ISSN 1846-6168 (Print), ISSN 1848-5588 (Online)
https://doi.org/10.31803/tg-20230218142012

Original scientific paper
Received: 2023-02-18, Accepted: 2023-03-21

Effect of AI: The Future Landscape of National Cybersecurity Strategies

Geunhye Kim, Kyudong Park*

Abstract: Artificial intelligence (AI) is considered a vital factor that will fundamentally alter the cybersecurity environment. AI technology is progressing much faster than expected, and AI-based security services are being introduced into the global security market on a daily basis. However, how AI can contribute to the cybersecurity field and what changes it will bring remain unknown. Nonetheless, cybersecurity is not merely a technical issue but also a process for dealing with regulations, policies, and security risks; therefore, the introduction of AI technology introduction can make a fundamental difference in cybersecurity policy as a whole. This study primarily aims to better understand the concept and characteristics of AI from the cybersecurity perspective and identify its future implications on cybersecurity environment at the national policy level. This study predicts what modifications will be made to national cybersecurity strategies (NCSS) when machine learning (ML) is introduced and implemented. It also provides a basic policy recommendation that offers potential responses to these changes. The study first describes the emergence of AI in the cybersecurity field and explains AI-ML technical services and AI security policy elements. Second, through NCSS material analysis, this study categorizes NCSS into 11 categories and selects the critical functions of each dimension. Finally, it predicts the changes that will occur when AI is introduced within the selected NCSS category. It also introduces the priorities and considerations required for these changes.

Keywords: artificial intelligence (AI); cyberattack; cybersecurity; machine learning (ML); national cyber security strategies (NCSS)

1 INTRODUCTION

Artificial intelligence (AI) has emerged as one of the most critical technologies in every aspect of the information age. In cybersecurity, technology development for solving security problems on the basis of AI is rapidly progressing. Compared with conventional cybersecurity solutions, AI-enabled security systems are more flexible, adaptable, and powerful [1]. Although AI technology remains incomplete, and the application of AI technology in cybersecurity remains in its infancy, experts believe that AI security systems will help to improve cybersecurity performance and defense, and ultimately, significantly impact the cybersecurity environment.

Meanwhile, AI utilization in cybersecurity also affects the aspect of the attack. Previous studies have predicted the future AI cyberattacks as follows. First, even if the influence of AI is stronger in cybersecurity, the fundamental goal of cyberattacks will not change. In addition to stealing data and shutting down systems, AI-powered cyberattacks also manipulate data to influence human behavior. Second, AI-powered cyberattacks will not be used in all areas. AI cyberattacks require more time, resources, and capital than traditional cyberattacks. Therefore, AI-powered cyberattacks will be employed in a much more sophisticated way in large-scale cyberattack targeting, government agencies, and companies rather than individuals. Third, experts have different opinions about when exactly AI-armed cyberattacks will transpire, but they predict that they will occur in the near future [2].

Thus, how can countries respond to these cybersecurity changes? On the basis of the National Cyber Security Strategy (NCSS), this study attempts to envision how AI will affect national cybersecurity and what areas the country should improve. However, AI cybersecurity research has paid limited attention to national behavior and national strategies. Thus, when considering the characteristics of AI cyberattacks, national behavior must also respond to these changes. The reason for this is that the government's national cybersecurity strategy is critical to addressing cybersecurity issues, even though private companies that own and operate the majority of information technology (IT) are critical to improving the country's cybersecurity system [3].

Over the last decade, NCSS has been widely used worldwide as a national guideline for addressing cybersecurity issues at the national level. On the basis of the NCSS, we determined that the development of countermeasures in an evolving AI cybersecurity environment is a good starting point for a national review of AI security policy.

This study extensively reviews existing AI and NCSS-related materials. The study is organized as follows. First, it introduces the emergence of AI in the cybersecurity field and explains related technical services and policies. Second, the outline of NCSS is explained, and its categories and elements are selected on the basis of the existing materials. Finally, we predict the changes that will occur when AI is introduced within the selected NCSS category. We also suggest priorities and considerations required for these changes.

2 RELATED WORKS

In the field of cybersecurity, research on changes and countermeasures resulting from the introduction of AI technology has been conducted since 2010. Existing studies can be broadly classified into two categories. First, studies on AI technology application in cybersecurity. Ref. [4] analyzed the errors of AI and suggested how to effectively apply it to cybersecurity. Ref. [5] investigated how to respond to cyberattacks using AI on the basis of a literature review and proposed ways to construct a safe AI system. Ref. [6] presented a future research direction by analyzing "AI-based cybersecurity", which is expected to play an important role in intelligent cybersecurity services and management. Ref. [7] presented an AI-based cybersecurity model on the basis of papers published from 2016 to 2020. Ref. [8] explained

the current state of AI use in cyber security and presented case studies and application programs.

Second, studies that describe countermeasures and recommendations on the basis of changes in the implementation of AI technology in the cybersecurity from a specific perspective. Ref. [9] analyzed how to effectively utilize AI technology, which is expected to have the greatest impact in cybersecurity, with a focus on web application security. Ref. [1] presented from an organizational perspective on a mature cyber environment combined with AI technology. Ref. [10] described the role of AI in cybersecurity and provided recommendations on how organizations can leverage AI in cybersecurity. Ref. [11] analyzed how AI can affect cyber defense and attacks from the 5G technology perspective and suggested countermeasures. Ref. [12] identified major problems in cybersecurity regarding AI use from a criminological viewpoint. Ref. [13] evaluated current challenges related to AI in cybersecurity in the US and proposed solutions.

Research on policy changes and responses at the national level due to the introduction of AI technology in the cybersecurity environment remains scant. Thus, the study's primary goal is to identify changes in national cybersecurity policies as a result of the introduction of AI technology and to provide considerations for responding to them. Particularly, this study aims to outline NCSS, a key national guideline for solving cybersecurity problems at the national level. Over the past decade, many countries have adopted NCSS tailored to their characteristics, and roughly 80 countries have announced NCSS since 2006 [14]. In addition, this study focuses on machine learning (ML), which is currently receiving the most attention and activation in cybersecurity research in AI technology. The research questions of this study are as follows.

- Research Question 1. How does the introduction of AI technology in cybersecurity environments change the core functions of NCSS?
- Research Question 2. What are the recommendations or considerations that NCSS can make to address the key challenges associated with these changes?

This study aims to answer research questions through an extensive review of AI national strategy reports published by countries worldwide, NCSS guidelines, and data released by various international organizations and research institutes. Moreover, we analyze the key changes and provide recommendations for NCSS core features adopted in the study.

3 AI IN CYBERSECURITY

3.1 Brief History of AI in Cybersecurity

Attempts have been made to predict and detect various cyberattacks using AI technology. The security industry has utilized AI for more than a decade to withstand changes in attackers and to create a system that analyzes, shares, and defends attack information [15]. However, malicious cyberattacks were not as diverse a decade ago as they are today. Thus, attempts to introduce AI technology into cybersecurity have only received limited attention. In addition, the method of pattern matching allowed the intrusion detection and attack analysis system to fully defend against these attacks. In contrast to the situation 10 years ago, however, the recent cyber threats caused by cybersecurity issues are substantial in terms of quantity and scope [16].

These attacks are likely to increase even further. Recent cyberattacks have been more successful than in the past as they have become more intelligent, organized, and diverse as a result of the constant emergence of new Information and Communications Technology (ICT) industries. To effectively respond to these cyberattack changes, various solutions and response systems have become increasingly necessary, technically and administratively. People have also inquired about how cyberattacks respond; is it possible to anticipate daily evolving cyberattacks? Or, is it possible to detect and respond in advance to unforeseeable Black swans (which, once they occur, cause severe system damage)? Recent attention has been drawn to the need for the introduction of AI technology, which is anticipated to provide answers to these questions [15].

Specifically, ML is one of the most prevalent ways to describe AI applications in cybersecurity and one of the fundamental elements of the next frontier of cybersecurity defense [17]. Using ML technology, research and applications are being conducted in various cybersecurity fields, including security control, threat detection, and prevention. It also provides an immediate, powerful, and proactive response to cyber threats in real time [18]. These security services make cybersecurity more straightforward, proactive, and effective [17].

Such secure ML models can be classified into three general types. First, there is supervised learning. This algorithm is a method of giving and learning problems and answers simultaneously. This algorithm is mainly used for problem solving, such as recognition, classification, diagnosis, regression, and decision trees. In the cybersecurity field, the method is used for network traffic analysis, spam filtering, and malware detection. Second, unsupervised learning is a way of learning only by giving problems. The method is mainly used for clustering, density estimation, and dimensional reduction, and it is best suited for identifying features. In cybersecurity, the algorithm is used for malware identification, user behavior analytics, and network anomaly detection. Third, reinforcement learning is a method for learning through the evaluation of outcomes. Through this method, ML agents can learn to behave through game-like environmental experiences [19].

3.2 Description of AI in Cybersecurity

The discussions on AI use in cybersecurity can be divided into technical and policy issues. Particularly, discussions on AI technology use are a key part of cybersecurity. Based on the existing discussions, the current and future applications of AI in cybersecurity technology are as follows.

- **Intrusion and threat detection.** The technology quickly detects, analyzes, and defends against cyberattacks or

malicious activity in real time; it is useful for threats, such as data leakage.
- **Security monitoring.** This technology identifies information about network traffic, internal and external behavior, data access, and many other functions and activities. It focuses on handling log files and error messages from various products.
- **Vulnerability scan and removal.** The technology removes vulnerabilities by identifying and prioritizing weaknesses in the system to counter attacks, such as target zero-day attacks and IoT devices.
- **Data classification.** The technology examines newly introduced data and categorizes sensitivity levels. The system is then protected according to the characteristics of the data, such as privacy and data protection regulations.
- **Spam filtering and social engineering detection.** The technology uses predefined parameters and various statistical models to detect and block spam and classify malicious activities.
- **Security automation.** This technology helps automate repetitive tasks, eliminating the need for repeated, low-value decisions, and it is effectively used in areas, such as threat intelligence.
- **User behavior analytics.** The technology identifies user behavior and accurately detects and blocks new forms of cyberattacks in real time. It also detects accounts through suspicious user behavior analysis and protects the system.
- **Network traffic profiling and network anomaly detection.** The technology analyzes network traffic to calculate risk rating scores. The network risk score provides an estimated risk level and various data-based incompatibilities to rapidly identify anomalies and high-risk situations.
- **Endpoint security.** This technique is trained by unique algorithms. The algorithm is taught to discover new malicious files on the basis of the characteristics of previously discovered malicious files, and it can be used to censor traffic and automatically identify threats.

Meanwhile, global discussions and expectations regarding the application of AI technologies, including cybersecurity, have prompted a review of AI policy. AI cybersecurity policy and AI security policy are discussed. These policies provide some high-level principles and recommendations for technology use.

Ref. [20] predicted that AI development will directly impact nuclear weapons, aircraft, cyber, and biotechnology, which can be an innovative future technology for national security. Particularly, they explained that AI and ML can revolutionize cybersecurity and cyber warfare. Ref. [21] described the attributes of AI, which are expected to affect the security environment and the changes that can occur. The report provides high-level recommendations, such as close collaborations and identification of best practices, necessary for policymakers and stakeholders to respond to changing threat environments through analysis in the near future. Ref. [22] defined AI security as "the robustness and resilience of AI systems, as well as the social, political, and economic systems with which AI interacts". On the basis of this definition, she introduced the AI security map to explore complex AI security environments. Finally, she provided policymakers with recommendations, such as facilitating early global coordination and holding the technology industry accountable.

4 PARADIGMS FOR NATIONAL CYBERSECURITY STRATEGY

4.1 History of NCSS

In the late 1990s and early 2000s, many countries began to announce national security strategies (NSS) in response to the need to present a consistent approach to the various security issues that emerged from the Cold War [23]. These NSSs included non-traditional security domains, such as energy, climate change, terrorism, cyber, human rights, and the environment. At that time, the cybersecurity domain had been regarded as one of the new non-traditional security domains that policymakers should consider.

Until the 1990s, the idea that cybersecurity would affect national security was not considered possible [24]. This need for cybersecurity has become evident since the early 2000s, alongside a meteoric rise in the number of Internet users and a clear tendency for government agencies, private companies, the military, and economic activities to shift their operations online [25]. As data and information are considered the most valuable assets and values in society and the scope of cybersecurity areas to be protected gradually expands in the private and public sectors, cyberattacks are described as the most likely new threat to the country in the national security strategy [26]. Particularly as a result of this shift in perception, official recognition and responses regarding the dangers of cyberattacks that occurred worldwide in 2006. Moreover, cyberattacks on Estonia in 2007, cyberattacks during the Russo-Georgian War in 2009, and a cyberattack on Iran's nuclear program using the Stuxnet worm, prompted many countries to recognize that: first, a cyberattack that threatens national security is possible; second, the countries' critical infrastructure is extremely vulnerable to cyber security; and third, comprehensive policy responses should be discussed at the national level, as these attacks can be under the control of a foreign power [23].

Since the mid-2000s, a series of cyberspace incidents have elevated cybersecurity to a higher priority than physical security at NSS. In addition, countries have recognized the need for a cybersecurity strategy distinct from national security strategies in order to implement a comprehensive strategic approach. Since 2006, in response to cyber threats, a growing number of nations have begun to publish the NCSS; today, this includes approximately 80 countries. Essentially, NCSS describes a country's priorities, principles, and strategies for addressing cybersecurity issues at the national level.

The NCSS worldwide has similar goals and shares common topics and interests in many areas. However, slight differences exist in cybersecurity approaches depending on the country's cyber threat environment, social and political

situation, geopolitical security tendencies, and cyber awareness level [27]. For example, no official definition of cybersecurity exists, and only a few countries define it. Additionally, countries have diverse perspectives regarding the extent to which cybersecurity should be addressed. Meanwhile, over the past decade, NCSS has constantly evolved to address new cybersecurity challenges with the rapid expansion of ICT. The scope of the NCSS has expanded as the cybersecurity field has become more inclusive and expansive over the past decade.

4.2 Categories and Elements of NCSS

Many countries have announced NCSS in the last decade. Furthermore, research institutes, international organizations, and companies have issued guidance on the NCSS elements. The cumulative NCSS and recommendations over the last decade have laid a solid foundation for the nation to build a comprehensive NCSS and, eventually, an implicit international agreement on what should be included in the NCSS. This study identifies the major categories and elements of NCSS on the basis of the most recent NCSS published by 15 countries and the NCSS guidelines of international organizations, research institutes, and companies.

- **Critical infrastructure protection.** Countries strive to protect vital infrastructure and provide pertinent services in a secure manner. Countries make efforts to identify and mitigate the risks associated with their primary CIs and CIIs; strengthen network security, develop the next-generation security infrastructure, determine the roles and responsibilities of government branches, and share information [28].
- **Foster a cybersecurity culture.** To foster a cybersecurity culture, countries should raise citizens' awareness of the dangers of cyber threats and the importance of cybersecurity. In addition, the demand for the security of citizens' basic rights, such as privacy and cybersecurity, must be balanced [29].
- **Counter cybercrimes.** Cybercrime activities include various malicious activities that affect citizens and society. Blocking cybercrime is key to protecting society from online attacks. Cyber-crime response mainly comprises the enactment of cyber-crime laws, expansion of cooperation among related government agencies, and expansion of international cooperation [29].
- **Cyber diplomacy.** Understanding and effectively responding to the ever-evolving cyber threat environment is a crucial aspect of international cooperation. Through various international cooperation and exchange measures, such as trust-building support, cybersecurity capacity building, international standards development, and participation in international organizations, the countries can create a common knowledge base and cybersecurity synergies, such as combating transnational crime [30].
- **Public-private partnerships.** Public-private partnerships are the cornerstone of effectively protecting critical infrastructure and managing security risks in the short and long terms [30]. Countries consider public-private common goals, information sharing, and incentives to effectively build partnerships with the private sector.
- **Foster R&D.** NCSS focuses on R&D and technical innovation to enhance its competitiveness by transforming into cutting-edge products and fostering the growth of highly qualified professionals and researchers [30]. These R&Ds not only include the development of new tools for defense and recovery from cyberattacks, but also scientific research in computer science, electrical engineering, mathematics, and cryptography, as well as social science research in psychology and economics.
- **Training and educational programs.** Educating and training cybersecurity personnel is a significant factor in ensuring the long-term sustainability of national cybersecurity capabilities. NCSS covers cybersecurity education and training for professionals and citizens in the public and private sectors. In this regard, countries use many forms, such as developing advanced curricula and adding cybersecurity-related education to curricula, e.g., mathematics and science, to improve workforce expertise [31].
- **Cybersecurity emergency readiness and cybersecurity exercises.** The Computer Emergency Response Team (CERT) plays a crucial role in preventing, detecting, mitigating, and responding to cybersecurity incidents on a national scale. The national CERT provides proactive and reactive functions as well as preventive and educational services, despite variations in operation methods, organizational forms, the scope of roles, requirements, and available resources for each country [30]. Nationally, the Computer Emergency Response Team (CERT) plays a pivotal role in preventing, detecting, mitigating, and responding to cybersecurity incidents. The national CERT provides proactive and reactive functions as well as preventive and educational services, despite differences in operation methods, organizational forms, the scope of roles, requirements, and available resources for each country [29].
- **Cyber contingency.** A cyber contingency plan is a primary element of NCSS and is a procedure for rapid response and recovery in case of a sudden cyber emergency, which can lead to a national disaster. The cyber contingency plan is primarily contained within the national contingency plan. Countries should define cyber crisis responses in stages to respond to emergencies and clearly delineate the roles and responsibilities of all parties involved [29-30].
- **Effective governance.** Many countries adopt specific government agencies, such as the National Cybersecurity Center, to coordinate their cybersecurity initiatives. For effective governance, the government seeks to promote effective cooperation between the public and private sectors and to establish and encourage formal or informal information-sharing exchanges [32].

- **Cyber military and counter-intelligence.** NCSS includes military affairs related to cybersecurity. Some countries separately issued cyber defense strategies from the Department of Defense. Many countries focus on cyber military activities, such as protecting their networks, cyber defense, tactical cyber war, strategic cyber war, and cyber deterrence [23].

5 FUTURE LANDSCAPE OF NCSS

On the basis of the NCSS categories identified in the study, this study details future changes in the cybersecurity environment as a result of the AI use. It lists critical considerations for governments.

- **Critical infrastructure protection.** Major critical infrastructures, such as transportation, health care, and energy, are becoming increasingly dependent on AI-ML. Conventional cyberattacks employing machine learning focused on automating attacks. Future cyberattacks that use ML are anticipated to generate new attack vectors utilizing programs, such as genetic algorithms and enhanced learning, as well as systematically infiltrating various systems, such as the cloud, IoT, and industrial IoT/SCADA, resulting in greater damage [2].

  The country should develop successful backstops by actively introducing AI solutions to protect critical infrastructure from AI cyberattacks by malicious actors [33]. To this end, major infrastructure cybersecurity teams should reliably introduce and deploy AI security systems using various methods, such as systems and network testing, traffic analysis, and identification of normal network behavior. In addition, they should host spam filters to block malicious links that may contain malware, conduct routine system checks, and update security monitoring. These systems should be highly robust and enhance the resilience of systems against unanticipated cyberattacks.

  Meanwhile, these AI solutions necessitate dedicated personnel for system management. The government requires personnel to train the AI, monitor the threat identification results of the AI security system, and ascertain whether the identified threats are in fact threats. Therefore, the government should consider how to recruit new AI-skilled staff and how to retrain existing security staff [34].
- **Foster Cybersecurity Culture.** Several security systems are already using monitoring systems to identify suspicious behavior and criminal activities. The integration of AI-ML functions in the monitoring system has enabled the processing of information, images, and audio on a larger scale. In addition, AI monitoring systems are likely to detect unauthorized humans and devices in significant quantities, by combining physical security to complement endpoint telemetry, logs, and network data with security cameras and device webcams [35].

  These changes will make it easier for countries to monitor their citizens and will reduce the associated costs [22]. Several future AI security monitoring systems designed for everyday life may not integrate value systems that consider human rights. AI technology will significantly impact basic human rights [22], including privacy, surveillance, and control, which are likely to be of the most significant issues of contention. Therefore, striking a balance between people's fundamental rights and cybersecurity will be more important than ever. Citizens will be increasingly interested in when, where, and how AI systems are used by government agencies, and the kinds of biases in AI data [36-37].

  The NCSS must consider ways to disclose how AI security systems and data are collected, stored, protected, shared, and managed to strengthen the government's credibility and ensure that national interests are intact. Furthermore, standards that encourage the ethical use of AI to balance basic human rights and security must be developed. Decision makers of NCSS should explicitly consider how to develop such a standard by establishing a council, committee, or task force. Finally, the government should strive to enhance security awareness through AI ethics education on the dangers of AI misuse and accidents targeting various actors.
- **Public-Private Partnership.** The AI security environment is a structure that cannot achieve desired results through governments or businesses alone. The success of the AI security strategy depends on the cooperation and active participation of the private and public sectors. Rather than attempting to solve AI-related problems independently, decision makers and the national security community should discuss how to collaborate with AI companies. To achieve satisfactory technical outcomes in various aspects, such as safety, security, sustainability, and long-term planning of AI security system development, continuous government investment and incentives that can be provided to companies must be considered [22]. Furthermore, while maintaining active partnerships with the private sector, cybersecurity policymakers must also establish internal guidelines on how much the country can rely on the private sector to develop AI security capabilities, or what capabilities the government should develop internally.
- **Training and Educational Program.** At the workforce level, AI use in cybersecurity has the following advantages. First, the workload of the security team is reduced. Cyber security analysts spend considerable time reviewing security logs and incident records. When AI takes care of a time-consuming and straightforward tasks, the cybersecurity analyst can spend more time and effort analyzing accidents identified by AI-based cybersecurity systems. Second, human errors and oversights can be reduced. AI-based technologies and robotic process automation technologies will ultimately strengthen the cybersecurity team's capacity to cope with low-level security threats, such as ransomware, malware, and crypto mining, among others. Finally, models can be tailored to the specific needs of the operator. Machine learning performs better on specific tasks than on a broad range of tasks [2].

When companies or nations struggle to find qualified cybersecurity professionals, AI can be a viable alternative. AI security systems cannot, however, replace every aspect of cybersecurity. Particularly, machine learning, which focuses primarily on security, is most effective when it assists "human" analysts. Utilizing AI, cybersecurity professionals should concentrate on new forms of precision threats. Therefore, AI-powered cybersecurity training should be included in the education of future cybersecurity experts.

The NCSS must consider such training and education in the future; for example, how to improve the accuracy and efficiency of security systems using ML as well as measures to compensate for weaknesses in AI systems, among others. AI security education includes re-education and retraining of existing experts, as well as newly introduced experts.

- **Effective Governance.** Effective governance is crucial for AI cybersecurity success. NCSS has not mandated a single governance structure to clarify the nation's cybersecurity strategy to date. To effectively respond to the AI cybersecurity environment, the NCSS of the future should establish a transparent, ethical, all-encompassing, and unified AI cybersecurity governance [33]. There is a need for a standardized method of collecting and organizing the government's information on its citizens.

  Governance of cybersecurity that is centralized requires the assignment of roles and responsibilities across all organizations. Moreover, such governance should include defining the role of cyber analysts, monitoring the output of algorithms, detecting abnormal behavior, identifying the risk tolerance range of the output of algorithms, establishing alternative plans in the event that algorithms fail, and defining performance metrics that objectively measure AI success.
- **Cyber Military and Counter-Intelligence.** The military will utilize AI for multiple purposes, including defense and offense. It will aid in accelerating cyber operations. Specifically, the military can use AI systems to collect vast quantities of data from enemy forces and take advantage of the increasingly asymmetrized strategy of modern warfare. The arms race of an Autonomous System is a crucial concern, as it ranges from simple upgrades and more effective weapons to the development of fully autonomous weapons and killer robots.

  AI systems and automated weapons will continue to remain an issue in the near future because no consensus exists on the available configurations for their use in the military. In addition, the military is considering adopting autonomy in the command chain using an AI security system based on data within an acceptable. The problem is that AI-automated security systems are likely to significantly impact deterrence and escalation dynamics. In the case of deterrence, people sometimes give up their arguments for better decisions in the decision-making process, but that is not possible in automation systems using AI [22]. Future NCSS must develop AI principles to guide the ethical and responsible use of AI in the military, and establishing clear international standards should be a major priority. In addition to the introduction of AI systems, it should consider how relevant personnel, such as AI security experts, can be recruited, educated, and trained to adapt to the military's unique culture.
- **Data Management: Categories to Add.** AI effectively collects, organizes, and analyzes vast amounts of data, enabling organizations to derive more value from the data. Data are the core of AI implementations and cybersecurity. AI security systems build models on the basis of data and determine the construction of proactive protection functions, the timing of alarm issuance, the determination of countermeasures to potential threats, and the response to abnormal actions. For AI technology to be effective in a cybersecurity environment, AI algorithms must be driven by the correct data system. Security data can lead to effective results only if it can provide detailed information about events that have occurred within AI security systems, such as machines, applications, protocols, and network sensors. Therefore, the NCSS of the future should consider proper access and the management of AI security data. The NCSS data strategy should be organically linked to the main content of national security and the national data strategy.

  Meanwhile, the goal of future cyberattacks involves manipulating data and algorithms, as well as simply attacking major infrastructure. Data manipulation and algorithmic interference not only have a decisive impact on decision makers but can also cause unintended conflicts and disputes, such as political friction between countries and escalations into war. Governments must provide a coherent, transparent, and standardized governance framework for sharing different data sets among government agencies, researchers, and the private sector, in conjunction with national data strategies. This framework should be aligned with the governance framework proposed by International Organization for Standardization (ISO) and Organisation for Economic Cooperation and Development (OECD).

6 CONCLUSION

The cybersecurity environment is vast and intricate, and we cannot accurately predict all the changes that will occur because this requires a great deal of trial and error, time for the introduction of new technologies, and stable social and institutional shifts. This study introduces, at an elementary level, the changes in the cybersecurity environment that will be applied to AI in the near future and the policy priorities accordingly. On the basis of the research analysis, this study predicts the future landscape that the NCSS will encounter due to the effects of AI.

The predictions are as follows: First, even though the NCSS's scope and function have been expanding over the past decade, the implementation of AI will result in further expansion. This is a natural consequence of the cyber domain permeating the social community gradually. Cybersecurity and artificial intelligence are closely intertwined, and cybersecurity is not only a security domain but also a broad domain that encompasses critical infrastructure sectors and other social domains. For a nation to successfully build an AI security environment, national policies must be incorporated

into goals and plans. The NCSS will play a crucial role in presenting the country's common goals and direction to other high-level national strategies, such as national security and defense strategies, AI strategies, information system strategies, national digital safety strategies, and big data strategies.

Second, the NCSS must establish a cybersecurity environment in which humans and systems can work together. AI-based cybersecurity solutions require close partnerships between people and systems, and in the near future, the coexistence of humans and AI security systems will become critical in the agenda for the cyberspace domain. Many people in the AI marketing industry assume that AI-based cybersecurity technology can easily replace humans. The ability to collect and process vast amounts of information is important, and AI will affect the diagnosis, decision making, and evaluation of the national security strategy establishment. However, even though AI positively improves many areas of the cybersecurity environment, AI-based security systems cannot yet fully and automatically adapt to environmental changes. In the near future, while AI technology is still not completely developed, a national-level discussion on the interdependence of AI systems and human factors is warranted, and highly trained security teams will continue to play a key role in the final decision-making stage in detecting, identifying, and protecting various cybersecurity threats.

This study is significant in that it explains the policy implications of adopting the evolving cybersecurity environment and provides insights into the evolution of the cybersecurity landscape. This study is an excellent starting point for comprehending the ebb and flow of NCSS within the AI cybersecurity environment. Given that the development and implementation of AI technology remain in their infancy, precisely analyzing changes in the nation's AI cybersecurity strategy and proposing countermeasures are challenging.

Future research must aim to understand national and global trends by specifically comparing and analyzing changes in national strategies in the AI cybersecurity environment on the basis of the NCSS and national AI strategies described by current countries.

Acknowledgments

This work was supported by the Ministry of Education of the Republic of Korea and the National Research Foundation of Korea (NRF-2020R1I1A1A01073424) and (NRF-2021R1F1A1063411).

7 REFERENCES

[1] Wirkuttis, N. & Klein. H. (2017). Artificial Intelligence in Cybersecurity. *Cyber Intelligence, and Security Journal, 1*(1), 103-119.

[2] Finnie, S. (2018). Cyber Threats with AI: Next Challenges for Security. CIO, November 6, 2018. https://www.csoonline.com/author/Scot-Finnie/

[3] Clarke, A. & Knake, R. (2014). *Cyber war*. Old Saybrook: Tantor Media, Incorporated.

[4] Yampolskiy, R. V. & Spellchecker, M. S. (2016). Artificial intelligence safety and cybersecurity: A timeline of AI failures. arXiv preprint arXiv:1610.07997.

[5] Li, J. H. (2018). Cyber security meets artificial intelligence: a survey. *Frontiers of Information Technology & Electronic Engineering, 19*(12), 1462-1474. https://doi.org/10.1631/FITEE.1800573

[6] Sarker, I. H., Furhad, M. H., & Nowrozy, R. (2021). Ai-driven cybersecurity: an overview, security intelligence modeling and research directions. *SN Computer Science, 2*(3), 1-18. https://doi.org/10.1007/s42979-021-00557-0

[7] Zhang, Z., Ning, H., Shi, F., Farha, F., Xu, Y., Xu, J., & Choo, K. K. R. (2021). Artificial intelligence in cyber security: research advances, challenges, and opportunities. *Artificial Intelligence Review*, 1-25. https://doi.org/10.1007/s10462-021-09976-0

[8] Chan, L., Morgan, I., Simon, H., Alshabanat, F., Ober, D., Gentry, J., & Cao, R. (2019, June). Survey of AI in cybersecurity for information technology management. In *2019 IEEE technology & engineering management conference (TEMSCON)*, 1-8. https://doi.org/10.1109/TEMSCON.2019.8813605

[9] Morel, B. (2011, October). Artificial intelligence and the future of cybersecurity. In *Proceedings of the 4th ACM workshop on Security and artificial intelligence*, 93-98. https://doi.org/10.1145/2046684.2046699

[10] Lazić, L. (2019, October). Benefit from Ai in cybersecurity. In *The 11th International Conference on Business Information Security (BISEC-2019)*, 18th October 2019, Belgrade, Serbia.

[11] Benzaïd, C. & Taleb, T. (2020). AI for beyond 5G networks: a cyber-security defense or offense enabler? *IEEE Network, 34*(6), 140-147. https://doi.org/10.1109/MNET.011.2000088

[12] Khisamova, Z. I., Begishev, I. R., & Sidorenko, E. L. (2019). Artificial intelligence and problems of ensuring cyber security. *International Journal of Cyber Criminology, 13*(2), 564-577. https://doi.org/10.17150/2500-4255.2019.13(4).564-574

[13] Soni, V. D. (2020). Challenges and Solution for Artificial Intelligence in Cybersecurity of the USA. Available at SSRN 3624487. https://doi.org/10.2139/ssrn.3624487

[14] Center for Strategic & International Studies (CSIS). Global Cyber Strategic Index. https://csis-website-prod.s3.amazonaws.com/s3fs-public/220414_Cyber_Regulation_Index.pdf

[15] LG CNS. (2016). Intelligence and Security. LG CNS Blog. November 7, 2016. https://blog.lgcns.com/1247

[16] Yoo, G. (2017). Correlation between Machine Learning and Information Security. SK infosec Blog. February 20, 2017. http://blog.naver.com/PostView.nhn?blogId=skinfosec2000&logNo=220937047579&parentCategoryNo=&categoryNo=8&viewDate=&isShowPopularPosts=true&from=search

[17] Perlman, A. (2019). The Growing Role of Machine Learning in Cybersecurity. SecurityRoundtable.org. Jun 18, 2019. https://www.securityroundtable.org/the-growing-role-of-machine-learning-in-cybersecurity/

[18] Kumar, S. (2019). How AI & Machine Learning Can Help With Government Cyber Security Strategies. Xlpat. July 30, 2019. https://en.xlpat.com/how-ai-machine-learning-can-help-with-government-cyber-security-strategies/

[19] Bommelaer, C. et al. (2017). Artificial Intelligence and Machine Learning: Policy Paper. Internet Society. https://www.internetsociety.org/resources/doc/2017/artificial-intelligence-and-machine-learning-policy-paper/

[20] Allen, G. & Chan, T. (2017). Artificial intelligence and national security. Cambridge (MA): Belfer Center for Science

and International Affairs. https://www.belfercenter.org/publication/artificial-intelligence-and-national-security
[21] Brundage, M. et al. (2018). The malicious use of artificial intelligence: Forecasting, prevention, and mitigation. arXiv preprint arXiv:1802.07228.
[22] Newman, J. (2019). *Toward AI security: global aspirations for a more resilient future*. Center for long-Term Cybersecurity, UC Berkeley.
[23] Klimburg, A. (2012). *National cyber security framework manual*. NATO Cooperative Cyber Defense Center of Excellence.
[24] Lewis, J. A. (2018). *Rethinking Cybersecurity: Strategy, Mass Effect, and States*. Lanham: Rowman & Littlefield.
[25] Harknett, R. & Tever, J. (2011). The new policy world of cybersecurity. *Public Administration Review 71*(3), 455-460. https://doi.org/10.1111/j.1540-6210.2011.02366.x
[26] Elkhannoubi, H. & Belaissaoui, M. (2015). Fundamental pillars for an effective cybersecurity strategy. In *2015 IEEE/ACS 12th International Conference of Computer Systems and Applications (AICCSA)*. https://doi.org/10.1109/AICCSA.2015.7507241
[27] Shafqat, N. & Masood, A. (2016). Comparative analysis of various national cyber security strategies. International *Journal of Computer Science and Information Security, 14*(1), 129-136.
[28] Ciglic, K., Mckay, A. et al. (2018). *Cybersecurity Policy Framework: A practical guide to the development of national cybersecurity policy*. Microsoft.
[29] ENISA. (2016). NCSS good practice guide: Designing and Implementing National Cyber Security Strategies.
[30] ITU. (2018). Guide to developing a national cybersecurity strategy - Strategic engagement in cybersecurity. https://www.itu.int/pub/D-STR-CYB_GUIDE.01-2018
[31] Osula, A.-M. & Kaska, K. (2013). *National Cyber Security Strategy Guidelines*. CCDCOE.
[32] Salamzada, K. et al. (2015). A Framework for Cybersecurity Strategy for Developing Countries: Case Study of Afghanistan. *Asia-Pacific Journal of Information Technology and Multimedia, 4*(1), 1-10. https://doi.org/10.17576/apjitm-2015-0401-01
[33] Chbib, A. (2019). How AI and Machine Learning Can Help With Governmental Cybersecurity Strategies. *Intelligent HQ*. January 3, 2019. https://www.intelligenthq.com/how-ai-and-machine-learning-can-help-with-governmental-cybersecurity-strategies/
[34] Garcia-Tobar, A. (2019). The Promise and Limitations of AI in Cybersecurity. Nextgov. April 4, 2019. https://www.nextgov.com/ideas/2019/04/promise-and-limitations-ai-cybersecurity/ 156064/
[35] Shomo, P. (2019). Security AI, there's a bubble, but... Three things to do vs. two things not to do. CIO. April 23, 2019. http://www.ciokorea.com/news/121556#csidx4b5108de9ce95f0b36115c983e84248 (in Korean)
[36] Briner, A. (2019). AI & National Security: A Primer. INKSTICK. June 18, 2019. https://inkstickmedia.com/ai-national-security-a-pr Cybersecurity imer/
[37] Park, D. W. (2013). Analysis and Comparison of Regulations for National Cybersecurity. *International Journal of Security and Its Applications, NADIA, 10*(10), 207-214. https://doi.org/10.14257/ijsia.2016.10.10.19

Authors' contacts:

Geunhye Kim, Research Professor
Institute of Cyber Security & Privacy, Korea University,
145, Anam-ro, Seongbuk-gu, Seoul, Korea
geunhyekim1@gmail.com

Kyudong Park, Professor
(Corresponding author)
Department of Public Administration, University of Seoul,
163 Seoulsiripdaero, Dongdaemun-gu, Seoul 02504, Korea
kdpark@uos.ac.kr