategies in developing the defense industry in responding to cyber threats in order to support national defense. This study uses a qualitative method with a literature study approach. The theoretical framework in this research is the theory of development strategy, and the concept of cyber threats. The purpose of the defense industry development strategy in response to cyber threats is to find out the best efforts made by Indonesia using SWOT analysis. It was found that the best strategy in building Indonesian defense industry in responding to cyber threats is the development of the quality of Human Resources and an increase in the budget for research and development of defense industry and technology. This is because some of the obstacles faced are (1) the weak understanding of state administrators related to the cyberspace, and the weak competence of human resources related to soft skills that must be possessed, (2) the weak legal umbrella in handling attacks in the cyberspace. (3) the weakness of the research and development department of the Indonesian defense industry (4) the weakness of the industry in producing and developing hardware with information technology.

Keywords: *Cyber Threat; Indonesian Defense Industry; Development Strategy; State Defense*

Introduction

In the Law of Republic Indonesia No. 16 of 2012 article 1(1), it is stated that the defense industry is a national industry consisting of State-Owned Enterprises and Private-Owned Enterprises, both in groups and individually to produce defense and security equipment, and maintenance services to fulfill strategic interests in the field of defense and security of the *Negara Kesatuan Republik Indonesia*.

In addition, it is stated in articles 3 and 4, that, the purpose of holding a defense industry is to realize the independence of the Indonesian State in fulfilling the defense and security equipment in order to build a reliable defense and security force. Meanwhile, the function of holding the defense industry is to strengthen and make the defense industry independent and increase national economic growth by building strong human resources in the development and utilization of the national defense industry.

However, being in this era of globalization makes the spectrum of threats in the strategic environment more complex, such as the shifting of battlefields that were originally in the real world, now many occur in cyberspace. This makes cyber threats rife both on a small scale such as hacking personal accounts to cyber attacks on government agencies, such as hacking the National Cyber and Crypto Agency of The Republic of Indonesia with the deface method since Wednesday, 20th October 2021 for approximately one week (CNN Indonesia, 2021). This case indicates a weakness in Indonesian cyber defense and security system, and causes demands on the national defense industry to catch up, especially in cyber technology aspect.

Indonesia is required to be able to develop its defense industry in the cyberspace, such as software exploits, zero-days, cyber weaponry, surveillance technologies and related tools for perpetrating cyberattacks.

The term may extend to both grey and black markets online and offline (Applebaum, 2015). More over, these days, traditional arms producers and military services companies such as BAE Systems, EADS, Leonardo, General Dynamics, Raytheon, and Thales have all expanded into the cybersecurity markets (Boulanin, 2013). Some other cyberarms companies include Endgame, Inc., Gamma Group, NSO Group, Birmingham Cyber Arms LTD and Ability. Circles, a former surveillance business, merged with NSO Group in 2014 (Brewster, 2019). Sehingga dapat dikatakan bahwa, walaupun the cybersecurity industry, though still immature, is already important to the defense industry. The 2013 NATO review deemed cyber attacks as one of the greatest risks to defense in the next decade. The military in particular needs better protections of the systems it uses for reconnaissance, surveillance, and intelligence gathering.

Unfortunately, the development of the Indonesian defense industry is still not optimal, for some types of Defense and Security Equipment, they still rely on imported products. On average from 2015 to 2019, Indonesia is in 17th position as the largest importing country for defense equipment. Furthermore, there are several challenges in the development of the defense industry, including limited technology, lack of budget, and the lack of transparency in the procurement process (Aida, 2021: 1). In addition, in efforts to develop the cyber security industry, there are still many obstacles, including:

1) Weak understanding of state officials related to the cyberspace.

2) The low capacity of Human Resources and national industry in producing and developing cyber defense tools, both hardware and software, with existing information technology.

3) There are no regulations that regulate the cyber defense industry. (Edu, 2021).

Therefore, in this research, the researcher analyzes how is Indonesia's strategy in building the defense industry in dealing with cyber threats to support state defense witj considering the current weakness of the defense industry, so that it can provide recommendations to related parties in developing Indonesian defense industry in the cyber realm.

Theoretical Framework

Development Strategy Theory

The development strategy is a way to achieve the Vision and Mission which is formulated in the form of a strategy to boost performance. Performance is strongly influenced by how an organization (government) accepts success or failure from a government organization's mission. The success factors

serve to focus the strategy more in order to achieve the goals and missions of government organizations in a synergistic and efficient manner. To formulate a strategy, a strategic environmental analysis is needed.

Strategic environmental analysis is carried out using the Strength, Weakness, Opportunity, and Threat (SWOT) method, where the Strength and Weakness are used to analyze the internal environment to identify the strengths and weaknesses of various aspects of the Indonesian Defense Industry as a response to cyber threats. Meanwhile, Opportunity and Threat are used to analyze the external environment to identify external factors that influence the development of the Indonesian defense industry in dealing with cyber threats (Dinas Komunikasi dan Informatika Kabupaten Karo, 2021).

Cyber Threat Concept

Cyber threats are actions that have the potential to cause serious problems for computer networks and public security in cyberspace, or even in the real world. In the realm of the state, for example, computerized components are part of critical government infrastructure and are vulnerable to hackers and become targets for cyberattacks. Minor disturbances to system performance can cause significant economic losses (Kovacevic & Nikolic, 2015; Tabansky, 2011). As for entrepreneurs, the most common cyber threats are intellectual property theft and security and data breaches. Meanwhile, in the individual realm, it is necessary to be aware of the risks associated with data theft and the spread of malicious software and viruses (Bendovschi, 2015).

Defense Industry

The defense industry or arms industry is a global business that the participants is engaged in manufacture, sell, and service weapons; military technology, and complementary equipment. They involved in research and development in engineering, producing, and servicing military material, equipment, and facilities. Generally, arms industry provides military aircraft, vehicles, ships, guns, ammunition, electronic system and the complements. But nowadays arms industry is engaged in cyber-warfare as a responses to cyber threat. In other words, arms industry products more narrowly conceived have involved three categories of weapons: land-based weapons, including small arms; naval systems; and aerospace systems, which is in each categories cybersecurity.

Research Methodology

Method and Research Design

This research is about the development strategy of Indonesian defense industry in responding to cyber threats to support state defense. This research uses a qualitative method, where based on the theory by Creswell, in conducting a research with qualitative methods, researchers can identify directly by being involved in informants activities, or by investigating with a narrative approach obtained through a collection of stories of individuals who involved (Creswell, 2013: 225). Qualitative research itself is a research process that takes place systematically. The reason for using qualitative methods in this study is that the primary data in this study involves informants who are considered credible in providing the data and information needed, either through interviews, observation and documentation.

This research use descriptive analysis to collect actual information in detail that describes existing symptoms, identify problems or examine conditions and prevailing practices, make comparisons or evaluations and determine what other people do in dealing with the same problem and learn from experience. them to set plans and decisions in the future (Nurdin and Hartati, 2019).

Discussion

The condition of the Indonesian Defense Industry is influenced by technology, both in order to maintain the security of its data and in industrial development both in terms of raw material processing, and human resources. In other words, there are still many efforts that must be made by Indonesia to build its defense industry in order to achieve Indonesian Defense Industry's independence in 2024.

However, on the other hand, the Indonesian defense industry is also required to adapt to the rapid development of cyber technology. Because of this, to be able to determine strategic efforts in building Indonesian defense industry in response to cyber threats, an appropriate strategy is needed. In determining the strategy, aspects that influence both internally and externally must be considered, for that a SWOT strategy analysis (Strength, Weakness, Opportunity, Threat) is used.

By using SWOT analysis, internal factors which are Human Resources, Technology, and Facilities and Infrastructure were analyzed using Strength and Weakness, while external factors in the which are Strategic Environment Development, Regulations and Policies, and Competence of Policy Makers, were analyzed using Opportunity and Threat.

Internal Factor

a. Human Resources

1) Strenght

The strength that comes from human resources is the quantity of human resources. In addition, the obligation to receive state defense trianing and education is also one of the strengths in building human resources, so they will have competence and nationalism and can help build the defense industry from inside, especially in responding to cyber threats.

2) Weakness

Weaknesses in human resources are, there is still a lack of competent experts in certain jobs related to cyber and defense, this causes the need for trainings that support the competence of human resources in the Indonesian defense industry.

b. Technology

1) Strenght

The strength possessed by the technological aspect is that there are many derivative technologies that can be used for non-military interests. In dealing with cyber threats, the information technology that is owned good enough, so, it can be used to complement the development of the defense industry in responding to cyber threats in the technological aspect.

2) Weakness

The weaknesses are, it is still difficult to do a transfer technology. This is due to the weakness of the research and development department in the Indonesian defense industry, and the developed country who cooperate with Indonesia in transfer technology. The research and developmpment department in Indonesian defense industry is lack of budget and lack of qualified human resources, usually reearch and development department considered as an unimportant place. More over, if we talking

about the transfer technology, not all developed countries are willing to transfer technology fulyl, thus making the Indonesian defense industry still dependent on foreign products. The same thing happened to the cyber technology used both in the manufacture of security and security guard, as well as used in controlling the security of data belonging to companies engaged in the Indonesian defense industry.

In addition, there are still very few companies in Indonesia that are engaged in the cyber field. In addition, the industry that produces both hardware and software in Indonesia is also not yet qualified to be able to compete in the international class.

c. Facilities and Infrastructure

1) Strenght

The Minimum Essential Forces that are applied can be one of the strenght if they are allocated properly, so that Indonesia can use the minimum budget as much as possible. In addition, on November 27, 2019, the Indonesian Defense Industry Association was formed to accelerate the development of the Indonesian defense industry by collaborating between companies engaged in the defense industry. In response to cyber threats, this forum is useful in cooperation related to joint cyber attack countermeasures.

2) Weakness

The budget for the development of the defense industry must be increased considering that the budget provided must be divided into 3 component (Land, Sea, and Air). While the cyber realm is still general in nature, the budget that must be added is to increase supporting facilities and infrastructure to conduct training related to cyber technology, as well as supporting facilities and infrastructure for the development of cyber technology in the defense industry.

External Factor

a. Strategic Environment Development

1) Opportunity

The dynamic development of the strategic environment requires Indonesia to have an independent defense industry is high. Globalization that occurs provides wider access for communication that is hindered by distance in conducting trainings and transferring technology over long distances. In addition, in the development of the defense industry in responding to cyber defense, training materials can be accessed from many sources.

2) Threat

Globalization does not always have a positive impact. The gap of defense technology has made it difficult for the Indonesian defense industry to move forward. But on the other hand, globalization also stimulates a shift in threats, where threats that initially only exist in the real world, also occur in cyberspace.

b. Regulations and Policies

1) Opportunity

Good regulations and policies can be an added value in efforts to develop the Indonesian defense industry in responding to cyber threats. Policies that support the implementation of development and research, as well as ensure the welfare of human resources within the defense industry.

2) Threat

The weak regulation in arrange the cooperation between the government and companies makes trhe accountability related to the production of Defense and Security Equipment is often hampered. In addition, there is no further regulation that regulates strategic steps in building defense infrastructure in dealing with cyber threats for defense industry.

c. Competence of Policy Makers

1) Opportunity

Policy makers who come from all aspects of government, can see the problem from a wider perspective. Of course, this can provide a lot of input to the development of the Indonesian defense industry. In addition, the making of rules and policies can also be considered from a broader perspective.

2) Threat

It is feared that the lack of level of understanding of policy makers regarding the cyberspace will affect the regulations and policies taken, especially related to the cyberspace on the Indonesian defense industry. Considering that there is often a mismatch between the competence of policy makers and the positions held, other than that, policy makers in Indonesia often make decisions without involving experts. Of course, this will be a threat to the development of the defense industry in order to respond to cyber threats, because the regulations needed are not in accordance with what is applied.

Conclusion and Recommendation

Based on the analysis that has been carried out, it is known that in formulating a strategy for the development of the Indonesian defense industry in response to cyber threats, the things that need to be considered are:

a. Improving the quality of human resources, both in the form of soft skills and hard skills. Because soft skills and hard skills are a unity that influence each other, especially soft skills related to the cybespace, such as creativity skills, digital literacy, social intelligence, and a sense of nationalism. So that it can support activities, and prevent unwanted things, such as the growth of destructive cyber spies from within the Indonesian defense industry itself.

b. Facilities and infrastructure, as well as technology are a crucial part in the development of the Indonesian defense industry in responding to cyber threats. However, there are many obstacles faced, such as difficulties in transferring technology from developed countries, lack of funding which leads to neglect of research and development sections in the Indonesian defense industry, which will result in the defense industry being far behind and lack of economic welfare for its human resources. Where human

resources are classified as experts, preferring to serve other state companies which instead build the defense industry of the other country.

In addition, the backwardness of technology makes Indonesia still far behind in creating or applying cyber elements to its Defense and Security Equipment, especially for the Defense and Security Equipment which is useful in conducting espionage activities, border guarding, as well as counter-attack tools that are useful in cyber warfare. In this case, if a cyber attack occurs, Indonesia will only take a defensive stance. For this reason, it is necessary to conduct training in developing hardware and software production by domestic human resources, so that the cyber industry in Indonesia does not depend on other countries.

d. External factors that greatly influence the development of Indonesian defense industry are funding, as well as regulations and policies taken. For this reason, synergies from various main lines are needed, especially in terms of research and technology development. In addition, it is important for users (government) to be able to coordinate with industry players in planning for the needs of Defense and Security Equipment. The procurement of Defense and Security Equipment also needs to have standards that reflect transparency, accountability, and the integrity of industry players. Support through increasing the budget is also needed in the development of the defense industry. Finally, the need for coordination of all relevant stakeholders.

Reference

Aida, Ade Nurul. (2021). Tantangan Pengembangan Industri Pertahanan dalam Mendukung Sistem Pertahanan Negara. Politik dan Keamanan Budget Issue Brief Vol 01,Ed 8, hal. 1-2.

Applebaum, Jacob Von. (2015). NSA Preps America for Future Battle. Retrieved from https://www.spiegel.de/international/world/new-snowden-docs-indicatescope-of-nsa-preparations-for-cyber-battle-a-1013409.html. [29/10/21]

Boulanin,Vincent. (2013). Arms Production Goes Cyber: A Challenge for Arms Retrieved from Control. https://www.sipri.org/node/361. [29/10/21]

Brewster, Thomas. (2019). A Multimillionaire Surveillance Dealer Stepped Out of Shadow and His 9 Million Whatsappa Hacking Van. Retrieved from https://www.forbes.com/sites/thomasbrewster/2019/08/05/a-multimillionaire-surveillance-dealer-steps-out-of-the-shadows-and-his-9-million-whatsapp-hacking-van/?sh=79b1622731b7. [29/10/21]

Bendovschi, A. (2015). Cyber-attacks – trends, patterns, and security countermeasures. *Procedia Economics and Finance*. Doi: 10.1016/S2212-5671(15)01077-1 . [29/10/21]

Byrne, Edmund F. (2017). Arms Industry. Indiana University- Purdue University. Indianapolis: USA. Retrieved from https://philarchive.org/archive/BYRAI. [29/10/21]

CNN Indonesia. (2021). Situs BSSN Diduga Sudah Diretas Hampir Sepekan. Retrieved from https://www.cnnindonesia.com/teknologi/20211026073327-185-712307/situs-bssn-diduga-sudah-diretas-hampir-sepekan. [29/10/21]

Creswell, J. W. (2013). *Research design*: pendekatan kualitatif, kuantitatif, dan mixed. Yogyakarta: PT Pustaka Pelajar.

Dinas Komunikasi dan Informatika Kabupaten Karo. (2021). Strategi Pembangunan. Retrieved from https://www.karokab.go.id/id/profil/strategi-pembangunan. [29/10/21]

Edu, Heylaw. (2021). Pertahanan Siber di Indonesia: Meneropong Tantangan dan Upaya yang Dilakukan. Retrieved from https://heylawedu.id/blog/pertahanan-siber-di-indonesia-meneropong-tantangan-dan-upaya-yang-dilakukan. [29/10/21]

Kovacevic, A., & Nikolic, D. (2015). Cyber-attacks on critical infrastructure: Review and challenges. *Handbook of Research on Digital Crime, Cyberspace Security, and Information Assurance.* Doi: 10.4018/978-1-4666-6324-4.ch001. [29/10/21]

Lineberger, Robin., Faver, Alan D., Gallagher, Kevin., and Lucy, Jefferey. (2019). Cybersecurity in The Defense Industrial Base: Evolving Cybersecurity Regulations for Defense Contractors. Retrieved from https://www2.deloitte.com/us/en/pages/manufacturing/articles/cybersecurity-in-defense.html. [29/10/21]

Nurdin, Ismail and Hartati, Sri. (2019). *Metodologi Penelitian Sosial.* Surabaya: Media Sahabat Surabaya.

Sharma, Sanjana. (2017). Cyber security for the defence industry. Retrieved from https://www.cybersecurity-review.com/industry-perspective/cyber-security-for-the-defence-industry/. [29/10/21]

Tabansky, L. (2011). Critical infrastructure protection against cyber threats. *Military and Strategic Affairs*, 3 (2). Diambil dari: https://www.inss.org.il/wp-content/uploads/sites/2/systemfiles/(FILE)1326273687.pdf.

Copyrights