The Future of Cyberwarfare in Northeast Asia

Minwoo Yun, Ph.D.[1]
Gachon University

Abstract

A new phase of global geostrategic hegemonic conflict is intensifying. The theater of this emerging hegemonic struggle encompasses not only conventional physical realms-land, sea, air, and space-but also virtual realms of cyber and human cognition. Northeast Asia has emerged as the epicenter of this new round of global conflict. The victor in the geostrategic struggle within Northeast Asia is poised to exert a greater influence over the entire Eurasian theater of the New Cold War. In the Northeast Asian theater, the US, Japan, and South Korea stand against China, North Korea, and Russia. Cyberwarfare holds a pivotal role in this confrontation, as all parties possess advanced information technology, scientific capabilities, and cyberwarfare prowess. Consequently, in the context of Northeast Asia, cyberwarfare could be a decisive factor in determining the outcome of the geostrategic conflict, possibly more so than in any other region. This article explores the future of cyberwarfare in Northeast Asia. To accomplish this, it will delve into the geostrategic significance of Northeast Asia in the broader global hegemonic conflict, underscore the importance of cyberwarfare in future warfare, and ultimately examine the current state and prospective evolution of cyberwarfare in the Northeast Asian context.

Keywords: Northeast Asia, North Korean cyberwarfare, cyber cognitive operations, cyber espionage, influence operations, Unit 121, RuNet 2020, Golden Shield Project

Intersection of Cyberwarfare and Geopolitics of Northeast Asia

An intensifying global geostrategic hegemonic conflict is unfolding. The US and the West are facing off against China and Russia in a direct confrontation. This clash spans the entire Eurasian continent tracing the

[1] Ph.D. in International Politics and Criminal Justice, Professor, Gachon University, A Security Consultant for the Office of National Security, Researcher, Future Warfare Research Center, Institute of International Studies, Seoul National University, South Korea minwooy@hotmail.com

geopolitical fault line that divides the inner-land from the periphery. The theater of this new struggle for dominance encompasses not only the traditional physical realms of land, sea, air, and space but also the virtual domains of cyber and human cognition.[1]

Cyberwarfare has grown increasingly significant as a battleground in both present-day conflicts and presumably those of the future. It encompasses not only cyber technological warfare but also cyber cognitive warfare. Also, it has become an integrated domain that merges cyberwarfare, electronic warfare, and information warfare.[2]

Moreover, cyberwarfare blurs the traditional boundaries between war and peace. It operates within a gray zone that defies easy categorization as either war or peace. The same action could be deemed a crime, an act of terrorism, espionage, an influence operation, or even an act of war. Determining the nature of these actions depends on the actors involved, their motivations, targets, and the surrounding circumstances. Consequently, this ambiguity renders security concerns less distinct and the situation more unstable.[3]

The strategic significance of the cyber domain is also crucial in shaping the outcome of the hegemonic struggle in Northeast Asia, as well as globally. Northeast Asia has emerged as a pivotal frontline in the global geopolitical clash between the US-led liberal democratic bloc and the China-led authoritarian coalition. This region accommodates four nuclear powers and boasts five major military forces.[4] Importantly, all these actors possess world-class cyberattack capabilities and advanced IT (Information Technology) expertise. Any alteration in the status-quo within this region could significantly impact the broader global power struggle.

This paper delves into two crucial dimensions within the realm of global security. The convergence of cybersecurity and the geopolitical significance of the Northeast Asian region raises a weighty apprehension. The paper encompasses the evolution of modern cyberwarfare, the geopolitical importance of the Korean Peninsula and Northeast Asia, the ongoing landscape of cyber aggressions targeting South Korea, and prospects on the evolution of cyberwarfare in Northeast Asia.

Advancement of Cyberwarfare

Formerly cyberwarfare predominantly referred to hostile cyber technological acts through malicious codes. However, cyberwarfare increasingly encompasses not just conventional cyber technological actions but also cyber cognitive operations. Cyber-technology warfare

pertains to technical strategies for attacking and safeguarding hardware and software within computer networks.[5] Cognitive warfare aims to alter or influence people's perceptions. Cognitive warfare extends beyond cyberspace to offline realms such as traditional broadcasting, cable or satellite broadcasting, newspapers, journals, books, lectures, film/documentaries, music/art/sport events, and other social gatherings. Nevertheless, in today's IT environment, cyber space becomes a critical theater for cognitive warfare.[6] Cyberwarfare knows no domestic or international boundaries, and it often intertwines and overlaps with both times of war and peace. It merges military and non-military domains, as well as governmental and civilian sectors.[7]

Cyberwarfare also merges with electronic warfare. Electronic warfare involves offensive and defensive actions aimed at causing physical harm through the disruption, interference, and manipulation of intangible waves traversing the electromagnetic spectrum. Electronic warfare is more concerned with traditional communication mediums like radio and broadcasting, as well as newer technologies like Wi-Fi. In contemporary times, the convergence of cyber warfare and electronic warfare has grown stronger due to the interconnectivity of various wireless combat systems and human command centers.[8] As a result, electronic warfare has made it possible to influence cognitive warfare in the cyber realm. For instance, through electronic intrusion and theft, it is now feasible to install malicious software on devices like smartphones, tablets, and PCs connected via Wi-Fi. These compromised devices can then serve as launching points for conducting cognitive warfare, such as disseminating fake news, disinformation, and manipulation.[9]

With the expansion of its scope, cyberwarfare is waged by combining the virtual and the real worlds. Violence in virtual space and the physical spaces such as land, sea, air, and space are interconnected in both directions. One aspect involves cyber aggression in virtual space resulting in killings, destruction, and disruptions in the physical world. For instance, the use of offensive cyber weapons like Stuxnet can directly cause destruction, casualties, and harm to targets, especially critical infrastructures, in the physical space. Cyberspace supports actors of real-world violence by providing functions such as cyber espionage, training and recruitment of personnel, psychological disruption and indoctrination, provision of resources and weapons via the internet, command and control, influence operations, propaganda, and financial activities.[10]

Aggression in the physical space can also result in destruction, disruption, and casualties in cyberspace as well. Cyberspace relies on various physical platforms and critical infrastructures. Consequently, damaging, intercepting, or destroying such physical targets can have adverse effects on the stable functioning of cyberspace. For example, physical attacks against submarine cables and space satellites can effectively disrupt the stability of enemy operations. High-energy radio frequency guns or EMP bombs emit powerful electronic waves to induce abnormal behavior in computer circuits, leading to system malfunctions or shutdowns in computer networks. The development of drone technology allows for access to core computer networks using miniaturized drones, enabling direct infiltration of malicious viruses, information extraction, hacking, or system control from external sources.[11]

Cyberwarfare becomes increasingly intertwined with warfare in other domains. Future warfare takes place in a multi-domain environment encompassing not only the traditional domains but also cyber, space, and the human cognitive domain. This shift in paradigm is propelled by changes in how the results of war are determined. The essential features of future warfare involve the diversification and integration of war domains, erasing the lines between various domains, and ushering in an era of hyper-connected warfare that fuses all domains.[12] This trajectory of future warfare signifies a fundamental alteration in the paradigm of war generations.[13]

In response to this evolving trend of future warfare, the United States has introduced concepts such as Multi-Domain Operations (MDO). Russia's Gerasimov propositions also reflect their understanding of this trajectory of future warfare. South Korea's Defense Science Research Institute (DSRI) has similarly adapted to this trend, envisioning the concept of the "mosaic battlefield" where individual platforms are rapidly and flexibly integrated through a dispersed-adaptive kill web in multi-domain, multi-dimensional operations. This approach maximizes survivability through decentralization and enables lethal strikes against adversaries. This concept is regarded as the cornerstone of future defense and security, with South Korea aiming to establish its own mosaic battlefield based on advanced defense science and technology.[14]

In the context of multi-domain integrated warfare, the cyber domain holds significant strategic importance. In the past, the seas served as massive highways with strategic importance, and those who controlled maritime space held global dominance. This was because controlling sea

communication routes allowed for the freedom of access, movement, and communication essential for successful military operations. This capability could be defined as strategic flexibility. Similarly, the vast steppes connecting the northern Korean Peninsula to the Eurasian continent and the Hungarian plains served as enormous highways for cavalry armies in the past. These routes, much like the seas, provided strategic flexibility. Today and in the future, the cyber domain is expected to provide the same strategic flexibility as the seas and steppes did in the past. As previously discussed, the cyber domain acts as a massive highway connecting various other domains like land, sea, air, space, and human cognitive space. Thus, the controller of the cyber domain can gain a significant advantage in terms of freedom of access, movement, and communication necessary for military victory.[15]

Lastly, cyberwarfare tends to blur the boundary between war and peace. It establishes a state of constant peaceful war (or warlike peace) as the norm. Crime, terrorism, espionage, influence operations, and warfare become ambiguously intertwined. Combatants, criminals, terrorists, hackers, spies, mercenaries, and civilians are all interconnected. Peace and war are no longer strictly dichotomous concepts; instead, they need to be understood as part of a continuous spectrum. The current situation lies somewhere along the spectrum between absolute peace and absolute war, and this position is always shifting.[16]

From this perspective, Russia's conceptual distinction is quite insightful. Russia categorizes the peace-war spectrum into four subtypes: ① Peaceful coexistence, ② Conflict in understanding or natural competition, ③ Armed conflict, and ④ War. According to Russia's theoretical framework, war is not limited to a specific period but is a progressive process where tensions and conflicts escalate over time. The stages of ② and ③ involve activities such as espionage, covert operations, criminal investigations, economic and diplomatic pressures, threats through military maneuvers, historical-cultural influence, cognitive warfare, election interference, political manipulation, assassination and sabotage, hacking and technology theft, terrorism and organized crime, artificially induced disasters, proxy wars, and insurgency warfare, which shape the landscape of grey wars, secret wars, or spy wars. These stages lead up to the onset of conventional warfare just before the stage of ④. The ④ stage represents the beginning of conventional warfare, including all-out military confrontations that lead to nuclear warfare. Cyberwarfare can easily trigger conventional warfare in other domains or function as

preliminary battle associated with an impending full-scale military invasion.[17]

Geopolitics of Northeast Asia and the Korean Peninsula

The Korean Peninsula is a dual-purpose instrument of offense and defense. This distinct geopolitical nature of the Korean Peninsula often shapes the overall geopolitical landscape of Northeast Asia, regardless of its unification. Decades after the Cold War, the strategic importance of the Korean Peninsula remains unchanged. For the U.S. and the West, it continues to be seen as a launchpad for potential operations against China and a frontline defense for implementing a blockade in the East Asia-West Pacific region. Conversely, for China, the Peninsula still serves as a protective shield against vulnerabilities from the United States and its allies, as well as a strategic base for possible retaliatory measures.[18]

The strategic alliance formed by China, Russia, and North Korea in this region emerges from a combination of North Korea's survival imperatives, Russia's constrained strategic capacities, and China's calculated pursuit of regional hegemony. North Korea is compelled by economic sanctions and diplomatic constraints imposed by the US and its allies due to its pursuit of nuclear armament. To ensure its regime survival, North Korea seeks support from China and Russia. Meanwhile, Russia faces pressure from the US-Western powers in areas such as the Sea of Okhotsk, the Arctic, and the western and southern regions of the Eurasian Plate. Given its diminishing military and economic capabilities, Russia cannot independently pursue strategic interests that compete with the US-West and China in the Northeast Asian region. As a response, Russia aims to forge a strategic alliance with China by yielding regional hegemony to China and seeking Chinese assistance in other parts of the Eurasian Plate. China, for its part, requires regional allies to counterbalance the US-led alliance, which seeks to isolate China in the context of regional hegemonic rivalry.[19]

North Korea, Russia, and China share a common interest in diminishing US influence within the region. The presence of the US forces, particularly in South Korea, poses an existential threat to North Korea, a potential destabilizing factor for Russia's Far East territories, and a challenge to China's aspirations for reunification with Taiwan and the establishment of a Chinese hegemonic sphere in the area. Motivated by these shared interests, all three countries set aside potential rivalries and reservations among themselves. For example, Russia is engaging in

negotiations with China, acknowledging China's regional hegemony while receiving security assurances for its Far East and Siberian territories from China, along with recognition of Russia's regional power status.[20]

Contrary to prevailing assumptions, the North Korean nuclear matter might not be a significant security apprehension for China and Russia. Russia's primary focus lies in securing its Far East region. Consequently, as long as North Korea, its neighboring nation, maintains a non-hostile stance towards Russia, the presence of nuclear weapons in North Korea does not pose a security risk for Russia. Similarly, for China, the key concerns revolve around North Korea's positioning between the US and China, as well as the durability of the North Korean regime that acts as a buffer against the US. Whether North Korea possesses nuclear weapons or not could be of secondary importance to these core considerations.[21]

China, North Korea, and Russia perceive South Korea as a vulnerable link within the South Korea-U.S.-Japan alliance structure. Consequently, their aim is to diminish the influence of the U.S. in the region by dislodging South Korea from this alliance. However, employing conventional military methods to isolate South Korea from the U.S.-led coalition is deemed ineffective due to South Korea's substantial military and economic strength, as well as the enduring nature of the U.S.-South Korea alliance. Thus, they opt for unconventional tactics, with cyberwarfare being a pivotal element in their strategy. During peacetime, China and North Korea prioritize influence operations, cyber espionage, and cyber theft targeting South Korea. In times of conflict, cyberwarfare becomes an asymmetric tool of choice for China and North Korea against the advanced and intricate military capabilities of the U.S. and South Korea.[22]

The waters surrounding the Korean Peninsula hold immense significance within China's naval strategy, driving its desire to bring South Korea into its sphere of influence. This importance is closely tied to China's goal of securing its capability for mutually assured destruction against the U.S. On the one hand, China aims to establish dominance over the West Sea, effectively turning it into its own inland sea. The presence of U.S. and its allied naval forces in the West Sea place China's core regions (including Beijing, Shanghai, Qingdao, and the eastern coastal areas like Bohai Bay) within range of potential attacks from the U.S.-led alliance. On the other hand, China holds critical strategic interests in the East Sea for two primary reasons. Firstly, the East Sea is crucial for China's utilization of the Northern Sea Route. Secondly, to facilitate its operations involving strategic nuclear submarines aimed at countering the

U.S., China must navigate its vessels through the East Sea. Hence, China has demonstrated prolonged interest in establishing a port along the Eastern Shore of the Korean Peninsula. If South Korea were to align with China, the US could potentially encounter China's strategic nuclear submarines in areas like the Sea of Okhotsk, North Pacific, and the Arctic Ocean. This would provide China with a significant strategic upper hand in terms of its mutually assured destruction capabilities vis-a-vis the U.S.[23]

The regional geopolitical rivalry between the Chinese-led and the U.S.-led factions extends beyond physical territories—it is also manifest in the realm of cyberspace. This cyber Cold War on a regional level is intricately intertwined with the broader global power struggle between the U.S.-West and China-Russia across both physical and digital domains. In the cyber realm, we witness a clash of ideologies and priorities between the U.S.-West and China-Russia. The US-West champions ideals such as freedom of expression, limited government control, transparency, the free flow of information, and a globally unified internet unrestricted by borders. In stark contrast, China-Russia advocates for state control, national sovereignty, security, recognition of cultural relativism, and an internet divided by the principle of sovereignty. This expansion of the new cold war into cyberspace emphasizes the critical importance of controlling the cyber domain within the overarching power struggle.[24]

The arena of cyber international rulemaking stands as a heated battleground between the two opposing camps. The U.S.-West champions an open and transparent global internet space that curtails state control over individuals. In contrast, China-Russia advocates for the principle of "digital sovereignty," which entails segmenting cyberspace according to national borders and imposing state authority over individuals within these segmented realms. Their aim involves establishing national intranets that connect to the global internet via controlled gateways. Initiatives such as Russia's "RuNet 2020" and China's "Golden Shield Project (Great Firewall)" reflect strategic efforts to reshape their national internets into intranets and to encompass neighboring nations within their envisioned spheres of influence.[25]

Consequently, the global cyberspace is increasingly diverging into distinct territories aligned with two opposing camps. This divided global cyber geopolitics also extends its influence into the realm of Northeast Asia. As expected, China, North Korea, and Russia are gravitating towards isolating their internet from external influences. Notably, North Korea represents the most extreme case, with its internet entirely sealed off from

the outside world and strictly controlled by the state. China is progressively following suit, with trends exemplified by the 2023 Chinese Anti-Espionage Law and the 2017 Chinese Cybersecurity Law. In contrast, the U.S., South Korea, and Japan align with the liberal democratic camp, advocating for an open and transparent global internet framework. Just as in the physical domain, cyberspace in the region is increasingly cleaved into the spheres of these two opposing camps.[26]

In essence, the power struggle within Northeast Asia has grown increasingly intricate and multifaceted. This conflict intertwines traditional geopolitical contests involving politics, economy, military, and sociocultural dimensions with the rising prominence of cyberwarfare as a critical emerging security concern. As a result, geopolitics has undergone a transformation into what can be termed "multidimensional geopolitics." In contrast to the Cold War era of the past, this contemporary multidimensional conflict is defined by the convergence of numerous layers encompassing both conventional and nonconventional security issues including emerging security concerns like cyberwarfare.

Cyberwarfare against South Korea Today

While subject to debate, cyberwarfare remains a persistent threat against South Korea in the present day. China and North Korea pose continuous threats to South Korea, which has in turn become an exceptionally viable target for these cyber operations, aligning with the strategic objectives of these actors.

China

China's capabilities in the realm of cyberwarfare are regarded as highly menacing. According to assessments of U.S. intelligence agencies, China's cyberwarfare prowess ranks among the most potent globally, placing it on par with Russia. The 2022 Annual Threat Assessment from the U.S. Office of the Director of National Intelligence (ODNI) asserts that China almost certainly possesses the capacity to execute cyberattacks capable of inducing localized and short-term disturbances in critical U.S. infrastructure.[27]

Ever since Xi Jinping assumed leadership, China has dedicated itself to becoming the preeminent global cyber superpower. Over the past decade, Xi Jinping has placed significant emphasis on augmenting cyber prowess. Following his ascension to office, a consistent restructuring of military and intelligence entities has taken place. This restructuring has

facilitated the establishment of an unprecedented framework for the development and execution of hacking technology, characterized by the seamless fusion of military, intelligence agencies, and private entities. China's strides in cyber capabilities are projected to intensify, particularly with the commencement of its space station missions in 2021. China's self-built space station, also known as Tiangong, has been fully operational since late 2022.[28]

China's hacking endeavors and influence operations are integral components of its all-encompassing information warfare initiatives, harmonizing both physical and cyber domains. This interconnection signifies that China's cyber activities are closely interwoven with its information campaigns in the tangible world. These information activities align with an overarching national strategic objective: the pursuit of regional dominance.[29]

China's involvement in the 5G information and communication network supply chain have engendered apprehensions within South Korea, paralleling the concerns of its Western counterparts. These concerns stem from the profound implications for information security. Considering the intricate interplay between 5G technology and a plethora of Internet of Things (IoT) devices, China's sway over the information and communication technology (ICT) supply chain transcends mere hardware provision. This influence spans critical domains like cybersecurity and cyberwarfare, extending into realms of intellectual property, economic interests, and industrial advancement. Consequently, South Korea finds itself voicing escalating worries regarding China's sway over IT networks, materials, components, and equipment.[30]

China's overarching, seamlessly integrated, and medium- to long-term information activities, both in the digital realm and the physical world, are steered by a core strategy known as "Unrestricted Warfare" or "Chao Xian Zhan." This strategic framework is anchored in the belief that information activities serve as instrumental tools for achieving China's geopolitical objectives. In essence, Unrestricted Warfare signifies a departure from conventional notions of warfare, encapsulating a multifaceted approach that ventures beyond the boundaries of norms, ethics, and conventional reasoning. This strategy employs an extensive spectrum of unorthodox and non-normative methods, spanning organized crime, bribery, cyber technology appropriation, manipulation of political processes and elections, propagation of disinformation, economic reprisals, cultural maneuvering, and manipulation of public opinion.[31]

Unrestricted Warfare arises from China's strategic perception that it cannot achieve victory through traditional forms of warfare against the United States and its allies. Instead, it adopts an asymmetric or non-conventional approach. In this context, cyberespionage and information activities online are considered a means of warfare. The clear distinction between traditional war and peace becomes blurred, resulting in a constant state of peaceful warfare or a warlike peace.[32] This concept is somewhat similar to Russia's "Gerasimov Doctrine," in which non-military means are integrated with military methods to achieve strategic objectives.[33]

China's information activities can be broadly divided into two primary domains. The first pertains the acquisition of scientific and technological advancements, which in turn supports ongoing economic growth and the modernization of national defense capabilities. In this context, China conducts cyber espionage and cyber theft, alongside various offline methods. To achieve this, China focuses its efforts on advanced countries like the United States and other Western nations. Within Northeast Asia, South Korea and Japan are key targets for China's cyber operations aimed at pilfering industrial and defense science and technology.[34]

The extent of China's cyber espionage and theft efforts directed at South Korea is notably intense. Orchestrated by hacking groups with suspected affiliations to Chinese intelligence agencies, these activities have resulted in the illicit acquisition of industrial data. From December 2019 to May 2020, a total of 854 hacking attempts aimed at South Korea's biotech sector were recorded, with roughly 18% of these traced back to IP addresses originating in China. Moreover, in 2019, the South Korean cybersecurity firm East Security disclosed attempted cyberattacks on the nation's online game companies and media outlets, suspected to be the work of a Chinese APT hacking group. Additionally, the M-Trends 2019 report points to the Chinese APT 40 hacking group's involvement in cyber espionage endeavors aimed at globally renowned shipbuilding companies based in South Korea.[35] According to a South Korean cybersecurity official, in 2023 China was the second most important cyber security threat against South Korea only after North Korea both in attack frequency and degree of damage.[36]

The attacks orchestrated by Chinese hacking groups go beyond the theft of advanced industrial technology from South Korea. These hackers also target South Korean government agencies and steal military and security-related information. For example, in 2022, the Chinese hacking group known as Teng Snake infiltrated South Korea's Ministry of National

Defense's intranet, hacking into key institutions. This group claimed responsibility for hacking the South Korean Ministry of Health and Ministry of National Defense, stealing nearly 3.8 terabytes of data.[37]

Considering Teng Snake as a mere non-state hacking entity proves challenging. The organization's declarations on platforms like Twitter and Facebook add complexity, asserting that South Korea's potential NATO membership might incite a new war. They also claim possession of confidential documents linked to South Korea's Ministry of National Defense, along with unhindered access to its intranet. Given China's advanced hacking capabilities, it is more reasonable to speculate that South Korea has been susceptible to cyber espionage activities originating from Chinese intelligence authorities.[38]

Secondly, for years, China has been engaged in cyber influence operations as part of its "unrestricted warfare," directed at South Korean elites and the general public. These operations are designed to sway South Korea's orientation toward a more pro-Chinese and anti-American (as well as anti-Japanese) stance. Cyber cognitive operations, coupled with offline influence efforts like those through Confucius Institutes, have been utilized to reshape the opinions of both elites and the public, ultimately influencing election outcomes within South Korea.[39]

The core strategic objective of China's influence operations is to secure and expand pro-China factions and supporters within South Korea, thereby maximizing China's influence. To achieve this goal, various means are used in coordinated form. They include "economic retaliation and exploitative economic cooperation," "diplomatic pressure and coercion," "traditional media and mass demonstrations," "cyberspace manipulation," "organized crime and covert expansion," "influence expansion through the engagement of key figures such as opinion leaders, media, political parties, governments, academia, cultural and artistic communities, and civil society organizations," "cultural and historical appropriation," and many others. This pattern of Chinese influence operations poses a significant threat to South Korea, similar to many other countries including the US, Australia, Canada, the UK, Pakistan, Mongolia, and Taiwan. This strategy aims to foster distrust, antipathy, and ultimate paralysis of national identity and systems.[40]

Chinese internet services are indiscriminately collecting various types of information, including massive amounts of personal data. This poses a substantial threat to South Korea. China's targeted collection of personal information, known as "hybrid information collection," is carried out with

clear information collection objectives. When China engages in information operations against other countries, it identifies vulnerabilities of target individuals (such as financial debts or compromising personal information) to use as leverage for coercion, recruitment, bribery, or manipulation. By revealing sensitive information about key political figures, government officials, or socially influential individuals, China can manipulate public opinion. Moreover, it can identify vulnerabilities within domestic populations based on involvement, age, generation, and group, using them for propaganda or election interference. AI algorithms and technologies like deep learning enable such sophisticated influence operations. Similar large-scale incidents of personal data breaches have occurred in South Korea, with many involving North Korean or Chinese hackers and affiliated institutions.[41]

There have also been attacks on South Korea by patriotic Chinese hackers. In 2017, these attacks were in protest of the deployment of the Terminal High Altitude Area Defense (THAAD) system in South Korea. Chinese hackers used China's social media platform Weibo to make propaganda statements against South Korea and Lotte, a South Korean conglomerate. The groups that criticized the THAAD deployment and conducted hacking activities within South Korea were suspected to be large-scale hacker organizations with potential ties to the Chinese government. Prominent groups involved in these attacks include the Panda Intelligence Bureau (PIB), 1937cN, China Eagle Union, and Team Tonto. The targets of their attacks were Lotte Group and major government institutions in South Korea. From February to March 2017, they posted explicit criticisms and insults aimed at South Korea on the defaced webpages of the hacked South Korean institutions. The defaced screens displayed the logo of Panda Intelligence Bureau and an English message. The English message, translated from Chinese using a translation tool, was written in very basic English.[42]

North Korea

North Korea is another significant source of cyber threats against South Korea. The country's capabilities in cyberattacks and espionage activities are currently considered among the highest in the world. They have rapidly developed their capabilities within a short span of time, making them one of the most significant cyber threats globally. The U.S. cyber security firm Crowdstrike ranks North Korea's cyberattack capabilities as the second highest in the world, behind only Russia.[43]

North Korea has been enhancing its cyberattack capabilities since an early stage. The country recognized the significance and importance of cyber warfare after observing the Gulf War in 1991. As a result, North Korea has been training cyber warriors since the mid-1990s to address its economic and military asymmetry with South Korea. North Korea has developed considerable capabilities, organizations, and personnel for conducting cyberattacks, espionage activities, and various cybercrimes. Kim Jong Un's regime considers cyberwarfare as one of the three key pillars of North Korea's military capabilities.[44]

North Korea harnesses its cyber capabilities for diverse purposes, encompassing cybercrime, cyberattacks, cyber espionage, and preparation for cyberwarfare in the event of full-scale war. Firstly, within the realm of cybercrime, North Korea leverages its cyber prowess for financial gains through activities such as cryptocurrency hacking and ransomware attacks. Secondly, in the context of cyberattacks, North Korea deploys its cyber capabilities to execute retaliatory strikes in response to perceived provocations, as well as to instill fear and uncertainty among enemy governments and populations. This involves launching malware attacks against pivotal government institutions, financial organizations, critical infrastructure, and communication or broadcasting networks. Thirdly, in the realm of cyber espionage, North Korea employs its cyber capabilities to pilfer defense technologies, medical-pharmaceutical data, and other valuable scientific and technological information. Fourthly, the nation engages in information warfare activities, encompassing the dissemination of propaganda, psychological operations, and the propagation of misinformation, with a particular focus on South Korea. Lastly, North Korea is bolstering its cyber power to cultivate capacities for potential cyberwarfare, especially as a means of supplementing its comparatively inferior conventional military capabilities vis-a-vis South Korea and the United States.[45]

In the establishment and operation of North Korea's cyber capabilities, the central command center of utmost importance is recognized as the Reconnaissance General Bureau (RGB). Within the RGB, a highly skilled cyber unit, referred to as 'Unit 121,' stands as the central entity responsible for North Korea's cyberattacks and espionage endeavors. This Unit 121 boasts around 6,000 dedicated cyber agents and personnel. More recently, Unit 121 has gained notoriety for its involvement in hacking and ransomware attacks targeting worldwide financial institutions and cryptocurrency exchanges, including those situated in South Korea,

amassing substantial illicit proceeds. A portion of these ill-gotten gains has been channeled towards financing nuclear and missile development efforts.[46]

North Korean hackers are widely recognized for their advanced skills, and recent revelations indicate their active targeting of blockchain technology, resulting in substantial theft of cryptocurrencies. In August 2022, a research report highlighted that Lazarus, an APT attack group linked to North Korea, intensified its focus on infiltrating Apple's M1 chip. The Lazarus group is prominently known for targeting government, financial, and media institutions. One of its members, Park Jinhyuk, responsible for the WannaCry 2.0 ransomware attack, is featured on the FBI's Most Wanted list. Similarly, groups like BlueNoroff and Andarial are also actively engaged in cyberattacks against foreign financial institutions to generate illicit income. BlueNoroff, comprising around 1,700 members, successfully executed fund theft operations in South Korea. Meanwhile, Andarial, composed of approximately 1,600 members, specializes in identifying vulnerabilities within foreign computer networks. Another entity operating under the Reconnaissance General Bureau, Kimsuky, conducts international cyber espionage activities. According to reports, Kimsuky is involved in comprehensive espionage endeavors centered around security issues on the Korean Peninsula.[47]

North Korea's cyberattacks and cyber espionage activities against South Korea encompass a range of actions, including disseminating malicious code to major media and financial institutions, infiltrating computer networks of key governmental entities such as the Presidential Office and the Office of the Prime Minister, compromising university hospitals and university network servers, hacking organizations like Korea Hydro & Nuclear Power, and even breaching the organization and design plans of nuclear power plants within Hanwha Corporation. For instance, in 2021, attempts were made to hack six pharmaceutical companies located in South Korea, the U.S., and the UK. Among the targeted entities were Johnson & Johnson, Novavax, and Samsung BioLogics, all sought for their COVID-19 vaccine and treatment technologies. That same year, a hacking incident involving Kimsuky was reported, leading to the suspected technology leaks related to the KF-21 Boramae fighter jet and the Surion military helicopter. Additionally, in 2021, Kimsuky infiltrated a server and 62 PCs at Seoul National University Hospital, resulting in the exposure of 6,969 patient records. As of late August 2022, Seoul National University has emerged as the primary target for cyberattacks within South

Korea, with a notable portion of these originating from China and North Korea. This concentration of attacks on Seoul National University is attributed to the institution's profound scientific and technological expertise, as well as its advanced information and communication environment, rendering it an appealing entry point for attackers.[48]

North Korea's cyberattacks pose the greatest threat to South Korea. However, due to North Korea's low level of digitalization, effectively conducting cyberattacks against North Korea is very difficult. As a result, the cyber strategies of South Korea and North Korea exhibit asymmetric characteristics.[49]

In addition, North Korea actively employs online platforms such as websites, YouTube, Twitter, Facebook, etc., for conducting cyber cognitive warfare, propaganda, and influence operations directed towards South Korea. Recently, YouTube content featuring "mukbang (literally, 'eating broadcasting,' or videos showing people eating large quantities of food)" and daily life in North Korea by North Korean YouTubers such as YuMi and Song A has garnered significant worldwide attention. These channels have accumulated more than 10,000 views and subscribers, accompanied by a plethora of comments. YuMi's YouTube channel, established on January 27th, 2022, currently boasts 2.53 million subscribers and 1,865,377 views. North Korea's utilization of YouTube reflects its shift in external influence strategy. The YouTube content produced by YuMi and Song A actively promotes conspiracy theories that reinforce notions such as North Korea being a habitable country, unfairly isolated, and unjustly criticized by South Korea, the U.S., mainstream media, and the international community. Through the subtle association of YuMi and Song A, portrayed as attractive, benevolent, and seemingly ordinary individuals, North Korea is presented as a victim, thereby diluting its perceived aggression and barbarism. Such narratives have the potential to bolster beliefs in conspiracy theories and skepticism, potentially leading to a generally favorable outlook towards North Korea and a negative stance towards messages and reports from the South Korean and U.S. governments, mainstream media, and international community.[50]

Future of Cyberwarfare in Northeast Asia

The fundamental framework of the Northeast Asian security environment surrounding the Korean Peninsula, where South Korea-U.S.-Japan and North Korea-China-Russia intersect, could experience significant shifts contingent upon the outcome of the ongoing Russia-

Ukraine conflict. The paramount concern in this context is the potential decline of Russia's influence in Northeast Asia, regardless of the regaining strength of Russia elsewhere. Should Russia experience further weakening in military, economic, and social aspects, it could emerge as a destabilizing factor within the regional power balance. The waning of Russia's power in Northeast Asia could, in turn, foster the ascent of China's influence. Within the China-Russia-North Korea alliance, China's hegemonic leadership might consequently become more pronounced, bolstering its position.

This shifting landscape implies that the confrontation between China-Russia-North Korea, led by China, and the U.S.-Japan-South Korea, led by the U.S., is poised to intensify following the Russia-Ukraine War. As Russia's regional influence wanes, the power struggle between the U.S. and China will become more pronounced and discernible. Notably, the contrast between the historical U.S.-Soviet Cold War and the current U.S.-China power rivalry accentuates the heightened precariousness of the Korean Peninsula and Northeast Asia. During the post-Korean Armistice period of the Cold War, Northeast Asia experienced relative stability and was not a primary focus of contention, unlike Europe and the Middle East. Moreover, two opposing camps were clearly segregated. However, these conditions do not hold in the context of a new Cold War between the U.S. and China. Unlike the USSR in the past, China is not satisfied with the current division between North and South Korea. In this iteration, Northeast Asia occupies a central role as a theater of conflict, and the two opposing factions remain interconnected through the internet, economic trade, sociocultural exchange, and the movement of people. This intricate interdependence underscores the complexity and potential volatility of the current situation.

Amidst this intense hegemonic competition within the region, both the U.S. and China find it challenging to discover compromises that can satisfy all parties. The U.S. is compelled to uphold its position as a global and regional hegemon in the area, while China, in alliance with North Korea and Russia, seeks to displace the U.S. from the region to establish its sphere of influence. Within this tense confrontation, three pivotal variables have the potential to reshape the outcome of the geopolitical rivalry between these two factions.

The first variable revolves around the latent conflict between China and Russia. Despite collaborating on a hostile front against the U.S.-Japan-South Korea alliance, Russia harbors reservations about China's ambitions

for regional dominance. China's increasing security threat to Russia's Far East and Siberia strains their relationship. While China and Russia may forge a temporary strategic alliance against their common adversaries, it remains challenging for them to coexist harmoniously in Northeast Asia. China ultimately envisions a hegemonic order in the region that induces the retreat of both the U.S. and Russia.

The second variable pertains to the potential fall of the Kim Jong Un regime in North Korea. While accurately predicting the outcome of North Korea's economic, sociocultural, and demographic crises is complex, the collapse of the regime will inevitably reshape the dynamics of regional geopolitics.

Lastly, the third variable involves a potential shift in South Korea's direction. These shifts could arise due to forced regime changes, the election outcomes, increased economic reliance on China, and changes in the perceptions of both the elites and the general population. Such shifts could be facilitated by means of cyberwarfare orchestrated by China and North Korea. These three variables collectively represent influential factors that have the capacity to significantly alter the trajectory of the ongoing geopolitical competition between the two opposing camps in the region.

Due to its relative vulnerability compared to the US and Japan, South Korea becomes a primary target for China and North Korea, both of which seek to alter the existing regional status quo. China and North Korea consider cyberwarfare an ideal tool to disrupt South Korea's stability. This can be accomplished through two distinct avenues in the absence of a full-scale war.

First, cyber cognitive operations offer a highly cost-effective approach. Unfortunately, South Korea is currently experiencing significant societal divisions. The potential for a regime change, whether through elections or other methods, could push South Korea closer to the pro-Chinese camp. The nation's elites and populace are deeply polarized, creating fertile ground for external manipulation of information, interference, disinformation, and the sowing of discord among the elite class and the general public. This intricate political and sociocultural landscape provides ample opportunities for influencing elections through foreign information campaigns conducted over the internet. State-sponsored hacktivists and individuals unwittingly supporting foreign agendas could be strategically employed to impact election outcomes and public sentiment.

Secondly, South Korea remains a highly attractive target for cyber espionage and theft by China and North Korea. This preference is largely attributed to the profound political and social divisions existing among the nation's elites and the general public. Any proposals or efforts to fortify security measures against such cyber breaches can swiftly ignite intense political and social debates between the opposing political factions within South Korea. The severity of this political and social clash can at times escalate to a point approaching civil conflict, even in the absence of physical violence. Consequently, implementing substantial security measures becomes exceedingly challenging. This dynamic is a primary factor that has contributed to the prolonged absence of comprehensive cyber security legislation, despite the relentless onslaught of cyber espionage and theft campaigns from China and North Korea directed at South Korea.

Given this favorable context, Chinese and North Korean cyber operations are likely to continue targeting South Korea for a considerable duration. China confronts economic and technological constraints due to the western bloc led by the U.S. In response, cyber espionage and theft represent a strategic avenue to counteract this challenge. China views South Korea as a viable source for industrial information and technology acquisition, with cyber measures serving as an alternative to navigate the obstacles posed by the U.S.-led alliance. Moreover, these measures offer a means to gather intelligence on counter-Chinese diplomatic-security policies, military strategies, and defense technologies pursued by the U.S.-Japan-South Korea alliance. China perceives South Korea as a potential conduit for such critical intelligence, targeting not only South Korea but also extending its scope to encompass Japan and the U.S.

North Korea shares a parallel approach with China in this regard. Confronting severe economic sanctions and an ongoing requirement for financial resources to support nuclear capabilities and other conventional military expansions, North Korea seeks both funding and military-industrial technology. In this context, cyber espionage and theft become readily available tools of choice. South Korea is a fitting target in this scenario as well. Furthermore, North Korea aims to acquire insights into South Korea's security-diplomatic policies and military strategies pertaining to North Korea, in addition to those of the U.S.

Lastly, during a full-scale war, cyberwarfare emerges as a viable option for China and North Korea to bolster and augment their ground military operations, given their relatively inferior naval, air force, and

space capabilities compared to the US, Japan, and South Korea. Cyberwarfare will be employed for both preliminary and supportive attacks. In the context of a next Korean War, a blend of combatants, civilians, hackers, criminals, and radicals will be intricately intertwined, engaging in both online and offline warfare. The war will extend beyond the geographic confines of traditional battlegrounds. Cyberwarfare will be executed across the globe, transcending geographical boundaries.

In conclusion, South Korea occupies a central position as a major battleground for cyberwarfare, both during times of peace and in the event of a full-scale war in Northeast Asia. The significance stems from South Korea's positioning along the spectrum of pro-Chinese and pro-American alignment, which has the potential to sway the outcome of the geopolitical rivalry between the two opposing camps in the region. Therefore, it is imperative for the US, Japan, and South Korea to remain resilient against cyber aggressions from China and North Korea, whether during periods of peace or the potential outbreak of full-scale conflict. Northeast Asia has become the epicenter of the new wave of global conflict between the U.S. and China, in contrast to the previous iteration of the Cold War between the U.S. and the USSR. The victor in the geostrategic competition within Northeast Asia is likely to emerge triumphant in the broader New Cold War across the entire Eurasian continent. As such, in Northeast Asia, cyberwarfare stands out as a pivotal factor that could decisively influence the outcome of the geostrategic conflict, exerting a profound impact for years to come.

Notes:

[1] Sangbae Kim, *The US-China Digital Hegemonic Competition* (Seoul: Hanwool, 2022), pp. 120-123

[2] ROKA (Republic of Korea Army), "Future Operational Environment Analysis," ROKA Training and Doctrine Command, 2022, p. 41

[3] David Killcullen, *The Accidental Guerrilla: Fighting Small Wars in the Midst of a Big One* (New York: Oxford University Press, 2009)

[4] Global Firepower Index 2023 - World Military Strength Rankings (byjus.com)

[5] Benjamin Wittes and Gabriella Blum, *The Future of Violence: Robots and Germs, Hackers and Drones* (New York: Basic Books, 2015), pp. 17-90

[6] Francois Du Cluzel, "Cognitive Warfare," Innovation Hub, NATO Allies Command Transformation (ACT) Sponsored Study, innovationhub-act.org, 2020, pp. 5-35

[7] Paul Ottewell, "Defining the Cognitive Domain," OTH (Over the Horizon) Journal, December 7, 2020, https://othjournal.com/2020/12/07/defining-the-cognitivedomain/

[8] Soyeon Kim, Sungpyo Kim, Boemjun Park, Woonsub Jung, Hyunwoo Choo, Jeong Yun, and Jinyong Kim, "Cyber Electronic Warfare Technologies and Development Directions," *The Journal of Korean Institute of Electromagnetic Engineering and Science*, 2021, Vol. 32 No. 2, pp. 119-126.

[9] Minwoo Yun, *All Wars: Strategic Discourse on Cognitive Warfare, Information Warfare, Cyberwarfare, and Future War* (Seoul: Bakyoungsa, 2023), p. 300

[10] Wittes and Blum, *The Future of Violence: Robots and Germs, Hackers and Drones*, pp. 17-90

[11] Sergei A. Medvedev, "Offense-Defense Theory Analysis of Russian Cyber Capability," Thesis, Naval Postgraduate School, Monterey, California, USA, 2015

[12] Donald J. Reed, "Beyond the War on Terror: Into the Fifth Generation of War and Conflict," *Studies in Conflict and Terrorism*, 2008, Vol. 31 No. 8, pp. 686-690

[13] Minwoo Yun, "The Emerging Military Security and the Rise of Non-State Actors," In Sangbae Kim (ed.). *4th Industrial Revolution and Emerging Military Security* (Seoul: Hanwool, 2020), pp. 275-318

[14] Doohyun Nam, Taeho Im, Daejung Lee, and Sanggun Cho, "Mosaic Warfare in the 4th Industrial Revolution Era," *National Defense Review*, 2020, Vol. 63 No. 3, pp. 157-160

[15] Yun, *All Wars: Strategic Discourse on Cognitive Warfare, Information Warfare, Cyberwarfare, and Future War*, pp. 100-101

[16] Juha-Pekka Nikkarila and Mari Ristolainen, "RuNet 2020-Deploying Traditional Elements of Combat Power in Cyberspace?" in Juha Kukkola, Mari Ristorainen, and Juha-Pekka Nikkarila (eds.). *Game Changer Structural Transformation of Cyberspace. Puolustusvoimien tutkimuslaitoksen julkaisuja* 10 (Finnish Defence Research Agency Publications 10), Finnish Defence Research Agency, 2017, p. 194

[17] Ibid.

[18] Michael Sadykiewicz, "The Geostrategic Role of Korea in the Soviet Military Doctrine," *Asian Perspective*, 1983, Vol. 7 No. 1, p. 106

[19] Artyom Lukin and Georgy Toloraya, "Moscow's Diplomatic Game on the Korean Peninsula," In *Nuclear Weapons and Russian-North Korean Relations*. Foreign Policy Research Institute, Chapter 4, 2017

[20] Yun, *All Wars: Strategic Discourse on Cognitive Warfare, Information Warfare, Cyberwarfare, and Future War*, pp. 142-145

[21] Stephen J. Blank, "North Korea: Nuclear Threat or Security Problem?" *Journal of Indo-Pacific Affairs*, Air University Press, December 2, 2020, https://www.airuniversity.af.edu/JIPA/Display/Article/2432401/north-korea-nuclear-threat-or-security-problem/

[22] Yun, *All Wars: Strategic Discourse on Cognitive Warfare, Information Warfare, Cyberwarfare, and Future War*, p. 142

[23] Ibid, p. 143.

[24] Minwoo Yun, "The US-Russia Cybersecurity Rivalry and China-Russia Cooperation," In Sangbae Kim (ed.). *National Security Strategy 2.0 of Cybersecurity* (Seoul: Sahoepyeongron Academy, 2019), pp. 297-333

[25] Ibid

[26] Uidal Song, "China Prism," *Chosun Ilbo*, September 10, 2020

[27] Yun, *All Wars: Strategic Discourse on Cognitive Warfare, Information Warfare, Cyberwarfare, and Future War*, pp. 207-208

[28] "China to Double Size of Space Station, Touts Alternative to NASA-led ISS," *Reuters*, October 5, 2023; Yun, *All Wars: Strategic Discourse on Cognitive Warfare, Information Warfare, Cyberwarfare, and Future War*, pp. 207-208

[29] An interview with a South Korean security official

[30] "Potential Threat Vectors to 5G Infrastructure," CISA, ODNI (Office of Directorate of National Intelligence), 2021, www.odni.org.

[31] Liang Qiao and Xiangsui Wang, *Unrestricted Warfare* (Beijing: PLA Literature and Arts Publishing House, February 1999)

[32] Ibid

[33] M. K. Mockew, "The Gerasimov Doctrine," *Politico Magazine*, September/October 2017.

[34] Yun, *All Wars: Strategic Discourse on Cognitive Warfare, Information Warfare, Cyberwarfare, and Future War*, 186

[35] Ibid, pp. 213-214

[36] An interview with a South Korean cybersecurity official

[37] *Boan News*, "China, Spy Activities Against One Belt, One Road Target Countries," June 16, 2019

[38] Patrick Howell O'Neill, "How China Built a One-of-a-Kind Cyber-Espionage Behemoth to Last," *MIT Technology Review*, March 12, 2022

[39] An Interview with a South Korean security official

[40] Yun, *All Wars: Strategic Discourse on Cognitive Warfare, Information Warfare, Cyberwarfare, and Future War*, 186

[41] Song, "China rism."

[42] Mincheol Im, "Cyberattacks Spread Under the Pretext of Retaliating for THAAD from China," *ZDNET Korea*, March 8, 2017; Jun Kwon, "Chinese Hacker Organizations Mobilize to Attack Korea. General Mobilization Order for Defense Information Leaks," *Boan News*, March 8, 2017

[43] Bomi Kim and Ilsuk Oh, "North Korea's Cyber Threats in the Kim Jong Un Era and Major Countries' Responses," INSS Strategic Report, Institute for National Security Strategy, 2021, https://inss.re.kr/upload/bbs/BBSA05/202112/F20211206172938667.pdf

[44] Ibid

[45] Ibid

[46] Ibid

[47] Yun, *All Wars: Strategic Discourse on Cognitive Warfare, Information Warfare, Cyberwarfare, and Future War*, 172-173

[48] Ibid, 173-174

[49] An Interview with a National Cybersecurity Center official

[50] Minwoo Yun, "North Korea's Use of YouTube as a Cognitive Warfare," *Global NK Zoom & Connect*, April 17, 2023. Global North Korea (globalnk.org)