JURNAL MULTIDISIPLIN MADANI (MUDIMA)
Homepage: https://journal.formosapublisher.org/index.php/mudima
ISSN: 2808-5639 (Online)
Research Article

Volume 4, No 9, September (2024)	DOI: https://doi.org/10.55927/mudima.v4i9.11372	Page: 1395-1407

The Role of Cybersecurity in Defense Technology Innovation: A System Thinking Approach to Deal with Cyber Threats in The Era of Industrial Revolution 4.0

Agus Juniawan Khairi[1*], Sri Yanto[2], Aries Sudiarso[3]
Study of Defense Industry, Republic of Indonesia Defense University
Coressponding Author: Agus Juniawan Khairi agus.khairi@gmail.com

ARTICLE INFO

Keywords: Cyberattack, Technology Innovation, Technology Mastery, System Thinking

Received : *17 July*
Revised : *18 August*
Accepted : *20 September*

ABSTRACT

The world has entered the era of the Industrial Revolution 4.0, where defense technology has undergone a transformation to digital technology, thus presenting new problems in the form of cyber threats that develop dynamically following technological developments. The threat of cyber-attacks can be in the form of theft of confidential data or sabotage of military or public facilities. The all-digital defense technology innovation process is an advantage in the aspect of cyber security, where military equipment is interconnected to facilitate and increase the efficiency of operations in the field. This article discusses the strategic role of cybersecurity in supporting defense technology innovation, using a system thinking approach, enabling a more holistic understanding of the interaction between components in the defense technology system, as well as its impact on national cybersecurity. Using a literature review and case study analysis, this article explores in depth the incidence of cyberattacks, and through a system thinking approach it identifies, analyzes and mitigates the risks arising from cyber threats. In addition, this article also discusses the importance of cybersecurity integration in defense technology innovation to ensure system resilience in the face of various forms of cyberattacks. It is hoped that this method can increase the durability of defense technology by focusing on strategic advantages in global competition

INTRODUCTION

The Indonesian government continues to encourage the implementation of the industrial revolution 4.0 program in various sectors, including the defense technology innovation sector, thus bringing about a massive transformation in the defense industry sector in the country. Where in the development of defense system technology is inevitable from the integration process with information and communication technology (ICT). Using ICT technology in various weapons systems, military communications, and logistics systems will increase efficiency and effectiveness in the implementation of operations in the field. However, problems arise with the use of ICT technology in every development of Defense and Security Equipment (Alpalhankam), resulting in a major threat that continues to lurk in the security of data and information known as cyber-attacks.

The increasing dependence on digitalization in defense technology makes the defense system a target for cyber criminals. Weapon systems that were once developed by relying on mechanical components, have now been developed by integrating software and complex communication networks in them, in order to facilitate operation and decision making. If the development of defense technology innovation does not consider cybersecurity factors, it will make the system vulnerable to various types of attacks, ranging from data theft to sabotage of state-owned Alpalhanhan.

Ironically, the magnitude of the threat of cyber-attacks is an obstacle to the development of defense technology with integration in internet-based communication systems, where technological innovations that should increase the capabilities of Alpalkankam will instead become an entry point for cyber security threats. The danger of cyber-attacks can paralyze weapons systems, and can even hinder the process of developing new technologies in modern Alpalhankam. Defense technology developers must make cybersecurity a priority, starting from the product development planning stage, so that the resulting innovations are not only modern, but also safe from hacking by irresponsible parties.

The occurrence of cyber-attacks on various modern weapon systems is increasingly common. This shows the importance of strengthening the cyber security system. One example of a cyberattack that has occurred is the Stuxnet attack that targeted nuclear power plant facilities in Iran. The attackers succeeded in carrying out a cyberattack by inserting a virus into the industrial control system at a nuclear facility in Iran, thus damaging a large number of vital equipment such as uranium enrichment centrifuges. This incident shows that cyberattacks not only have the potential to disrupt military operations, but can also hamper a country's strategic programs.

Cyberattacks that have occurred, not only threaten weapons systems, but also attack critical infrastructure that supports the lives of the general public, thus disrupting the social life of a country. One example that is still remembered today is the cyberattack on the power grid in Ukraine, which occurred in 2015 and 2016. Hackers managed to get into the control systems of power plants and disable a number of substations, causing widespread power outages in Ukraine. These attacks show that energy infrastructure, which underpins people's lives, the economy, and national security systems, is highly vulnerable to cyberattacks. In addition to disrupting electricity supply, an attack can trigger massive social unrest.

Cyber Security in Defense Context

In the process of defense technology development and innovation, the main factor that should not be forgotten is cyber security, especially in the era of the Industrial Revolution 4.0. Where the use of ICT technology is increasingly widespread in defense systems, so the risk factor of cyber-attacks is increasingly important to consider. In his article, Schneier (2015) emphasizes that cybersecurity is not only related to technical issues, but also a strategic issue that needs serious attention from the government and the military sector. In the context of integrating ICT technology, including software and internet networks in modern weapon systems, there is a great risk of potential cyber-attacks from irresponsible parties.

The development of defense systems that were previously mechanically based, in the industrial era 4.0 has changed towards digitalization, which opens up opportunities for cyber criminals to exploit new security gaps. Rid & McBurney (2012) argued that cyberattacks on weapon systems can cause serious disruptions that impact the security of the country. Therefore, an in-depth understanding of cyber threats is very important in formulating a

comprehensive security policy related to cyber security at vital state facilities.

Defense Technology Innovation and Cyber Threats

Improving the capabilities of Alpalhankam aims to achieve the efficiency and effectiveness of military operations that can be obtained through the innovation in technology. In the industrial era 4.0, the process of technological innovation has a new challenge in the form of cyber security threats. Referring to Lynn's (2010) expression, emphasizing that there will be more loopholes that can be exploited by hackers, along with the increasing complexity of defense technology. Thus, cybersecurity aspects must be studied in more detail in every defense technology innovation.

Examining the Stuxnet attack presented by Zetter (2014) shows the tremendous impact of a cyber-attack on the national defense system. The tragedy in Iran, related to the Stuxnet virus attack on its nuclear program, resulting in damage to critical infrastructure, proves that cyber-attacks can cause fatal damage in the context of state security. This incident also revealed that the most modern defense technologies are vulnerable to cyberattacks, making it important to ensure adequate security in line with technological developments.

Effective Cybersecurity Technology

A top priority for protecting weapon systems and critical infrastructure from attack threats is the development of cybersecurity technologies. Choo (2011) identifies a number of cybersecurity technologies that have proven effective, such as the use of sophisticated encryption, intrusion detection systems and firewall reinforcement. These technologies are designed to protect military communication networks from hacker attacks and acts of sabotage.

Additionally, Pomerleau (2017) emphasized the importance of artificial intelligence (AI) and machine learning in strengthening cybersecurity. These technologies can learn unusual attack patterns and prevent them before they happen. With AI, defense systems can respond to threats in real-time, providing a strategic advantage in the face of increasingly complex cyberattacks.

Human Resources and Cyber Security

The quality of human resources (HR) operating and managing defense systems is an equally important factor, so cybersecurity depends not only on the technology used, but also on the capabilities of human resources. The importance of training and developing HR skills in mastering cybersecurity technology to ensure that defense technology functions optimally and safely, according to Colwill (2009).

The development of cyber expertise in the military environment is critical, especially given the evolving cyber threats. Davis et al. (2015) underlines that cybersecurity education and training for military personnel should include an in-depth understanding of different types of cyberattacks and protection methods. By having trained personnel, the risk of a successful cyberattack can be minimized.

International Cooperation in Cyber Security

To deal with cyber threats in the era of globalization, it is important to conduct international collaboration. According to Nye (2011), international collaboration is important because cyberattacks are often transnational, requiring cooperation between countries to overcome them. International collectivity in developing effective solutions and sharing information about cyber threats is an important factor in minimizing cyber-attacks.

In his article, Lewis (2014) said that to face more complex global threats and strengthen the security of defense technology at the international level, international cooperation in the field of cyber security is needed. The initiation of cyber security cooperation has been carried out by international organizations such as NATO to protect its member countries from cross-border hacking.

Cooperation in cybersecurity should include the development of international standards to protect data and networks, because with globally recognized standards, countries can build safer and more coordinated defense systems, said Libicki (2009).

Challenges in Countering Cyber Threats

Addressing cyber threats is not an easy task. Identifying any cyber threat is one of the main challenges in cybersecurity. In a cyber-attack, the most difficult factor is identifying the origin of the attack. Cyber-attacks are often carried out by unknown actors, both individuals and countries, operating in hidden networks, Clarke & Knake (2010).

In addition, cyber threats are constantly evolving and dynamic in nature. This is conveyed by Singer & Friedman (2014), stating that cybersecurity technology must be continuously updated to respond to new emerging threats. This challenge requires flexibility and continuous innovation in the development of cybersecurity technology.

Limited budgets and resources are also obstacles that must be faced. Despite the importance of cybersecurity, not all countries have a robust cyber defense system, due to the lack of adequate resources to build a strong system, referring to Harknett & Stever (2011). This suggests the importance of support from the international community to strengthen cyber defense makes some countries more vulnerable to cyberattacks.

The Role of System Thinking in Strengthening Cyber Security

The use of systems thinking schemes plays an important role in solving problems related to cyber threats in defense technology innovation. System thinking enables in-depth analysis of the various elements involved in cybersecurity, including technology, people, policies and procedures. According to Senge (2006), using a system thinking approach will increase effectiveness in understanding the impact of interactions between variables in building cybersecurity, as well as in mitigating overall threats to defense technology innovation. Systems thinking is also used in identifying cause-and-effect relationships in the complexity of cyber threats, allowing stakeholders to design more comprehensive and sustainable solutions so that the resulting defense technology innovations are more resilient to cyber-attack vulnerabilities.

When new technological innovations are introduced, using systems thinking methods makes it possible to predict the potential for cyber risks, then integrated preventive measures are taken. A study conducted by Jackson (2019) showed that this approach can create an effective cybersecurity strategy, as it allows organizations to see the big picture of existing threats and take mitigation actions proactively. In addition, systems thinking helps in designing defense technology innovations that are more resilient to cyberattacks, through a better understanding of the dynamic interactions between elements in the defense system.

Thus, the early application of systems thinking in the development of defense technology innovations is an important step in the development of cybersecurity strategies. Various studies have shown that this approach is not only a tool to mitigate threats, but also to strengthen the overall security system through an understanding of the broader interrelationships between components. Therefore, systems thinking should be an integral part of the planning and development process of defense technology innovation in an era where all military equipment is developed connected to each other with internet connections.

Currently, many researchers and experts are discussing cybersecurity in various sectors related to the impact of the implementation of ICT technology integration on technological innovation, but there are still several challenges that need to be addressed in the future. Several questions related to the role of cybersecurity in defense technology innovation will be explored in more depth in this article, including: (1) What are the aspects of defense system protection against cyber-attacks? (2) What cybersecurity technologies are effectively applied to the military environment? (3) How to build competent human resources in the field of cybersecurity? (4) How to overcome challenges in international cooperation in the field of cybersecurity?

METHODS

The method used in the preparation of this article uses a literature study approach through a case study by exploring to examine more deeply the role of cybersecurity in defense technology innovation. Various information was collected from various literatures and continued with the analysis of relevant documents related to cybersecurity focusing on defense technology innovation. It is expected that the resulting article can examine in detail the cyber-attacks that affect the defense system and the steps to strengthen security in the future. After thematic analysis, patterns and key themes were identified from the data collected. Although there are limitations in generalization of results and access to information, this article attempts to validate through various accessible literature sources.

Using the case study method will provide a detailed examination of specific instances where

cybersecurity plays an important role in defense systems. The case study approach helps link the theoretical aspects of the research with practical real-world examples. However, the researcher realizes that this method has limitations to the access of sensitive classified information, this research validates its analysis through various publicly available sources, by mutually verifying documents and studies to ensure the credibility of the findings.

Furthermore, a systems thinking approach was used to understand the relative relationship between technology, threats, policies and human resources in cybersecurity. By thinking systemically, this research looks at how changes in one component, such as the development of a new technology, can affect the entire security system. This approach also helps identify weak points potentially exploited by cyberattacks and offers more comprehensive and sustainable solutions. The results of this research provide a strategic outlook on efforts to strengthen cybersecurity in defense technology innovation.

The end result of this research is expected to provide a strategic view on how to strengthen cybersecurity in defense technology innovation. By combining literature review, thematic analysis and systems thinking, this research offers actionable insights into how technology, policy and human resources should adapt to future cyber threats.

RESULTS AND DISCUSSION

The industrial world has now entered a phase where the application of digitalization technology has been used in various sectors of life. Thus, the implementation of the Industrial Revolution 4.0 in the development of defense technology is faced with a major challenge in the form of cyber threats. Through the integration of defense technology and ICT technology in the defense system, it will increase the efficiency of operations, but also increase the vulnerability to the danger of cyber-attack threats. In ASIA, a cyber-attack has occurred and shocked many parties, namely the Stuxnet attack, which targeted nuclear facilities in Iran. In the Stuxnet attack, hackers managed to insert a virus into the control system of the nuclear facility in Iran, thus damaging the centrifugal system for uranium enrichment, indicating the fatal impact of cyber-attacks on the country's strategic infrastructure. This attack shows that modern defense systems, which are integrated with ICT technology through software and internet networks, are highly vulnerable to cyber-attacks that can result in operational disruptions and fatal damage, to the point of affecting people's lives at large.

In addition, cyberattacks also target civilian facilities that affect social life at large. In 2015/ 2016, there was a cyberattack that struck vital infrastructure such as the power grid in Ukraine. The impact of this cyber-attack resulted in widespread power outages in many parts of Ukraine. Thus, highlighting the massive impact of cyberattacks, it is necessary to strengthen cyber security in protecting the systems that sustain the social and economic life of a country. In the context of cyberattacks on defense facilities, emerging threats include the theft of strategic data and state secrets, sabotage of weapons systems, or disruption of military operations that could be detrimental to the security of the state. This article further examines the readiness of a country, especially Indonesia, to deal with cyberattacks on defense technology innovations that continue to develop today, as well as the fatal impact on the national defense system.

The Role of Cyber Security in Defense Technology Innovation

The development of defense system technology innovation requires internet connectivity, so that defense equipment is interconnected for ease of operation in the field. The use of Industry 4.0 technology in defense technology innovation makes cybersecurity factors play a vital role. Of course, the integration of ICT technology in Alpalhankam innovation can increase the effectiveness and efficiency of military operations, but it is necessary to ensure cybersecurity factors starting from the initial design phase so that the resulting defense technology innovation is safe from the threat of cyber-attacks. The use of artificial intelligence technology in the defense technology innovation process needs to be developed in detail so that the defense system is protected from the threat of cyber-attacks. In addition, as a solution to minimize the danger of cyber-attacks, encryption technology and early detection systems are needed, and strengthening firewalls to protect military communication networks in defense technology innovation.

Every technological innovation must incorporate cybersecurity technology from the planning stage of product development to prevent weaknesses that can be exploited by hackers. This strategy ensures that weapon systems using defense technology advancements enhance operational capabilities while protecting against the risk of cyberattacks. Defense technology developers must consider cybersecurity as an important component in every step of innovation to minimize the dynamic threats that continue to emerge in response to evolving technological advances, given the many incidents of cyberattacks targeting various important state facilities. For this reason, government policies are needed to accelerate the improvement of cybersecurity in the defense industry sector.

Government Programs and Policies

The Indonesian government has launched programs and policies to accelerate defense technology innovation and improve cybersecurity. One of the government's flagship programs is Making Indonesia 4.0, which is a government initiative that aims to advance the industrial sector, including the defense industry, by integrating industrial technology 4.0 technology. This program includes a technology pillar initiative to strengthen cybersecurity in technological innovation in the defense industry sector.

In addition, the government also rolled out the Domestic Component Level (TKDN) policy which aims to encourage technological independence by encouraging the use of local components. By mastering local technology in data communication components, it is hoped that it will minimize dependence on foreign producers whose confidentiality cannot be controlled. The development of local products certainly requires special attention to the development of technological innovation from cybersecurity threats. Domestically developed components must be equipped with adequate protection to prevent vulnerability to cyber-attacks.

Another initiative from the government to encourage the acceleration of cybersecurity improvement is the Digital Talent Scholarship program and cybersecurity training as well, to build competent human resources in the cyber field. International cooperation in the field of cybersecurity, including with ASEAN countries and international organizations, also continues to be carried out by the government as evidence of the importance of cybersecurity in various aspects of people's lives. This international cooperation is important to support national efforts in dealing with cyber threats that are multilateral or cross-border.

To discuss more deeply, a SWOT matrix is compiled related to the Indonesian government's policies in dealing with cyber threats that greatly impact national level security.

Table 1. SWOT Analysis of Government Policy on Cyber Attacks

	Internal Factors	
	Strengths	**Weaknesses**

		Internal Factors	
		Strengths	**Weaknesses**
External Factors	**Opportunities**	**International Collaboration** Leverage local technology strengths and supportive government policies to establish collaborations with other countries and international organizations in the development and application of cybersecurity technologies. This can enhance defense technology capabilities and open up access to new technologies. **Human resource development** Initiatives such as the Digital Talent Scholarship and cybersecurity training increase the capacity of human resources who can handle cyber threats.	**Infrastructure Investment** Overcoming infrastructure limitations by capitalizing on the opportunities of technological advancements such as AI and blockchain. This involves allocating budgets to strengthen infrastructure that supports the adoption of new technologies that can enhance cybersecurity. **International Training** Address skills gaps by partnering with international institutions for more comprehensive training and education programs. This can help improve HR skills and meet the demands of evolving cybersecurity technologies.
	Threats	**Government Policy** Leverage existing government policies to develop security strategies that are adaptive to evolving cyber threats. This involves formulating policies that are flexible and responsive to new threats. **Local Technology** Using local technological advancements to reduce dependence on foreign technologies that may have vulnerabilities. Domestic technology development can strengthen the defense system against cyber threats and reduce the risks of technology dependence.	**Budget Limitations** Address budget limitations by prioritizing the allocation of funds to the most critical areas of cybersecurity, as well as seeking additional funding or partnerships to strengthen existing cybersecurity systems. **Infrastructure Improvement** Address infrastructure weaknesses by increasing investment in security technologies and updating existing systems to deal with evolving cyber threats. This includes modernization and continuous improvement to maintain resilience against attacks.

The SWOT analysis above shows that success in addressing cyber threats in defense technology innovation depends on leveraging internal strengths, such as local technology and support from government policies and work programs, to take advantage of external opportunities, such as international collaboration and technological advances.

Then to overcome internal weaknesses, such as infrastructure limitations and HR skills gaps, as well as external threats such as the evolution of cyber threats and technological dependence, requires an integrated strategic approach. By prioritizing infrastructure development, strengthening HR training, and investing in advanced security technologies, as well as forging international partnerships, Indonesia can increase the resilience of the defense system against cyber threats and ensure safe and effective technological innovation.

From the SWOT analysis above, a closed loop system thinking scheme for defense technology innovation resilience is obtained as follows:

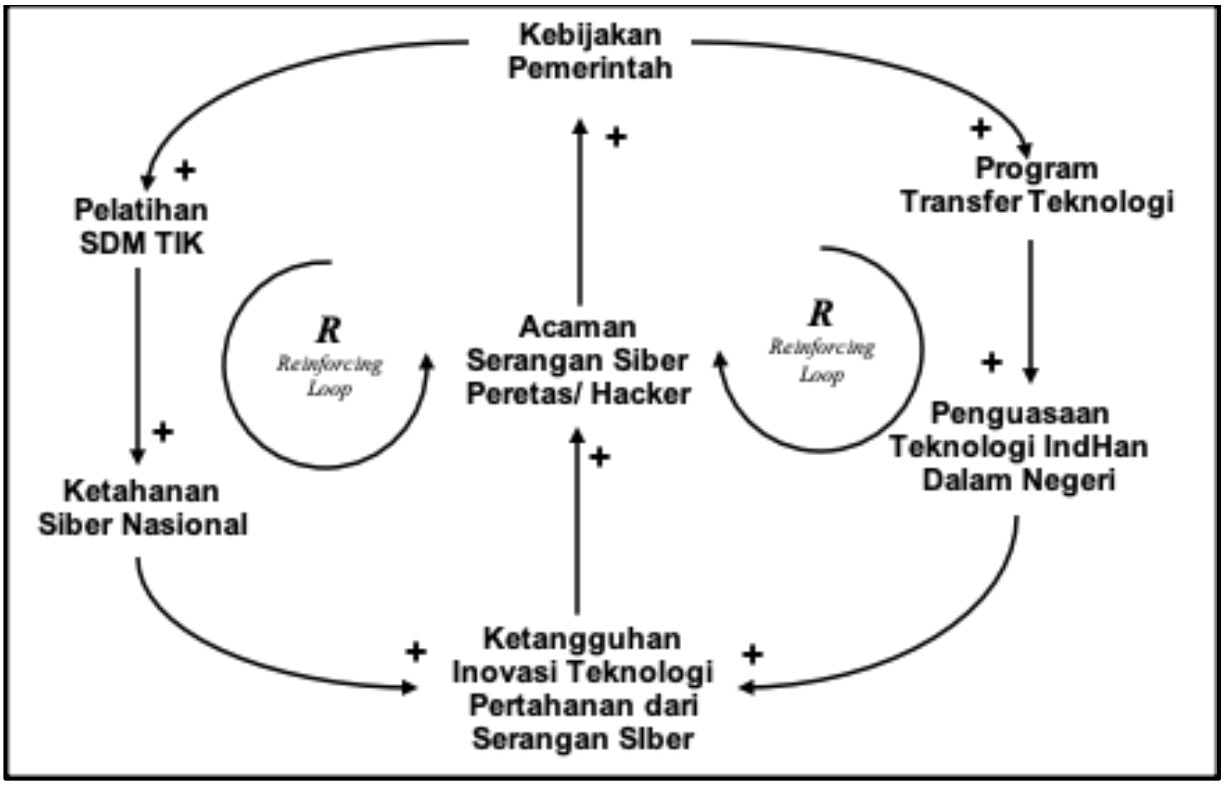

Figure 1. Loop System Thingking of Defense Technology Innovation
(Resilient to Cyber Attack Threats)

Drawing description:

Left Side

- With the high threat of cyber-attacks, the government issued a policy to improve the capabilities of human resources in the field of ICT (especially cyber resilience), through the ICT HR training work program.
- With the training program, it will increase cyber resilience nationally.

Right Side

- In parallel, government policies in the defense industry increase technology transfer programs.
- With the technology transfer work program, it will encourage increased mastery of domestic technology.

Center Side

- With the establishment of national cyber resilience and mastery of domestic defense technology, will increase the innovation of defense technology that is resilient to cyber attacks
- Over time, the ability of hackers / hackers increases, thus increasing vulnerability to cyber-attacks, so a sustainable policy is needed to continue to maintain the ability of human resources both from defense technology and human resources capable of cyber security.

CONCLUSION

Based on the analysis conducted, it can be concluded that defense technology innovation in the era of the Industrial Revolution 4.0 is inseparable from the risk of cyber-attacks that continue to change dynamically following technological developments.

The use of ICT technology in modern weapon systems will increase operational efficiency and effectiveness, but there are opportunities for hackers to exploit weaknesses in the security system built. For this reason, cybersecurity factors are a priority in every development of defense technology innovation, starting from the design to implementation phase.

The Indonesian government has taken strategic steps through policies such as TKDN and Making Indonesia 4.0, as well as improving human resources in the cyber field through training initiatives. However, there are still major challenges, such as budget and infrastructure limitations, that need to be further analyzed.

Some recommendations that the author can make to improve cybersecurity capabilities in defense technology innovation are as follows:

1. Continue and expand multilateral cooperation and international organizations to strengthen cybersecurity at the global level, and improve access to the latest security technologies.
2. Increase investment in the development of domestic cybersecurity infrastructure, such as: development of encryption technology and artificial intelligence-based threat detection systems.
3. Strengthen human resource training and development programs, including creating an educational ecosystem that supports cyber expertise.
4. Adjust national regulations related to cybersecurity and privacy to ensure that defense technology innovations are well protected from increasingly dynamic cyber threats.

With the implementation of these measures, Indonesia is expected to improve its ability to deal with evolving cyber threats, while advancing resilient and secure defense technology innovation.

REFERENCES

Choo, K.-K. R. (2011). The cyber threat landscape: Challenges and future research directions. Computers & Security, 30(8), 719-731.

Clarke, R. A., & Knake, R. K. (2010). Cyber War: The Next Threat to National Security and What to Do About It. HarperCollins Publishers.

Colwill, C. (2009). Human factors in information security: The insider threat – Who can you trust these days? Information Security Technical Report, 14(4), 186-196.

Davis, J. S., Boudreaux, B., Welburn, J. W., & Chase, M. S. (2015). U.S. Military Cybersecurity: Forging Information Assurance Teams for the Future. RAND Corporation.

Farwell, J. P., & Rohozinski, R. (2011). Stuxnet and the future of cyber war. Survival, 53(1), 23-40.

Hamdan Abd manaf Ismail, O. (2015). Ancaman Keselamatan Internet Sebagai Isu Utama Negara: Isu-Isu Kontemporari, Pendekatan, Dan Penyelesaian. Majalah Ilmiah UNIKOM.

Harknett, R. J., & Stever, J. A. (2011). The cyber security triad: Government, private sector partners, and the engaged cybersecurity citizen. Journal of Homeland Security and Emergency Management, 8(1).

Jackson, M. C. (2019). Critical Systems Thinking and the Management of Complexity. Wiley.

Lewis, J. A. (2014). Cybersecurity and Cyberwar: What Everyone Needs to Know. Oxford University Press. Libicki, M. C. (2009). Cyberdeterrence and Cyberwar. RAND Corporation. Lynn, W. J. (2010). Defending a new domain: The Pentagon's cyberstrategy. Foreign Affairs, 89(5), 97-108.

Nye, J. S. (2011). The Future of Power. PublicAffairs. Pomerleau, M. (2017). How artificial intelligence can boost cybersecurity. Defense Systems. Retrieved from https://defensesystems.com.

Rid, T., & McBurney, P. (2012). Cyber-weapons. RUSI Journal, 157(1), 6-13.

Schneier, B. (2015). Data and Goliath: The Hidden Battles to Collect Your Data and Control Your World. W.W. Norton & Company.

Senge, P. M. (2006). The Fifth Discipline: The Art & Practice of The Learning Organization. Doubleday/Currency.

Singer, P. W., & Friedman, A. (2014). Cybersecurity and Cyberwar: What Everyone Needs to Know. Oxford University Press.

Streltsov, L. (2017). The system of cybersecurity in ukraine: principles, actors, challenges, accomplishments. European Journal for Security Research, 2(2), 147-184.

Zetter, K. (2014). Countdown to Zero Day: Stuxnet and the Launch of the World's First Digital Weapon. Crown Publishers.