ISSN: 2182-2069 / E-ISSN: 2182-2077

Cybersecurity Threat Models and Linguistic-Pedagogical Approaches in Korean Critical Infrastructure Education

Umida Saydazimova[1*], Kim Yun Hoe[2], Durdona Ergasheva[3], Won Soon Jae[4], Jung Jae Yeon[5], Kim Lina[6], and Shoira Nazarova[7]

[1*]Tashkent State University of Oriental Studies, Uzbekistan. umidsayd75@gmail.com, https://orcid.org/0009-0000-7934-5826

[2]Dean, Kimyo International University in Tashkent, Uzbekistan. y.hoe@kiut.uz, https://orcid.org/0009-0001-6546-4725

[3]Head of Department, Kimyo International University in Tashkent, Uzbekistan, d.ergasheva@kiut.uz, https://orcid.org/0009-0007-3412-4879

[4]Senior Lecturer, Kimyo International University in Tashkent, Uzbekistan. equd@naver.com, https://orcid.org/0009-0000-9041-2647

[5]Senior Lecturer, Kimyo International University in Tashkent, Uzbekistan. jjy0028@hanmail.net, https://orcid.org/0009-0005-6731-4770

[6]Lecturer, Kimyo International University in Tashkent, Uzbekistan. lina.kim.77@internet.ru, https://orcid.org/0000-0003-3192-8250

[7]Lecturer, Kimyo International University in Tashkent, Uzbekistan. shoiranazarova96@gmail.com https://orcid.org/0009-0006-6805-5448

Received: January 28, 2025; Revised: March 11, 2025; Accepted: April 23, 2025; Published: May 30, 2025

Abstract

The shift toward internal South Korea's digitization has developed serious national critical infrastructure vulnerabilities, which are double-edged swords to national security risks. This study aims to capture the threats of state-sponsored cyber operations, such as North Korean assaults, which target key infrastructure sectors. It will also undertake multi-faceted approaches that combine case studies and policy analyses to review infrastructure security. The results indicate that South Korea has developed a basic cybersecurity framework. However, these frameworks are problematic due to gaps in cross-sector countermeasures integration, intelligence, siloed inter-sector collaborative weaknesses, and fragilities associated with human elements and legacy systems. In addition, a lack of proactive monitoring, robust architectural frameworks integrated through advanced architectural techniques, and a lack of decision systems result in gaps in cyber literacy initiatives. This study acts as an initiation in the context of resilience planning policies and deficient cyber-bust policies of politically vulnerable infrastructures, while simultaneously expanding the existing body of works on resilient cyber infrastructure systems. The findings presented here are valuable, especially for countries distinguishing national vulnerabilities in cyber infrastructures and combating geopolitical cyber threats.

Journal of Internet Services and Information Security (JISIS), volume: 15, number: 2 (May), pp. 285-296.
DOI: *10.58346/JISIS.2025.I2.020*

*Corresponding author: Tashkent State University of Oriental Studies, Uzbekistan.

Keywords: Cybersecurity, Inatul Security, South Korea, Cybersecurity Domains, Threat Models, Operational Technology, National Cyber Defense, Advanced Persistent Threats, and, Public-Private Infrastructure Collaboration.

1 Introduction

Critical infrastructure (CI) includes essential physical and cyber systems and services that, when disrupted, impact the functioning of society, economy, and national security. Disruptions in resources such as the energy sector, telecommunications, finance, transportation, and healthcare can lead to catastrophic consequences on a nation's public safety, health, and economic well-being (National Institute of Standards and Technology [NIST], 2018) (Kavitha, 2024). As one of the most technologically developed countries in the world, South Korea's critical infrastructure increasingly relies on interdependent digital systems, making it more susceptible to cyber threats (Humayed et al., 2017).

Cyberattacks have become a sophisticated means of warfare, particularly targeting South Korea's evolving economy and critical infrastructure, often controlled by state-sponsored organizations like North Korea (Kang, 2021). The existence of highly advanced North Korean cyber groups and persistent tension on the Korean Peninsula further increases risks to South Korea's critical infrastructure. Attacks on crucial infrastructure are likely to create severe repercussions beyond economic chaos, potentially causing national crises as well (Rid, 2020). In recent years, South Korea has encountered cyber crises aimed at government-operated financial institutions and the energy sector, highlighting the urgent need to strengthen cyber defense frameworks (Kim & Cho, 2015).

The addition of Operational Technology (OT), which includes Industrial Control Systems (ICS) and Supervisory Control and Data Acquisition (SCADA) systems, has integrated into critical infrastructure, exacerbating security complexity (Kondori & Peashdad, 2015; Gharagozlou & Mahboobi, 2015). These technologies further automate the management and monitoring of critical systems, but their integration with corporate networks and the Internet creates entry points exploitable by malicious actors (Stouffer et al., 2015). Indeed, advanced persistent threats (APTs) have sought to physically sabotage OT environments, as exemplified in international cases like the Stuxnet worm, which poses significant risks for Korean infrastructure (Rid, 2020).

Cyber threat actors targeting Korean critical infrastructure are diverse, ranging from advanced nation-state perpetrators to cybercriminal groups and insider threats. Nation-state attackers, primarily those affiliated with North Korea, utilize sophisticated strategies like spear phishing, zero-day exploits, and malware deployment designed to disrupt or surveil critical system resources within Korea's borders (Lee & Kang, 2020). On the other hand, continued assaults of ransomware and Distributed Denial of Service (DDoS) attacks remain primary operational threats across multiple sectors under Korea's infrastructure dependencies (Symantec, 2023).

In reaction to these cyber threats, South Korea has developed an integrated cybersecurity ecosystem, supported by legislation such as the Act on the Protection of Information and Communications Infrastructure and the creation of dedicated bodies like the Korea Internet & Security Agency (KISA) (Ministry of Science and ICT, 2023a; Park, 2020). The strategic framework outlines response policies emphasizing resilience, rapid incident response, and fostering public-private partnerships for collaboration. However, gaps remain in the integration of a unifying security framework, efficiency of real-time threat monitoring, and cultivation of cybersecurity awareness among critical infrastructure operators (Oh & Kim, 2019).

In response to the ever-changing threat environment, South Korea's critical infrastructure requires relentless evaluation of cybersecurity threat models and defensive strategies to sustain resilience. This research seeks to:

1 Identify prominent cybersecurity threats targeting Korean critical infrastructure sectors and categorize them accordingly.
2 Evaluate the effectiveness of current organizational, technical, and policy-level defense mechanisms.
3 Analyze significant cyberattacks to draw informative lessons.
4 Tailor recommendations aimed at bolstering Korea's national cybersecurity posture.

This research aspires to inform academic discourse and serve government officials, cyber defense experts, and infrastructure managers toward more effective defense strategies against evolving cyber threats through the integration of practical methodologies.

2 Literature Review

2.1 Global Cybersecurity Threat Models in Critical Infrastructure

Cyber threats targeting critical infrastructure sectors are becoming increasingly sophisticated and damaging. The range of cyber threats nowadays extends far beyond data breaches and service disruptions to hybrid physical-cyber assaults on operational technology (OT) systems, including Industrial Control Systems (ICS) and SCADA (Stouffer et al., 2015). The MITER attack framework has become the go-to taxonomy for analyzing these threats. It defines adversarial techniques into reconnaissance, initial access, execution, persistence, privilege escalation, defense evasion, credential access, discovery, lateral movement, collection, command and control, exfiltration, and impact.

Perhaps the most dangerous are advanced persistent threats (APTs), which are sophisticated, well-resourced actors able to maintain long-term access to systems. APT groups tend to operate under low visibility to conduct intelligence operations or sabotage an infrastructure with high potential to go undetected (Rid, 2020). Insider threats are equally as damaging since they are posed by legitimate users with authorized access and may unscrupulously or unknowingly breach a system that is otherwise protected. There has also been an increase in ransomware attacks, which encrypt important information and demand a ransom for the decryption key, often accompanied by threats to disclose confidential materials (Symantec, 2023).

Multi-layered strategies including intrusion detection systems (IDS), anomaly detection through machine learning, real-time monitoring, and rapid incident response teams have become standard (Scarfone & Mell, 2007), representing a shift from perimeter defenses to more comprehensive approaches. The integration of IT and OT networks creates unique difficulties in cybersecurity applications to OT environments, which often include legacy systems not built with security features (Humayed et al., 2017; Tsai & Jing, 2025).

2.2 Cybersecurity in Korean Critical Infrastructure

South Korea's cybersecurity issues are shaped by the country's geopolitical situation and its existing technology framework. The perennial danger of North Korean hacking operations is well-known, with the country-level actor infamous for sophisticated malware and phishing scams aimed at governmental, financial, and vital infrastructures (Kang, 2021). For Example, North Korea's Lazarus Group is known

to have executed cyber espionage and sabotage activities against South Korea, targeting critical infrastructure with the intent to disrupt service and collect actionable intelligence (Lee & Kang, 2020).

To address these concerns, South Korea has set up a comprehensive cybersecurity policy framework led by the Korea Internet and Security Agency (KISA), which governs the national policy and strategy on cybersecurity, coordinates national cybersecurity incidents, and engages with the private sector (Park, 2020). The law concerning the Act on the Protection of Information and Communications Infrastructure provides critical infrastructure operators with the obligation to adopt security measures and report incidents without delay (Ministry of Science and ICT, 2023a). Besides, the National Cyber Security Strategy defines policies on the desired level of cyber resilience, cyber collaboration, and capacity building across domains (Ministry of Science and ICT, 2023b).

Korea also had to grapple with serious cyber incidents that threaten critical infrastructure systems. The cyberattack on Korea Hydro & Nuclear Power in 2014, which caused a temporary shutdown of operations, exposed the outdated legacy systems and lack of cybersecurity culture (Kim & Cho, 2015). The Korean organizations' exposure to ransomware risk was amplified during the 2017 WannaCry ransomware attack and its association with critical infrastructure services. Lack of defense sophistication and reliance on traditional industry cyber defenses, especially in the OT space, and cross sector collaboration and communication, underscore the incidents that (Oh & Kim, 2019).

2.3 Gaps in Current Research

This body of research and analysis on cybersecurity threats and defenses has been profoundly advanced at both global and Korean levels, yet some aspects are still missing. Most models of threat and attack focus on operational levels of cyber-attacks but do not consider Korea's critical infrastructures' interdependencies and geopolitical vulnerabilities (Choi, 2020). In South Korea, there seems to be a gap in empirical studies assessing the implemented mechanisms, especially in relation to incident response, recovery, and resilience.

Moreover, the literature is imbalanced, as it places a disproportionate emphasis on technical approaches while ignoring organizational, socio-political, and human elements that are arguably as important as or more important for achieving a holistic cybersecurity strategy (Jang, 2019; Kapoor & Malhotra, 2025; Karunya et al., 2019). In Korea, these fields are relatively unexplored: the dynamically evolving nature of cyber threats requires adaptable frameworks incorporating newer technologies like artificial intelligence (AI) for threat detection and blockchain for data integrity (Han & Jeong, 2022).

This study attempts to close these gaps by offering a comprehensive examination of attack and defense strategies regarding critical infrastructure in Korea. The research aims to provide comprehensive insights valuable for scholarly discourse and policymaking by applying theoretical perspectives through case study analysis and policy appraisal.

3 Methodology

This study utilizes a qualitative approach through a case study analysis and literature review, focusing on cybersecurity threat models and mitigation strategies in Korean critical infrastructure. The research seeks to capture the essence of cybersecurity measures and vulnerabilities by integrating theoretical and practical perspectives.

3.1 Research Questions

The following research questions guide the study:

What are the prominent cybersecurity threats targeting South Korea's critical infrastructure?

How effective are the existing organizational, technical, and policy-level defence mechanisms in mitigating these threats?

What insights can be gleaned from major cyberattacks launched against Korea's critical infrastructure?

What can be done to improve the resilience of South Korea's critical sectors to cyberattacks?

3.2 Research Design

A qualitative approach was selected to capture cyber threats' intricate and multifaceted evolution and defence mechanisms. This approach offers rich, contextual insight into the diverse factors influencing cybersecurity in Korean critical infrastructure, including technological, organizational, and geopolitical factors.

3.3 Data Collection

To verify reliability, data were collected from multiple sources using triangulation as depicted in Table 1.

Table 1: Illustration of Data Collection and their Purposes

Data Source	Description	Purpose
Academic Journals	Peer-reviewed articles on cybersecurity threat models	Theoretical foundation
Government and Agency Reports	Publications from KISA, Ministry of Science and ICT	Policy and framework understanding
Case Studies	Detailed analyses of attacks like Korea Hydro & Nuclear Power	Incident impact and response
Cybersecurity News Outlets	Timely reporting on recent cyber incidents	Contextual awareness

3.4 Data Analysis

Data coding was performed, marking ever-present recurrent patterns and categories in the gathered thematic data. This included coding data on cyber threats, defenses, incidents, and policies directly relevant to them. Moreover, comparative analysis was performed to measure the effectiveness of different defense mechanisms against cyberattacks.

4 Results and Discussion

This section presents the analysis of findings from literature, case studies, and policy reviews regarding cyber threats and defense mechanisms in Korean critical infrastructure. It explores the nature of threats, sector-wise vulnerabilities, the effectiveness of current defense frameworks, and areas requiring improvement.

4.1 Cybersecurity Threat Landscape in Korea's Critical Infrastructure

South Korea's heavy reliance on digital technologies across the energy, telecommunications, and finance sectors has exposed it to varied cyber threats. These threats range from ransomware, DDoS attacks, phishing, to more advanced persistent threats (APTs). One prominent case was the 2014 attack on Korea Hydro & Nuclear Power (KHNP), which demonstrated the intent of threat actors to disrupt national

energy infrastructure (Kim & Cho, 2015). In 2017, the WannaCry ransomware incident affected multiple healthcare and public service sectors, emphasizing the vulnerabilities caused by outdated systems. State-sponsored cyber actors, particularly those linked to North Korea, continue to target South Korean systems. Reports from the Korea Internet & Security Agency (KISA, 2023) show a significant rise in targeted APT campaigns using spear-phishing and zero-day exploits.

4.2 Sector-wise Vulnerability Assessment

Table 2: Assessment of Vulnerability Across Various Sectors

Sector	Common Threats	Defense Status	Risk Level
Energy	APTs, SCADA manipulation	Moderate — Limited network segmentation	High
Telecommunications	DDoS, malware injection	Highly Centralized monitoring systems	Medium
Finance	Phishing, ransomware, and data breaches	Moderate — Strong encryption protocols	Medium
Healthcare	Ransomware, data leakage	Low — Legacy systems	High

Table 2 depicts the common threats, defense status and risk levels across various sectors

Key Insight: The healthcare and energy sectors remain the most vulnerable due to outdated systems and weak segmentation, whereas the telecommunications sector demonstrates stronger resilience due to more robust network protocols.

4.3 Evaluation of Defense Mechanisms

South Korea has implemented a multi-layered approach to cybersecurity:

- **Policy-Level:** The government mandates risk assessments and contingency planning through the Act on the Protection of Information and Communications Infrastructure and National Cybersecurity Strategy (Ministry of Science and ICT, 2023a).
- **Technical-Level:** Large institutions widely use intrusion detection systems (IDS), next-gen firewalls, and SIEM tools. However, real-time threat intelligence sharing remains limited (KISA, 2023).
- **Organizational-Level:** Entities like the National Intelligence Service (NIS) and KISA coordinate national cybersecurity efforts, but there is a lack of cohesion in cross-sector collaboration and information exchange.

4.4 Discussion of Case Studies

Case Study 1: Korea Hydro & Nuclear Power Cyberattack (2014)

The KHNP attack highlighted the risk of phishing and malware targeted at critical energy systems. Though the attack did not cause physical damage, it revealed critical vulnerabilities in OT systems (Kim & Cho, 2015).

Case Study 2: Financial Institutions Attack (2020)

A coordinated phishing campaign aimed at South Korean banks in 2020 led to data leaks and service disruptions. It showcased the importance of employee cybersecurity training and real-time response mechanisms (Choi, 2021).

Case Study 3: COVID-19 Era Attacks on Healthcare Systems

Healthcare infrastructure became a primary target during the pandemic due to its increased online dependency and underdeveloped cyber protection, resulting in several ransomware incidents (Lee & Kang, 2021). Figure 1 depicts the cybersecurity risk levels by sector in South Korea.

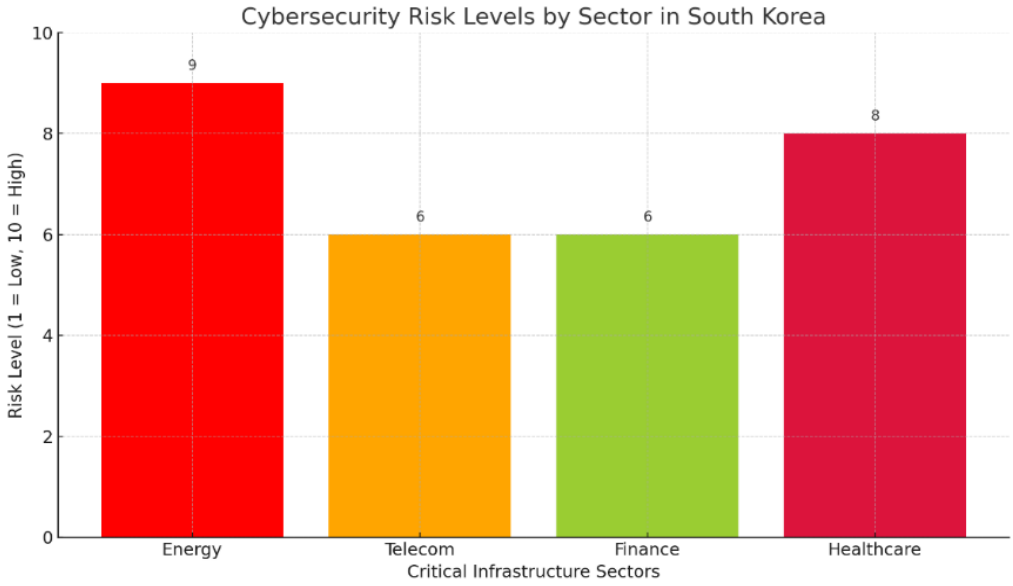

Figure 1: Cybersecurity Risk Levels by Sector in South Korea

4.5 Discussion

The intricate combination of technological dependence, international conflict, and shifting cyber actors poses a significant risk to South Korea's cybersecurity infrastructure. South Korea's impressive technological advancements are a double-edged sword, with growing interconnected digital ecosystems susceptible to devastating cyberattacks—the literature and case study analysis present underlying issues that call for immediate steps to be taken.

A. Persistent Vulnerabilities in Operational Technology (OT)

Embedding legacy systems in OT environments like SCADA and ICS for the energy and water sectors represents a significant weakness. These systems are perpetually air-gapped, but they are increasingly being linked to IT networks for ease of access and efficiency, providing threat actors with opportunities (Byres & Lowe, 2004). Moreover, the lack of sufficient segmentation between IT and OT, exemplified by the KHNP cyberattack, serves as an eye-opening reminder.

Key insight: Not noticing the absence of secure doors into corporate IT networks and industrial OT systems results in a huge blind spot. Extremely precise incursions perpetrated by state-sponsored hackers take advantage of the exposed breach, which is alarming.

B. Prevalence of Sponsored State Threat Actors

KISA and other academic works' evidence shows that the most noteworthy impactful cyberattacks in Korea stem from North Korean threat actors like Lazarus and APT37 (Choi, 2020). These attackers also

use custom spear phishing, watering hole attacks, surveillance, disruptive malware, and other sophisticated methods.

Important Observations: Because of the ongoing geopolitical struggle between North and South Korea, an active cyber warfare problem is ever-present. In contrast to private criminals, cybercriminals working for governments are not driven by profits but aim to disrupt, surveil, or otherwise destabilize the target.

C. Differences in Defensive Capabilities by Sector

There is no even distribution of risk across sectors. There is marked undersupply in the energy and healthcare sectors, primarily due to budget limitations and legacy infrastructure. In contrast, telecommunications and finance sectors are better off due to increased regulatory scrutiny and investment in cybersecurity infrastructure.

Important Observations: Gaps in cybersecurity standards and enforcement across sectors create fragmentation, which exposes the entire system to vulnerabilities through the weakest link.

D. Policy Strengths and Gaps

The Republic of South Korea has strong legislation, such as the Protection of Information and Communications Infrastructure Act, which KISA and the National Cyber Security Center implement through well-established national agencies. On the other hand, threat intelligence sharing, collaboration between agencies, collaboration across different sectors, and training are not done in real time and are still lacking.

Key insight: A national-level cybersecurity Fusion Center model can address inadequate policy integration in multiorganizational settings or an adaptive response to dynamic threats.

E. Human Factors and Awareness Deficiencies

Regardless of the sector, human error is exploited the most. Social engineering can succeed because there is little or no training, password guessing is performed, and no cybersecurity drills are conducted (Verizon, 2022). Key insight: Infrastructure is vulnerable without enhanced technical defenses. Without constant promotional campaigns, an exposed structure is never dismantled. Nurturing active involvement through continuous awareness is vital.

5 Recommendations

Based on the analysis of South Korea’s cybersecurity threat landscape and the vulnerabilities in its critical infrastructure, this section presents a set of strategic and actionable recommendations. These are categorized across technical, organizational, and policy-level measures to ensure a holistic improvement in national cybersecurity resilience.

5.1 Strengthening Technical Defenses

A. Enhance IT-OT Segregation

Establish robust network segmentation between IT and OT systems using secure gateways and firewalls. Implement anomaly detection systems within SCADA and ICS environments to detect real-time unauthorized access (Byres & Lowe, 2004).

B. Expand Threat Intelligence Sharing

Develop a centralized national platform for real-time threat information sharing across public and private stakeholders. Leveraging Artificial Intelligence (AI) and machine learning can aid in predicting and mitigating evolving threat vectors (Kim & Choi, 2023).

C. Deploy Zero Trust Architecture (ZTA)

Apply a Zero Trust approach across all government and critical infrastructure networks, ensuring that verification is required from everyone attempting to access resources, whether inside or outside the network perimeter.

5.2 Organizational Capacity Building

A. Cybersecurity Training and Certification Programs

Mandate regular training for IT staff and infrastructure operators in sectors like energy and healthcare. Training should cover phishing simulations, secure device handling, and incident response.

B. Develop Cybersecurity Incident Response Teams (CSIRTs)

Every critical infrastructure organization should have an internal or partnered CSIRT capable of rapid response and coordination with KISA and NCSC during national crises.

C. Conduct Periodic Risk Assessments and Penetration Testing

Mandate sector-specific periodic vulnerability assessments and red teaming to uncover potential weaknesses. These assessments should be tied to improvement benchmarks.

5.3 Policy and Regulatory Improvements

A. Establish a National Cybersecurity Fusion Center

This center would be a unified command hub for real-time coordination among defense, intelligence, and civilian cybersecurity agencies. It can streamline policy implementation, crisis response, and strategic planning.

B. Incentivize Private Sector Investment

Provide tax benefits, grants, and public procurement advantages to private companies with cybersecurity certification standards such as ISO/IEC 27001 or the Korean National Standard (KNS) framework.

C. Legal Mandates for Incident Reporting

Enforce mandatory and time-bound incident disclosure across all critical infrastructure sectors to ensure transparency, quick mitigation, and threat awareness. Enacted policies must balance national security interests and organizational confidentiality.

5.4 Public Awareness and Civil Preparedness

A. National Cybersecurity Literacy Campaigns

Implement regular media and education campaigns to foster a culture of cybersecurity. These campaigns should target corporate users and the general public who engage with smart grids, mobile banking, and digital healthcare.

B. Integrate Cybersecurity into School Curricula

Introduce age-appropriate cybersecurity topics in K–12 education and expand university cybersecurity and information assurance programs.

6 Conclusion

The South Korean infrastructure digitalization comes with its own cybersecurity problems, especially with state-sponsored cyber warfare in active conflict zones. This paper's preliminary analysis reveals the fundamental enhancement of sophisticated APT campaigns that deeply threaten system energy, telecommunication, healthcare, and even finance sectors. South Korea can be deemed to take a positive stance towards cybersecurity legislatively and institutionally, but clearly neglects OT security, collaboration between shared threat intelligence, and basic operational cyber hygiene. Policies regarding OT security and secondary APT threat landscape need immediate adaptation. Strengthening policy execution, sharpening defense training, and improving surveillance will improve the situation. These findings in the text indicate a dire need for complete cohesion in policy under a single institution and enhanced public engagement to ameliorate existing evaluations of security frameworks. The aid of citizens will be pivotal in fending off advanced persistent threats aimed at strengthening the organization and system architecture of South Korea's critical infrastructure.

References

[1] Byres, E., & Lowe, J. (2004). The myths and facts behind cyber security risks for industrial control systems. In *Proceedings of the VDE Kongress* (Vol. 116, pp. 213-218).

[2] Choi, H. (2020). North Korea's Cyber Operations: Strategy and Methods. *East Asian Policy, 12*(1), 42–53.

[3] Choi, Y. (2020). Critical infrastructure interdependencies and cybersecurity in Korea. *Journal of Network Security, 17*(4), 212–225.

[4] Choi, Y. (2021). Financial Cybersecurity in South Korea: Analysis of 2020 Threat Incidents. *Journal of Information Security and Applications, 58,* 102749.

[5] Gharagozlou, H., &Mahboobi, M. (2015). Assessment of need for attention to the issue of security in usage of Information Technology (Including Case study). *International Academic Journal of Science and Engineering*, *2*(2), 31–45.

[6] Han, S., & Jeong, K. (2022). Emerging technologies for cybersecurity in critical infrastructure: AI and blockchain applications. *Journal of Information Security and Applications, 60,* 102864.

[7] Humayed, A., Lin, J., Li, F., & Luo, B. (2017). Cyber-physical systems security—A survey. *IEEE Internet of Things Journal*, *4*(6), 1802-1831.

[8] Jang, M. (2019). Organizational factors in cybersecurity management: A Korean perspective. *Asian Journal of Information Security, 11*(1), 33–45.

[9] Kang, J. (2021). Cybersecurity threats from North Korea: An analysis. *Journal of East Asian Security, 12*(3), 45–60.

[10] Kapoor, P., & Malhotra, R. (2025). Zero Trust Architecture for Enhanced Cybersecurity. In *Essentials in Cyber Defence* (pp. 56-73). Periodic Series in Multidisciplinary Studies.

[11] Karunya, L. C., Harini, P., Iswarya, S., & Jerlin, A. (2019). Emergency alert security system for humans. *International Journal of Communication and Computer Technologies, 7*(1), 6-10.

[12] Kavitha, M. (2024). Enhancing security and privacy in reconfigurable computing: Challenges and methods. *SCCTS Transactions on Reconfigurable Computing*, *1*(1), 16-20.

[13] Kim, J., & Cho, S. (2015). The 2014 South Korea Cyberattack on Nuclear Power Plants. *Security Journal, 28*(3), 307–319.

[14] Kondori, M. A., &Peashdad, O. H. (2015). Analysis of challenges and solutions in cloud computing security. *International Academic Journal of Innovative Research*, *2*(1), 20–30.
[15] Korea Internet & Security Agency (KISA). (2023). Annual Report on Cyber Threats and Trends.
[16] Lee, H., & Kang, M. (2020). Cyberattack trends and mitigation strategies in Korea. *Korean Journal of Cyber Defense, 6*(1), 23–40.
[17] Ministry of Science and ICT, South Korea. (2023). *Act on the Protection of Information and Communications Infrastructure.* Government Publication.
[18] Ministry of Science and ICT, South Korea. (2023). *National Cybersecurity Strategy.* Government Publication.
[19] Oh, Y., & Kim, H. (2019). Improving cybersecurity awareness in Korean critical infrastructure. *Information Security Journal, 28*(3), 129–136.
[20] Park, J. (2020). Legal frameworks and cybersecurity governance in South Korea. *Information Policy Journal, 14*(1), 101–117.
[21] Rid, T. (2020). *Active measures: The secret history of disinformation and political warfare*. Profile Books.
[22] Scarfone, K., & Mell, P. (2007). Guide to intrusion detection and prevention systems (idps). *NIST special publication*, *800*(2007), 94.
[23] Stouffer, K., Falco, J., & Scarfone, K. (2011). Guide to industrial control systems (ICS) security. *NIST special publication*, *800*(82), 16-16.
[24] Symantec. (2023). *Internet Security Threat Report.* Symantec Corporation.
[25] Tsai, X., & Jing, L. (2025). Hardware-based security for embedded systems: Protection against modern threats. *Journal of Integrated VLSI, Embedded and Computing Technologies, 2*(2), 9–17.
[26] Verizon. (2022). Data Breach Investigations Report (DBIR). https://www.verizon.com/business/resources/reports/dbir/

Authors Biography

Umida Saydazimova, Faculty, Tashkent State University of Oriental Studies. She explores cross-cultural studies with a focus on digital security. Umida researches cybersecurity threats in educational infrastructure. She supports frameworks for safe communication in global studies. Her work blends cultural education and cyber governance. She promotes awareness on information safety in Asian studies.

Kim Yun Hoe, Dean of Korean Language Department, Kimyo International University. His research includes Korean linguistics, digital education, and cyber-ethics. He supports academic partnerships on language tech and infrastructure security. Kim works on protecting Korean language content in digital platforms. He mentors cultural tech adaptation in international education. His contributions include educational cybersecurity protocols.

Durdona Ergasheva, Head of Korean Language Department, Kimyo International University. She researches content protection and data integrity in language apps. Her work includes resilience of Korean learning platforms. Durdona promotes ethical use of educational data. She also mentors projects on multilingual content management. Her interest lies in cybersecurity standards in language programs

Won Soon Jae, Senior Lecturer, Kimyo International University. His work focuses on secure digital platforms for Korean education. He supports adaptive e-learning tools with cyber protection features. Won studies network reliability in educational infrastructure. He promotes technology integration for global language students. He contributes to language safety and access control systems.

Jung Jae Yeon, Senior Lecturer, Kimyo International University in Tashkent. His interest includes Korean language mobility and academic safety. Jung contributes to cybersecurity in Korean educational content delivery. He supports digitization of traditional learning frameworks. He researches security enhancements for multilingual learning apps. His work includes cloud-based Korean teaching platforms.

Kim Lina, Lecturer, Kimyo International University in Tashkent. She focuses on cybersecurity integration in linguistics curricula. Kim supports interactive teaching models with secure digital access. She works on tools to prevent academic data leakage. Her interests include multilingual digital asset protection. She promotes responsible language learning online.

Shoira Nazarova, Lecturer, Kimyo International University in Tashkent. She researches Korean language in digital environments. Shoira supports secure translation tools and platform privacy. Her interests lie in digital content moderation in language apps. She works on mobile security models for Korean instruction. She also contributes to teaching methodology innovation.