JRSR
JOURNAL OF REGIONAL STUDIES REVIEW

Journal of Regional Studies Review (JRSR)
Volume 4, Issue 1 (Winter 2025) | Pages: 1–14
ISSN (Online): 3006-6646
Digital Object Identifier (DOI): 10.62843/jrsr/2025.4a046
Correspondence should be addressed to Purwa Roshan; Purwaroshan@gmail.com

RESEARCH ARTICLE

The Evolving Cyber Landscape: Capabilities and Cyber Diplomatic Efforts of Korean Peninsula

Purwa Roshan [a]

Abstract: Cybersecurity has emerged as a critical domain in global politics, posing significant threats to economy, national security and the integrity of states. Korean peninsula, with its geopolitical dynamics in East Asia featuring south Korea as an emerging technological power, and the historically rival between North and South Koreas, holds particular importance. This region encompasses technologically advanced state, as well as a globally isolated state that remains wary of cyber warfare threats. As the scope of cyber politics expands, states have recalibrated their foreign policies, prioritizing cyber diplomacy as a key component of their strategic approach. This study tends to explore the policy implications mainly focusing on regional and international cooperation in order to initiate confidence-building measures and capacity-building the participating states. This research seeks to explain the cyber threat because of the strategic interconnectedness from the central concept of the al security and international cooperation by using the theory of neo-realism and neo-liberalism. The theoretical framework offers valid arguments to examine how the international cooperative measures and the inclusion of the strategic policies regarding cyber threats strengthen the strategic outreach of the states (South Korea, USA, Japan) to maintain their regional political positions and edge over North Korea. Moreover, the research investigates and elaborates the dynamics that drove the cyber politics from level of low politics to high politics and provide an analytical insight over the cyber diplomatic efforts of the states to maintain the global peace and security.

Keywords: Cyber-Politics, Korea Peninsula, Cyber Diplomacy, International Cooperation, Confidence Building Measures, Capacity Building, ASEAN, EU

Introduction

Cyber-security has emerged as a critical domain in global politics, posing significant threats to economy, national security and the integrity of states. East Asia, with its geopolitical dynamics featuring China as an emerging power, Japan, and the historically rival Koreas, holds particular importance. This region encompasses technologically advanced states, as well as a globally isolated state that remains wary of cyber warfare threats. As the scope of cyber politics expands, states in East Asia have recalibrated their foreign policies, prioritizing cyber diplomacy as a key component of their strategic approach. As the global digital landscape continues to evolve at a rapid pace, there is growing apprehension regarding the long-term viability of the internet's positive impact on state security and world politics. Until recently, cyberspace was primarily regarded as belonging to the realm of low politics, referring to background conditions and routine decisions and processes. In contrast, high politics encompassed matters related to national security, core institutions, and decision systems critical to the state and its fundamental values. High politics traditionally involved concerns such as nationalism, political participation, political disputes, conflict, violence, and warfare. However, in recent years, the significance of cyberspace and its applications has elevated it to the highest level of high politics (Zhukov, 2020). As the digital world becomes increasingly interconnected, the presence of diverse value systems amplifies the potential for misunderstandings and conflicts. Various cyber-specific advancements exacerbate the challenges and creates the environment of mistrust among nations in the realm of cyberspace (Pawlak, 2015).

[a] M.Phil. Scholar, University of Management and Technology, Lahore, Punjab, Pakistan. Email: Purwaroshan@gmail.com

Cite this Article: Roshan, P. (2025). The Evolving Cyber Landscape: Capabilities and Cyber Diplomatic Efforts of Korean Peninsula. *Journal of Regional Studies Review, 4*(1), 1-14. https://doi.org/10.62843/jrsr/2025.4a045

The Korean Peninsula, consisting of North Korea and South Korea, is a region known for its unique dynamics and complex geopolitical situation. In addition to the traditional political tensions, the Korean Peninsula is also a battleground in the realm of cyberspace. Both North Korea and South Korea have demonstrated significant cyber capabilities and face ongoing cyber threats from various sources. Until recently, cyberspace was primarily regarded as belonging to the realm of low politics, referring to background conditions and routine decisions and processes. In contrast, high politics encompassed matters related to national security, core institutions, and decision systems critical to the state and its fundamental values. High politics traditionally involved concerns such as nationalism, political participation, political disputes, conflict, violence, and warfare. However, in recent years, the significance of cyberspace and its applications has elevated it to the highest level of high politics (Zhukov, 2020).

The Republic of Korea's 2024 National Cybersecurity Strategy marks a significant shift from a defensive to an offensive cybersecurity posture, prioritizing proactive measures against North Korea, which is explicitly identified as the primary threat due to its persistent cyberattacks. The strategy emphasizes attribution through scientific evidence while remaining vague on proportional responses to cyber incidents. It also focuses on bolstering infrastructure resilience by implementing minimum-security requirements, rapid response teams, a 'Zero Trust' security model, and enhanced ICT supply chain security. To secure a competitive edge, the strategy highlights the industrialization of emerging technologies like AI and quantum computing, with plans for a cyber risk management system, quantum-resistant encryption, and stronger collaboration between government, industry, and academia. Industry-government coordination is reinforced through a public-private data-sharing platform and expanded cybersecurity workforce development (Wood, 2024). Globally, South Korea is deepening partnerships, particularly with the U.S., through frameworks like the Strategic Cybersecurity Cooperation Framework, enhancing regional resilience, and aligning cyber defense with the U.S.-ROK Mutual Defense Treaty. This comprehensive approach reflects the evolving cyber threat landscape and the policy priorities of the Yoon Suk Yeol administration (Nitta, 2014).

North Korea is a country facing numerous challenges, including economic poverty, technological underdevelopment, and global isolation. With a significant reliance on trade with China, North Korea's access to international markets is limited. Moreover, the country suffers from a lack of electricity and has limited connectivity, resulting in a poorly networked society. The North Korean government exercises strict control over information flow, tightly regulating both inbound and outbound communication. Despite the challenges and limited perception of North Korea's cyber capabilities, it is important to monitor and assess the country's activities in cyberspace. The evolving nature of cyber threats and the potential for North Korea to enhance its cyber capabilities require continued attention and analysis. In terms of cyber diplomacy North-Korea don't have a transparent approach its diplomatic efforts and international cooperative measures are very limited but North Korea's cyber offensive capabilities present a significant security threat, particularly in the emerging cyber-physical space (CPS) that bridges the gap between the physical and virtual realms. North Korea's cyber strategy primarily revolves around three key objectives: information collection, financial theft, and espionage (North Korea's Cyber Strategy).

The cybersecurity challenges and policies of North and South Korea significantly impact East Asia and the global community. North Korea's aggressive cyber activities, including espionage, financial theft, and attacks on critical infrastructure, destabilize regional security, disrupt global financial systems, and threaten supply chains. These actions push countries like China and Japan to enhance their cybersecurity defenses and drive South Korea's shift to an offensive posture, emphasizing resilience, emerging technologies, and international collaboration with the U.S. and NATO. South Korea's proactive measures strengthen regional and global cybersecurity frameworks while advancing technology standards, but they also heighten geopolitical tensions. These dynamics underscore the urgent need for coordinated international efforts to address evolving cyber threats (Byung-yeul, 2024).

This emphasizes the increasing global menace of cyber aggression and emphasizes the need for long-term solutions that extend beyond national cyber deterrence strategies. Diplomacy, through fostering confidence, establishing international norms, and promoting shared values, offers a more effective and cost-efficient approach to achieving enduring cyber security and stability. By strengthening collaboration between states and ensuring predictability in cyber conduct, it becomes possible to mitigate the risks of misperception, escalation, and conflict (Diplomatic Council, 2022). Policymakers are confronted with the unfamiliarity and unpredictability of this relatively unexplored territory, but they also acknowledge the pressing need for universally accepted rules, protocols, and behaviors that can facilitate harmonious interactions among global actors within cyberspace (Manantan, 2021).

If the cybersecurity dynamics between North and South Korea were to shift, the outcomes would vary depending on the nature of the change. Enhanced regional collaboration among East Asian nations, including China, Japan, and South Korea, could strengthen cybersecurity frameworks, reduce tensions, and improve defenses against cyber threats, potentially isolating North Korea and limiting its cyber operations. Conversely, an escalation in cyber aggression by North Korea or unchecked offensive measures by South Korea could heighten regional tensions, spark arms races in both cyber and kinetic domains, and destabilize the region. Globally, improved cooperation could serve as a model for managing cyber threats, while failure to address these tensions could disrupt international trade, financial systems, and diplomacy. The impact ultimately depends on whether the shift fosters collaboration or exacerbates competition and conflict.

Research Objectives

The objective of this research paper is to identify the emerging cyber challenges prevalent in Korean peninsula and examine their economic and political impacts on leading regional states in the realm of cyber warfare.

- To identify and analyze the emerging cyber security challenges faced by East Asian countries
- To explore the role of these leading states in the domain of cyber warfare and analyze their strategies for addressing and mitigating cyber threats.
- To analyze the advent of cyber diplomacy in the foreign policies of the north and south Korea and their future Implications
- How cyber diplomacy creates regional stability and increases state security by analyzing the potential for collaboration and cooperation among states in countering cyber security threats, with a focus on information sharing, joint initiatives, and diplomatic efforts.

Theoretical Framework

As cyber security is an emerging concept of international relation but there is no specific theory for this domain so this study got its relevance from the traditional theoretical framework as its main focus is on the global security and international cooperation regarding cyber environment.

Realism and its Relevance

Realism revolves around the concept of power and is underpinned by various theories that have distinct justifications and formulations, all based on a relatively coherent set of assumptions regarding the functioning of the world. Realism traces its origins back to the realpolitik ideology prevalent among statesmen, military strategists, and scholars engaged in imperialistic politics during the nineteenth and twentieth centuries. Notable figures such as E.H. Carr, Hans Morgenthau, George Kennan, Herman Kahn, and others contributed to the formalization of realism through their writings, which often had a strong political focus.

The ongoing progression in cyber technology on the Korean Peninsula and their impact on Japan can be better understood by the lens of neo-realism, a key theoretical domain in international relations. Neo-realism, also known as structural realism, emphasizes the importance of power dynamics and the global structure in shaping state behavior. This perspective focuses on how the distribution of power influences state interactions and decision-making. According to neo-realism, states act based on their national interests and security concerns, which often leads to competition and ongoing development in cyber domain leads to the creation of security nexus.

By applying neo-realism, we can gain valuable insights into the strategic challenges of cybersecurity in the region, as well as the potential for regional cooperation and cyber diplomacy. The Korean Peninsula is characterized by intense geopolitical landscape, with states fighting for influence and security. Cybersecurity threat such as state-sponsored cyberattacks, transnational cybercrime, and the protection of critical infrastructure can be analyzed through this theoretical framework. Countries in the region are likely to enhance their cyber capabilities, engage in offensive cyber operations, and develop cyber deterrence strategies to safeguard their interests and assert their influence in cyberspace.

Moreover, neo-realism highlights the significance of power imbalances and the security dilemma in cyber conflicts. In the region, major players like China, Japan, and South Korea may view cyber capabilities crucial for maintaining their power and security. This perception could foster a cyber arms race, further escalating tensions and competition among states in the region.

Neo-Liberalism

Neoliberalism, also known as liberal institutionalism, is a theoretical framework of international relations that focuses on cooperation, institutions, and shared interests between countries. When applied to cyber security, this perspective suggests that countries in the region have the potential to work together to cater common cyber threats.

Neoliberalism highlights the importance of international institutions and agreements and confidence building measures in promoting cybersecurity cooperation. Organizations like ASEAN and the ASEAN Regional Forum (ARF), as well as global agreements like the Budapest Convention on cybercrime and the UNGGE (United Nations Group of Governmental Experts), provide platforms for countries to share information, build trust, and coordinate their efforts against cyber threats.

Another important aspect in neoliberalism is the development of norm, shared expectations about how states should behave in cyberspace. These norms can help ensure responsible state behavior, protect critical infrastructure, and prevent cyber conflicts. When countries follow these norms, they create a more stable and secure cyber environment. Cyber diplomacy, or the use of diplomacy to address cyber issues, is another crucial aspect.

Neoliberalism emphasizes that countries can work together through diplomatic channels, negotiate agreements, and participate in joint initiatives such as cyber exercises and confidence-building measures. These efforts help build trust and strengthen regional and international cybersecurity cooperation (Cavelty, 2019).

Research Methodology

In this research, qualitative content analysis approach is used to provide a complete thorough understanding of the area of interest, drawing on existing theories and generating new insights based on contemporary scenarios. The study acknowledges the significant impact of sudden international and world order changes, which are often overlooked by qualitative content analysis. By incorporating complex structural and agent-based variables, the analysis seeks to codify data in order to obtain accurate information and insights. The utilization of content analysis proves advantageous in managing extensive amounts of theoretical and verbal information gathered from interviews, focus groups, and other media sources. As a result, the research addresses highly open-ended research questions and aims to contribute valuable findings to the field.

The issue in the research questions could be resolved by analyzing the previously conducted research by different think tanks. This research is conducted via an explanatory method to overlook the cyber warfare in the East Asian nation and to what extent these nations have the potential for cyber diplomacy in order to maintain the regional balance and state security.

The research methodology focuses on the secondary data which were published by JSTOR, Taylor and Francis, Google Scholar, media documents, and official documents from the government of targeted countries. The data has also been collected from different electronic media outlets such as Dawn, Al Jazeera, Forbes, BBC, Brookings, Statica, etc. The research official documents and press releases of South Korea, North Korea ,Japan, China, and others have been taken into consideration while performing research on this topic.

Data Collection and Analysis

Data collection is an essential aspect of conducting a research project, encompassing various techniques utilized throughout different stages of the study. It involves systematically gathering and measuring information on specific variables of interest. This systematic approach enables researchers to address their research questions and evaluate the outcomes of their study.

Additionally, this research project incorporates and leverages existing literature and relevant secondary data sources to reinforce its findings. These sources encompass a wide range of materials, including books, journal articles, magazines, academic research, media reports, internet sources, editorial opinions and analyses, as well as television talk shows, among others. Furthermore, to analyze the qualitative data available, grounded theory is employed. Grounded theory follows an iterative analytical process that starts with general observations and progressively develops conceptual categories to explain the topic being studied.

Discussion

Cyber Security as an Emerging Realm of International Relations

Although technology has not been a Focal point in most international relations (IR) theories and textbooks, there surely is a lot of literature on technology that exists which is rather extensive, diverse, and fragmented across many sub-disciplines of IR. This paper finds the interdisciplinary relationship between politics and the emerging cyber technology. (Newlove-Eriksson, 2021)

In the early years of the twenty-first century, novel cyber-related threats emerged, posing risks to individuals, economies, and societies. These threats added a new dimension to the familiar dangers of the previous century (Choucri, 2012). Cyberspace has become an integral part of our daily lives, encompassing the Internet, the vast network of interconnected computers, the supporting institutions, and the experiences it enables.

This paper finds that cyberspace capabilities not only offer opportunities but also expose vulnerabilities, posing potential threats to national security and disrupting the established international order. The interconnected nature of cyberspace, often characterized by non-transparency, has challenged conventional notions of leverage, influence, international relations, power dynamics, national security, borders, and boundaries. This has necessitated a reevaluation of various concepts and their corresponding realities in light of the evolving cyber landscape.

Cybersecurity has now entered the domain of cyber-politics, where states, international organizations, and non-state actors engage in strategic activities aimed at safeguarding their interests and countering cyber threats. It has become a focal point of diplomatic engagements, negotiations, and policy discussions among nations. States strive to enhance their cyber defenses, develop cyber capabilities, and establish norms and agreements to promote responsible state behavior in cyberspace.

Cyber-security: An Emerging Critical Domain within the Realm of IR

Technological progress is constant and pervasive, shaping our lives in profound ways. Every new innovation transforms how we communicate, process information, and engage with the world around us. However, with these changes comes a growing reliance on technology, which brings its own set of challenges. This dependency has made cyber conflict and cyber warfare pressing concerns in international relations. From the telegraph to the telephone, our increasing reliance on technology often leaves us feeling more exposed and vulnerable (Valeriano, 2018).

The traditional perspective on national security primarily revolves around military considerations, such as defending borders and repelling military invasions. However, the evolving nature of the twenty-first century requires a reassessment of these conventional notions of security. In today's world, the security and survival of societies, regardless of their level of development and industrialization, face threats that extend beyond the traditional security framework. Factors such as environmental challenges and internal sources of instability can jeopardize national security. Particularly significant for our discussion is the gradual recognition of the potential impact of cyber threats within the conventional security paradigm. (Choucri, 2011)

As cyberspace has become an integral part of daily life and critical infrastructure, cybersecurity has become a pressing concern for governments, organizations, and individuals. Cyber threats, such as state-sponsored cyber espionage, cybercrime, and disruptive cyberattacks, have the potential to cause significant harm to national security, economies, and societal well-being. The increasing frequency and sophistication of cyber threats have prompted the recognition of cybersecurity as a paramount issue in the realm of international relations.

The reliance of societies worldwide on uninterrupted digital technology has introduced new security concerns. In the last ten years, there has been a noticeable increase in significant cyber incidents, including Stuxnet, WannaCry, NotPetya, and interference in American elections. These incidents have underscored a growing pattern of cyber-attacks that are more specific in their targets, have higher costs, cause greater disruption, and are driven by political and strategic motivations. Consequently, cyber incidents, defined as disruptions to the normal functioning of digital technologies, have gained significant prominence in national and international security policies. State actors are actively seeking effective responses to counter this emerging threat (Cavelty, 2019).

Cybersecurity has now entered the domain of cyber-politics, where states, international organizations, and non-state actors engage in strategic activities aimed at safeguarding their interests and countering cyber threats. It has become a focal point of diplomatic engagements, negotiations, and policy discussions among nations. States strive to enhance their cyber defenses, develop cyber capabilities, and establish norms and agreements to promote responsible state behavior in cyberspace.

Furthermore, cyber-security has introduced new dimensions to traditional notions of power and security in international relations. It has challenged existing concepts of sovereignty, territoriality, and the boundaries between state and non-state actors (Meibauer, 2024). The interconnected nature of cyberspace has blurred the lines between domestic and international security, requiring new frameworks for cooperation and coordination. As the digital landscape continues to evolve and cyber threats persist, the realm of cyber-security will remain a central focus in cyber-politics and international relations. Foreign policymakers and International Relations (IR) scholars are grappling with the unique technological and structural characteristics of cyberspace, which set it apart from traditional security challenges (Kim, 2014).

Cyber Conflict: A Threat To Global Security

Cyber conflict has emerged as a significant threat to global security, reshaping the landscape of international relations and defense strategies. Unlike traditional warfare, cyber conflict operates in a borderless domain, making it challenging to attribute attacks and enforce accountability. State and non-state actors increasingly exploit vulnerabilities in critical infrastructure, financial systems, and governmental networks to achieve strategic objectives, often bypassing traditional security measures. For example, incidents such as the 2007 cyberattacks on Estonia and the Stuxnet worm targeting Iran's nuclear facilities underscore the destructive potential of cyber weapons (Nye Jr, 2017).

Cyber threats, also known as digital threats, are being recognized as significant risks to both national and international stability and security. Cconsequently, an escalating number of states are dedicating resources, whether publicly or discreetly, to develop cyber warfare capabilities that encompass offensive and defensive measures. This global trend signifies states' collective efforts to enhance their presence in cyberspace and deter potential adversaries. The concept of a "cyber arms race" is often invoked to depict this phenomenon, emphasizing the competitive nature of states' endeavors to strengthen their cyber capabilities (Meer, 2015). To moderate these threats, international cooperation, robust cybersecurity frameworks, and operative cyber deterrence strategies are essential to maintain global stability.

The United Nations Security Council (UNSC) is the primary body responsible for upholding international peace and security, making it a crucial and highly sensitive organ within the United Nations system. According to Article 2(4) of the UN Charter, the use of force against other states, whether direct or indirect, is strictly prohibited. This includes recognizing the potential indirect effects of electronic power. Therefore, one of the core purposes of the United Nations is to eliminate any threats to global peace and security and ensure that states and non-state actors adhere to international agreements. In the contemporary world order, the use of force in international relations should be regarded as a last resort. Efforts should instead be focused on diplomatic solutions, peaceful negotiations, and the promotion of dialogue to resolve conflicts and maintain stability (Abdallah, 2019).

Cyber Politics Of Cooperation In The International System

In recent years, there has been a significant rise in cyber-attacks worldwide. The growth of cyberspace has been remarkable, surpassing even the most optimistic predictions of the early Internet pioneers. Today, virtually every corner of the globe enjoys some level of cyber access, demonstrating the rapid expansion of this digital realm (Nazli, 2014).

Cyber aggression poses a growing threat to global security and stability. While national policies aimed at deterring cyber aggression may provide some short-term solutions, their long-term effectiveness is uncertain. Such policies carry the risk of perpetuating a cyber-arms race and escalating tensions between potential adversaries. Diplomacy, though yielding fewer immediate results, holds greater promise in the long run. Building confidence, establishing international norms, and promoting shared values may be challenging, but ultimately more effective and cost-efficient than solely focusing on national cyber deterrence strategies. Over time, fostering cooperation among states to establish trust and universally accepted behavioral norms in cyberspace offers the most viable path toward achieving lasting cyber security and stability. By enhancing interstate collaboration, promoting transparency, and ensuring predictability in cyber behavior, the risks of misperception, escalation, and conflict can be mitigated.

Korean Peninsula its Cyber Security Threats and Cyber Capabilities

The Korean Peninsula, consisting of North Korea and South Korea, is a region known for its unique dynamics and complex geopolitical situation. Along with the traditional political tensions, the region is also a battle field in the realm of cyberspace. Both North Korea and South Korea have established significant cyber capabilities and face ongoing cyber threats from various sources.

When it comes to cyber threats, North Korea has emerged as a prominent actor with a reputation for its cyber operations. South Korea, on the other hand, faces cyber threats from multiple sources, including

North Korea. In addition to the cyber threat from its northern neighbor, South Korea deals with cyber threats from other nation-states, hacktivist groups, and cybercriminal organizations.

In terms of cyber diplomacy, North Korea's approach is less transparent compared to other countries. However, it is believed that the regime uses cyber operations as a means to project power, gather intelligence, and advance its political objectives. On the other hand, South Korea actively engages in cyber diplomacy, collaborating with international partners to address cyber threats, promote norms of responsible behavior in cyberspace, and enhance information sharing and cooperation in cyber defense...

North Korean Cyber Capability, Strategy and Cyber Diplomacy

North Korea is a country facing numerous challenges, including economic poverty, technological underdevelopment, and global isolation. The North Korean government exercises strict control over information flow, tightly regulating both inbound and outbound communication. As a result, most cyber activities within North Korea are conducted under state supervision and guidance. Given these circumstances, North Korea's cyberwarfare capabilities are often perceived as both offensive and defensive, and it is not widely considered a significant cyber threat on the global stage.

North Korea lacks clear evidence of a formalized cyber strategy or doctrine. Insights into its approach can be partially inferred from leadership statements, though much must be deduced from its observed actions. These statements reveal a blend of ambitious rhetoric and more conventional views on using cyber operations in military conflicts. In practice, North Korea’s priorities appear to focus on domestic surveillance, intimidating South Korea, stealing funds to obtain hard currency restricted by financial and trade sanctions, conducting traditional espionage (particularly targeting strategic weapons systems), and occasionally employing cyberattacks to make bold geopolitical statements (CYBER CAPABILITIES AND NATIONAL POWER: A Net Assessment, 2021). The literature on North Korea's cyber capabilities and their implications for international security is still in its early stages and lacks comprehensive analysis. The existing research on this topic remains fragmented, with much room for further exploration and understanding.

Cyber Strategies of North-Korea

North Korea's cyber strategy primarily revolves around three key objectives: information collection, financial theft, and espionage. (North Korea’s Cyber Strategy) Over the last decade, North Korea has significantly increased up its hacking activities, with cybercrime emerging as a primary source of international revenue for the regime (Gracia, 2024).

Over the past years , there has been a growing concern among security experts and U.S. officials regarding the enhanced cyberattack capabilities of North Korea. Analysts specializing in North Korean affairs have identified various motives driving North Korea's cyber operations, including retaliation, coercion, espionage, and financial gain. A report from the UN Sanctions Committee on the DPRK indicates that the country may have carried out up to 58 cyberattacks on cryptocurrency firms between 2017 and 2023, making an estimated $3 billion. These cyber operations are believed to account for nearly half of North Korea’s foreign currency earnings and potentially fund up to 40% of its weapons of mass destruction programs (Gracia, 2024). The notable cyber incident involving the hacking of Sony Pictures Entertainment in 2014 was publicly attributed to the North Korean government by the Federal Bureau of Investigation (FBI) (Chanlett, 2017).

Furthermore, since 2009, North Korea has been involved in a series of cyberattacks targeting South Korean institutions and media outlets, showcasing their disruptive goals and espionage activities. Recent trends suggest that North Korea may increasingly prioritize financial gain through cyber operations. An example of this is the February 2016 cyberattacks on banks in Bangladesh and Southeast Asia, which resulted in the theft of approximately $81 million and included attacks on South Korean banks. These cyber activities can be attributed to North Korea's relatively limited conventional military capabilities and their isolation in the global community. Understanding North Korea's cyber landscape is essential for maintaining a comprehensive perspective on global cybersecurity and addressing potential risks that may arise from the country's actions in the digital realm.

North Korea’s Cyber Diplomatic Efforts

In terms of cyber diplomacy North-Korea don’t have a transparent approach its diplomatic efforts and international cooperative measures are very limited but North Korea's cyber offensive capabilities present a significant security threat, particularly in the emerging cyber-physical space (CPS) that bridges the gap between the physical and virtual realms. North Korea, as a UN member, participates in organizations like the International Telecommunication Union (ITU) and forums such as the World Summit on the Information Society. However, it has shown little involvement in shaping cyber norms, policies, or technical standards and has not demonstrated leadership in these areas. Diplomatic efforts by North Korea on such topics are rare. (CYBER CAPABILITIES AND NATIONAL POWER: A Net Assessment, 2021)

In the UN General Assembly, it frequently aligns its stance with Russia and China on cyberspace-related resolutions. For example, in 2018, North Korea joined 118 other nations in supporting a resolution initiated by Russia and China to establish the UN Open-Ended Working Group on international security issues related to ICT developments, opposing 46 Western-aligned countries. In 2024, North Korea marked a significant diplomatic milestone by hosting Russian President Vladimir Putin in Pyongyang. The visit resulted in a new treaty on comprehensive strategic partnership, replacing earlier agreements from 1961 and 2000. Key provisions of the treaty emphasize collaboration in science, technology, information security, and countering disinformation, laying the groundwork for closer cooperation in cyberspace. Shared adversaries and mutual goals are driving both nations to enhance their military cyber capabilities, with North Korea focusing on integrating cyber warfare into command operations. Kim Jong Un aims to modernize the military by establishing an independent AI and electronic warfare command to advance electronic weaponry and operational command using AI technology.

South Korea’s Cyber Security Strategy And Diplomatic Efforts

Cyber Security Strategy and Diplomatic Efforts

As South Korea continues to digitalize its economic, political, and social systems, the country has become increasingly susceptible to cyber-attacks from rival states, rogue actors, or criminal organizations. The Asia-Pacific region, in which South Korea is situated, is characterized by complex geopolitical dynamics, including the presence of technologically advanced nations like China, the DPRK, and Russia. These factors focuses the development of cyber strategies by South Korea to safeguard its national security and protect its cyberspace environment.

The competences of the National Security Office (NSO) have been strengthened. Specialized cybersecurity entities have been set up in every ministry and local government to address the specific cybersecurity needs within their respective domains. After unveiling the National Cybersecurity Strategy in February 2024, South Korea took several key steps to strengthen its cybersecurity framework. These included creating a national task force to enhance coordination between government agencies, bolstering the security of critical infrastructure such as financial systems and energy networks, and increasing funding for research into advanced cybersecurity technologies (Wood, 2024).

South Korea's cyber policy is based on two important strategic documents. The first one is the National Cyber Security Master Plan, introduced in 2011, which outlines the country’s long-term approach to cybersecurity. The second includes a series of Comprehensive Countermeasures, developed in 2009, 2013, and 2015, primarily in response to previous DDoS attacks. These documents provide a framework for strengthening South Korea's cyber defenses and protecting its digital infrastructure.

The 2011 National Cyber Security Master Plan was created by the Korean Communications Commission in response to major cyber-attacks, including a DDoS attack and a breach at NH Bank. The plan aimed to clearly define the roles of different government agencies, especially the National Intelligence Service (NIS), in managing cybersecurity. It also strengthened the powers of the NIS, the Ministry of Defense, and the Ministry of Home Affairs, focusing on improving national defense against cyber threats (Ebert & Groenendaal, 2020).

South Korea has initiated Comprehensive Countermeasures to strengthen its cybersecurity environment. In 2009, after a DDoS attack generated by North Korea, the government introduced the National Cyber Crisis Comprehensive Countermeasures, establishing a DDoS Cyber Shelter. In 2013, following the 3.20 and 6.2 cyberattacks, it launched the National Comprehensive Cyber Security Countermeasures to enhance the cybersecurity workforce, governance, and infrastructure protection. In 2015, after attacks on Korea Hydro and Nuclear Power, the National Cyber Security Posture and Capability Strengthening Plan was introduced, focusing on specialized cybersecurity teams, research investment, and strengthening the National Security Office (NSO). These efforts continue to evolve in response to emerging threats in cyberspace.

Cyber Diplomatic Efforts and International Cooperation

South Korean cyber diplomacy refers to the efforts and strategies employed by South Korea to address cybersecurity challenges and promote international cooperation in cyberspace. South Korean diplomats, along with governmental and non-governmental experts, have actively participated in global multilateral discussions concerning the application of international law in cyberspace, confidence-building measures (CBMs), and capacity building. The United Nations has served as a primary platform for the debate on the applicability of international law in cyberspace. In September 2019, South Korea joined a group of 27 states that convened prior to the first substantive session of the Open-Ended Working Group (OEWG) in New York. The group's joint statement emphasizes the importance of advancing responsible state behavior in cyberspace, committing to voluntary norms, practical confidence-building measures, and targeted capacity building to support the implementation of a global framework for responsible state behavior in cyberspace. (National Cybersecurity Strategy, 2019)

In 2015, the South Korean government established the Global Cybersecurity Center for Development (GCCD) under the Korea Internet & Security Agency (KISA). The main goal of the Global Cybersecurity Capacity Centre (GCCC) is to enhance cybersecurity knowledge and facilitate experience-sharing initiatives for policymakers and experts in the public sector of developing nations. In 2016, KISA launched the Cybersecurity Alliance for Mutual Progress (CAMP), a worldwide network for cybersecurity cooperation. CAMP enables members to share information and coordinate joint efforts in response to cyber threats. As of 2020, the network included over 59 governmental and non-governmental institutions from 45 countries, with a strong presence in developing regions like Asia, South America, and sub-Saharan Africa.

KISA plays a vital role in hosting the secretariat of CAMP, overseeing its organization, and conducting annual meetings. Furthermore, the South Korean government has provided funding for the project "Combatting Cybercrime: Tools and Capacity Building for Emerging Economies," which is implemented by the World Bank. This initiative aims to enhance the capabilities of developing countries in responding to cybercrime. In terms of diplomatic efforts, South Korea actively participates in Track 1.5 or Track 2.0 diplomacy to promote cybersecurity capacity building. This includes regular meetings such as the Seoul Defense Dialogue Cyber Working Group since 2014, the International Symposium on Cybercrime Response since 2000, the aforementioned GCPR since 2014, and the Jeju Forum for Peace and Security since 2001. These meetings serve as platforms for raising awareness and discussing strategies for enhancing cybersecurity capacity (Ebert & Groenendaal, 2020).

In 2014, Seoul played a significant role in launching a trilateral cybersecurity dialogue involving China, Japan, and South Korea. This initiative came almost six years after the three countries had agreed to enhance cybersecurity cooperation in the Action Plan for Promoting Trilateral Cooperation, which was released during a trilateral summit meeting in December 2008. Concurrently, as global multilateral negotiations faced challenges and concerns about the cyber capabilities of North Korea (DPRK) grew, regional organizations in East Asia witnessed an increase in cybersecurity cooperation. South Korea has actively engaged in bilateral and trilateral cyber diplomacy efforts, complementing its initiatives. Additionally, the country has been particularly involved in discussions within the ASEAN Regional Forum (ARF), which includes a dedicated working group on cybersecurity. These regional cooperation efforts serve as alternatives and supplements to global multilateral negotiations, addressing the specific regional concerns and challenges related to cybersecurity in East Asia (Handler, 2022)

In late 2024 South Korea inaugurate High-Level Cyber Dialogue with NATO laid the ground for deeper cooperation. This included sharing threat intelligence and collaborating on joint cyber defense strategies to report and cater emerging cyber threats in the Indo-Pacific and Euro-Atlantic regions (South Korea strengthens NATO cyber ties as new threats emerge globally, 2024). Further developments regarding cyber security in South Korea includes its trilateral cooperation with USA and Japan on January 2025 regarding collaboration in areas such as cybersecurity for nuclear facilities, ensuring that both nations can jointly address potential cyber threats to critical infrastructure.

These developments in early 2025 highlights the continuing efforts between the United States and South Korea to improve their cybersecurity synergies, particularly in countering threats from North Korea and securing the critical infrastructure (Joint Press Statement on the Fourth Nuclear Consultative Group Meeting, 2025).

Conclusion

To conclude, this research underscores the importance of gaining a comprehensive understanding of the increasing cyber security's scope in the realm of international relations and efforts of the states to enhance collaborative measures in order to protect the critical infrastructure, cybersecurity landscape in East Asia and utilizing cyber diplomacy to tackle the challenges. By thoroughly examining the specific threats, vulnerabilities, and impacts in Korean region, as well as exploring opportunities for collaboration and information sharing, this study seeks to provide valuable insights for policymakers and stakeholders in the region. The document focusses mostly on Korea's cybersecurity concerns and the possibilities for cyber diplomacy to address them. Its goals include gaining a thorough understanding of the cybersecurity landscape, identifying emerging cyber threats, analyzing the strategies used by leading states to counter these threats, investigating the role of cyber diplomacy in foreign policies, and examining the potential for international collaboration and cooperation. The analysis highlights the growing global threat of cyber warfare and the need for long-term solutions that go beyond national cyber deterrent policies. Diplomacy, by developing confidence, establishing international standards, and promoting shared values, is a more effective and cost-effective method to ensuring long-term cybersecurity and stability. By enhancing coordination among states and guaranteeing predictability in cyber behavior. It becomes possible to mitigate the risks of misperception, escalation, and conflict.

South Korea's highly digitized and networked society creates substantial cyber security issues. The country has taken a proactive approach to strengthening cyber security capabilities, recognizing the value of cyber diplomacy and international cooperation in resolving these concerns. South Korea has made significant strides in improving its cyber security capabilities, investing in R&D, establishing cyber security organizations, and enacting comprehensive legal frameworks. The government has also prioritized cyber security education and awareness programs to strengthen the resilience of its population and organizations to cyber threats.

North Korea's cyber capabilities provide substantial hazards to espionage, disruption, and political purposes. However, due to the country's diplomatic isolation and limited opportunities for direct contact, international collaboration on cyber diplomacy with North Korea remains challenging. Efforts to combat North Korean cyber threats are primarily driven by bilateral and multilateral exchanges with other countries in the region, as well as regional and international venues. Given the complex security dynamics on the Korean Peninsula, international collaboration on cyber diplomacy remains difficult but necessary for tackling common cyber threats and fostering stability.

References

Abdallah, J. A., Bin Awang, M. B., & Ahmad, A. A. (2019). Cyberterrorism as a threat to international peace and security: A critical discourse. *Scholars International Journal of Law, Crime and Justice*, *02*(10), 314–317. https://doi.org/10.36348/sijlcj.2019.v02i10.004

Bajak, F., & Associated Press. (2023, June 15). *Chinese hackers breached hundreds of public, private networks, security firm says*. PBS News. https://www.pbs.org/newshour/world/chinese-hackers-breached-hundreds-of-public-private-networks-security-firm-says

Byung-yeul, B. (2024, February 1). *Korea, US, Japan join forces to enhance cybersecurity, network, digital capabilities*. The Korea Times. https://www.koreatimes.co.kr/www/tech/2025/01/129_368071.html

Capabilities, C. (2021). National Power: A Net Assessment. *International Institute for Strategic Studies*, *28.*

Cavelty, M. D., & Wenger, A. (2020). Cyber security meets security politics: Complex technology, fragmented politics, and networked science. *Contemporary Security Policy*, *41*(1), 5–32. https://doi.org/10.1080/13523260.2019.1678855

Chanlett-Avery, E., Rollins, J. W., Rosen, L. W., & Theohary, C. A. (2017). *North Korean cyber capabilities: In brief* (pp. 1-12). Washington, DC, USA: Congressional Research Service.

Chansoria, M. (2012). DEFYING BORDERS IN FUTURE CONFLICT IN EAST ASIA: CHINESE CAPABILITIES IN THE REALM OF INFORMATION WARFARE AND CYBER SPACE. *Journal of East Asian Affairs,* 106-127. Retrieved from JSTOR: https://www.jstor.org/stable/23257910

China's Peaceful Development. (2012). *EMBASSY OF THE PEOPLE REPUBLIC OF CHINA*: http://zw.china-embassy.gov.cn/eng/zgjj/201209/t20120928_6408733.htm

Choucri, N. (2011). *Cyberpolitics in International Relations.* MIT press.

Choucri, N., & Goldsmith, D. (2012). Lost in cyberspace: Harnessing the Internet, international relations, and global security. *The Bulletin of the Atomic Scientists*, *68*(2), 70–77. https://doi.org/10.1177/0096340212438696

Ebert, H. (2020). Cyber Resilience and Diplomacy in the Republic of Korea. *EU Cyber Direct—Digital Dialogue Report, August*, *18*.

Foulon, M., & Meibauer, G. (2024). How cyberspace affects international relations: The promise of structural modifiers. *Contemporary Security Policy*, *45*(3), 426–458. https://doi.org/10.1080/13523260.2024.2365062

Gracia, S. (2024, august). *Asia Dispatches.* wilsoncenter.org: https://www.wilsoncenter.org/blog-post/facing-north-korean-cyber-threat-united-states-south-korea-coordination-cyberspace

Grossman, D. (2020, Jun 11). *What China Wants in South Asia*. OBSERVER RESERRCH FOUNDATION: https://www.orfonline.org/research/what-china-wants-in-south-asia-67665/

Handler, S. (2022). *The US-Japan-South Korea trilateral cybersecurity relationship.* Atlantic council: https://www.atlanticcouncil.org/content-series/the-5x5/the-5x5-the-us-japan-south-korea-trilateral-cybersecurity-relationship/

I. Duić, V. C. (2020). *International Cyber Security Challenges* .

Inkster, N. (2016). *china cyber power*. In N. Inkster.

Jobst, N. (2023). *Cyber security in South Korea - statistics & facts. statista.*

Joint Press Statement on the Fourth Nuclear Consultative Group Meeting. (2025, january 10). US department of defence: https://www.defense.gov/News/Releases/Release/Article/4026575/joint-press-statement-on-the-fourth-nuclear-consultative-group-meeting

Kim, S. (2014). Cyber security and middle power diplomacy. *The Korean Journal of International Studies*, *12*(2), 323. https://doi.org/10.14731/kjis.2014.12.12.2.323

Kshetri, N. (2013). Cyber-victimization and cybersecurity in China. *Communications of the ACM*, *56*(4), 35–37. https://doi.org/10.1145/2436256.2436267

Manantan, M. B. (2021). *defining cyber diplomacy. Retrieved from australian institute of internatioanl affair*: https://www.internationalaffairs.org.au/australianoutlook/defining-cyber-diplomacy/

Meer, S. V. (2015). *Enhancing International Cyber Security. security and human rights* (Vol. 26). brill nijhof.

Nazli Choucria, S. M. (2014). *Institutions for Cyber Security: International Responses and Global Imperatives.* Taylor and Fransis.

Newlove-Eriksson, J. E. (20 Apr 2021). Theorizing technology and international relations: Prevailing perspectives and new horizons. In *Technology and international relations* (pp. 3-22). Edward Elgar Publishing.

Nitta, Y. (2014). National cyber security strategy: are we making progress? Japan's efforts and challenges. *Geo. J. Int'l Aff.*, *15*, 89.

Nye Jr, J. S. (2016). Deterrence and dissuasion in cyberspace. *International security*, *41*(3), 44-71.

Office of the President. (n.d.). *National cybersecurity basic plan executive summary*. Office of the President. Retrieved February 6, 2025, from https://eng.president.go.kr/briefing/TE0xsLB6

Pawlak, P. (2015). Cyber diplomacy: Confidence-building measures. In *Cyber diplomacy: Confidence-building measures*.

People's republic of China cyber threat. (n.d.). Cybersecurity and Infrastructure Security Agency CISA. Retrieved February 6, 2025, from https://www.cisa.gov/topics/cyber-threats-and-advisories/advanced-persistent-threats/china

Renard, A. B. (2017). *Cyber-diplomacy: the making of an international society in the digital age*. Taylor and Fransis.

Sacks, S. (n.d.). *China's Emerging Cyber Governance System.* CSIS.org: https://www.csis.org/programs/strategic-technologies-program/archives/china-cyber-outlook/chinas-emerging-cyber

Segal, A. (2017). Chinese cyber diplomacy in a new era of uncertainty. *Hoover Institution, Aegis Paper Series*, *1703*, 1-23.

Segal, A., Akimenko, V., Giles, K., Pinkston, D. A., Lewis, J. A., Bartlett, B., & Noor. (2020). The Future of Cybersecurity across the Asia-Pacific. *Asia Policy*, *15*, 57–114.

South Korea strengthens NATO cyber ties as new threats emerge globally. (2024 , november). korea pro: https://koreapro.org/2024/11/south-korea-strengthens-nato-cyber-ties-as-new-threats-emerge-globally

The Brooking Institution. (2018). Asia Transnational Threats Forum: Cybersecurity in Asia: https://www.brookings.edu/events/asia-transnational-threats-forum-cybersecurity-in-asia/

Top 15 Cybersecurity Breaches in South Korea. (n.d.). Cyberlands.Io. Retrieved February 6, 2025, from https://www.cyberlands.io/topsecuritybreachessouthkorea

Ukhanova, E. (2022). Cybersecurity and cyber defence strategies of Japan. *SHS Web of Conferences*, *134*, 00159. https://doi.org/10.1051/shsconf/202213400159

Valeriano, B., & Maness, R. C. (2018). International Relations theory and cyber security: Threats, conflicts, and ethics in an emergent domain. In C. Brown & R. Eckersley (Eds.), *The Oxford Handbook of International Political Theory* (pp. 258–272). Oxford University Press.

Valeriano, R. C. (2015). *The Impact of cyber conflict on international relations*. SAGE.

Vosse, W. M. (2019). Japan's Cyber Diplomacy. *EU Cyber Direct: Research in Focus*.

Wood, N. (2024). South Korea's 2024 Cyber Strategy: A Primer. CSIS. https://www.csis.org/blogs/strategic-technologies-blog/south-koreas-2024-cyber-strategy-primer

Zhao, F., Shi, Y., & Yao, K. (2021). Challenges and Countermeasures of China's Cyberspace Governance in the New Era. In *SHS Web of Conferences* (Vol. 96, p. 01005). EDP Sciences.

Zhukov, A. V., & MGIMO University. (2020). Cyberspace as a sphere of international relations and national security. *Scientific Review. Series 2. Human Sciences*, *3–4*, 60–68. https://doi.org/10.26653/2076-4685-2020-3-4-06