JULY 2025

Forging Forward

South Korea's Proactive Cyber Defense and Strategic Cooperation with the United States

By Joohui Park and Donghee Kim

Introduction

When countries design their cyber defense strategies, they do so on the premise that they can defend against malicious cyber operations only after the impacts of such acts materialize. Instead of taking this reactive posture, however, the United States spearheaded a paradigm shift to a proactive posture in 2018, when the Department of Defense (DOD) developed the **"Defend Forward" strategy**. This posture has since been maintained in the United States, and was reaffirmed in the introduction of the **2023 Department of Defense Cyber Strategy**. Variations on this approach have been adopted by some countries, including the Republic of Korea (ROK). South Korea introduced a proactive approach to cyber defense in its 2024 National Cybersecurity Strategy, some aspects of which **mirror** the DOD's Defend Forward.

Proactive cyber defense is just one option available to countries responding to cyber threats. In general, response options are various and can be structured with a range of typologies. For instance, options can diverge into defensive and offensive responses; defensive responses, in turn, can be classified as either reactive or proactive. Public attribution and countermeasures under international law are examples of reactive defense; proactive defense can include active cyber defense and other threat-hunting activities. In certain circumstances, alternatives to proactive cyber defense can be more effective. This paper is based on this conceptualization.

For proactive defense, countries need to glean insights into adversaries' acts in cyberspace before their impacts reach the intended targets. These insights are mostly embedded in physical infrastructures that adversaries exploit for malicious cyber operations—facilities primarily located in foreign territories. That is why working with allies and partners is crucial for proactive cyber defense. Fortunately, South Korea and the United States have made a great effort to cooperate in this space over the last few years. Such cooperation is primarily based on the alliance between the two countries. This paper aims to explore areas in which South Korea and the United States must deepen their collaboration to bolster their proactiveness in cyber defense.

South Korea's Cyber Defense Shift

MOVING TOWARD A PROACTIVE POSTURE

2019 National Cybersecurity Strategy

In 2019, the administration of former South Korean President Moon Jae-in unveiled South Korea's first **National Cybersecurity Strategy**. The defensive stance outlined in the 2019 strategy can be characterized as reactive rather than proactive. The strategy's second strategic task, "enhancement of cyberattack response capability," offers a glimpse into this reactive stance. According to the **2019 National Cybersecurity Basic Plan**, an implementation plan of the 2019 strategy, the administration, with a view to enforce cyberattack response capabilities, undertakes to (i) secure cyber deterrence by managing vulnerabilities and taking steps for attribution; (ii) fortify readiness against massive cyberattacks by revamping the framework for national response and developing cyberattack detection technologies; (iii) seek comprehensive and active means of response through international cooperation with like-minded partners and reinforcement of cyber warfare capacities; and (iv) improve cybercrime response by enhancing investigation and prosecution capabilities. In sum, the 2019 strategy appears to have been crafted without consideration of the proactive defense concept. The 2019 strategy is significant in that it represented the first-ever national cybersecurity strategy in South Korea and established a governance framework where the National Security Office of the Blue House took the lead in national cybersecurity. However, its strategic ideas concerning cyber defense seem to have remained at a rudimentary stage.

2024 National Cybersecurity Strategy

In February 2024, then-President Yoon Suk Yeol's administration made public the **second National Cybersecurity Strategy**, which shifted South Korea's approach to an offensive posture. In the 2024 strategy, the country set the "development of offensive cyber defense and response capabilities" as one of three primary objectives crucial to fulfilling its strategic vision of acting as a "global pivotal state." To that end, South Korea set forth five strategic tasks, one of which is "enhancing offensive cyber defense activities."

Although the 2024 strategy calls its defensive posture "offensive cyber defense," the strategy's posture is not so offensive that such naming is necessary, particularly considering the subtasks that South Korea is indeed planning to carry out to fortify "offensive cyber defense." The strategy's subtasks are specified in the **National Cybersecurity Basic Plan**, which details the activities that the administration intends to implement in pursuit of offensive cyber defense. These include establishing public attribution; tracing threat actors' cyber infrastructure; issuing joint advisories; and collecting and analyzing threat intelligence over attack origins, among other things. Although some of these subtasks may have offensive elements, these activities do not comfortably fit under the term "offensive."

Furthermore, inadequate naming could give rise to mischaracterization and misinterpretation, and thus escalation. It is hard to draw a clear line between the defensive and the offensive in cyberspace. In the spectrum of cyber activities, purely defensive actions such as firewall protections sit at one end, while offensive operations to destruct or destroy targets sit at the other end. It is hard to tell where on this spectrum the administration's "offensive cyber defense" sits. Given this, use of the term "offensive" may risk signaling that South Korea would resort to the spectrum's offensive extreme, which is not the intention reflected in the strategy.

In order to enhance offensive cyber defense, the Yoon administration's **strategy** highlights three main activities, some of which can be regarded as reflecting a proactive approach. The first is attribution. In the strategy, South Korea stated that it will identify the perpetrators of cyberattacks that impair national security and national interests by mobilizing the legal and technical capabilities necessary for attribution. The country also emphasized that it will use scientific evidence to identify actors behind cyberattacks and hold them accountable for their malicious behavior. To this end, South Korea is set to establish **a procedure and standard for attribution** and employ it to build a foundation for international cooperation.

The second activity highlighted in the strategy is the strengthening of joint deterrence with partner countries. The administration seeks to maximize deterrence of threat actors through the issuance of joint cybersecurity advisories, which South Korea has actively issued with partners over the last few years. For instance, in July 2024, South Korea issued **a joint cybersecurity advisory on APT40**—a group sponsored by China—with the relevant ministries of Australia, Canada, Germany, Japan, New Zealand, the United Kingdom, and the United States. In the same month, South Korea, the United Kingdom, and the United States issued **a joint security advisory on the activities of the Andariel**, a hacking group under the Reconnaissance General Bureau of North Korea.

The third activity is preemptive and proactive response through active detection and attack origin analysis. This reflects an approach similar to the United States' Defend Forward. South Korea's strategy gives its intelligence agency and its military a preemptive and proactive mission to detect and analyze the sources of cyberattacks, catch signs of attacks in advance, and quickly share information with relevant ministries. To implement this, the **2024 National Cybersecurity Basic Plan** states that South Korea will develop technologies to identify threat actors and track their bases, infrastructure, and activities. Notably, there is a nuanced difference between attribution and the identification of the source of a cyberattack. The former is a procedure necessary to impose responsibility—i.e., legal or political costs—on persons or states conducting malicious acts in cyberspace. On the other hand, the purpose of source identification is to proactively track down the source of the attack before the intended target is affected, reducing the impact (if any) on the target's network. With this third element, South Korea can be seen as taking a step toward proactive cyber defense.

ORGANIZATIONAL FRAMEWORK AND PROACTIVE CYBER DEFENSE

In South Korea, the National Security Office (NSO) is **responsible** for coordinating overall cybersecurity-related tasks as well as setting up and reviewing mid- to long-term policy directions. Under the coordination of the NSO, governmental agencies and departments carry out their respective cybersecurity-related responsibilities. In particular, the National Intelligence Service (NIS) and the Cyber Command under the Ministry of National Defense (MND) play central roles in proactive cyber defense.

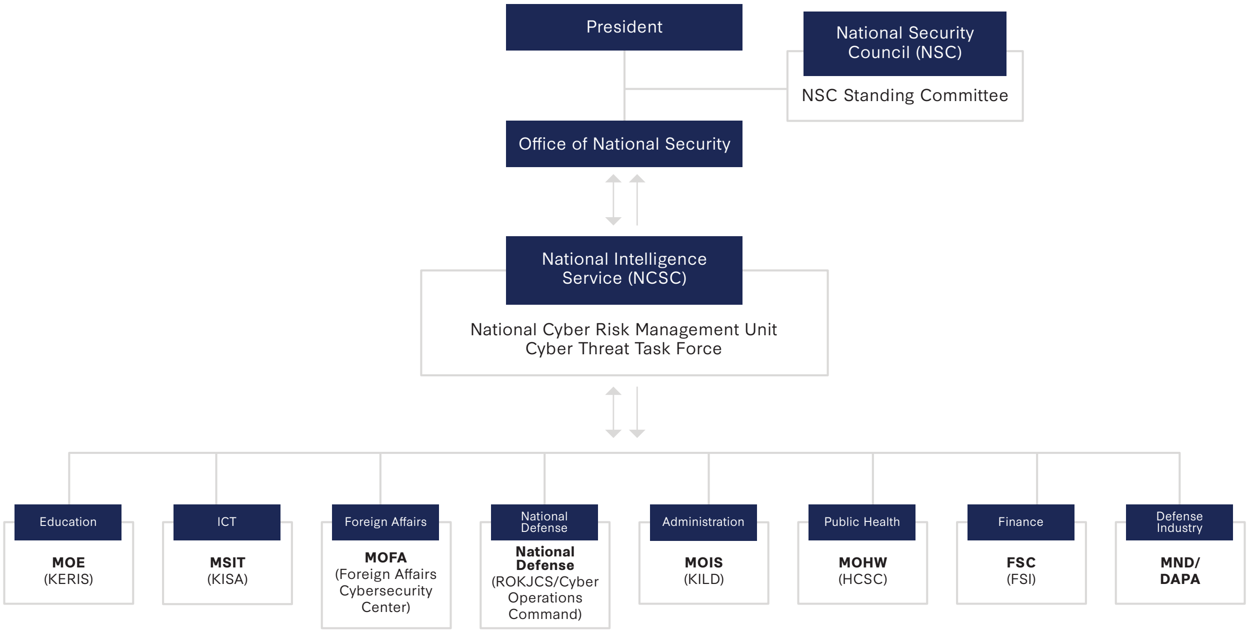
As South Korea rearranged its cybersecurity strategy in 2024, the National Intelligence Service Act and its presidential decree, the Regulation on Cybersecurity Duty, were amended accordingly and entered into force. As a result, the NIS's four major cybersecurity duties became more refined and streamlined. First, the NIS performs intelligence activities for national cybersecurity. That is, the NIS collects, prepares, and distributes intelligence on international hacking organizations or state-sponsored hacking groups (**NIS Act**, Article 4(1)(1)(e); **Regulation on Cybersecurity Duty**, Article 3(1)(a)). Second, the NIS takes measures to identify, deter, and block threatening cyber activities conducted by North Korea; foreign states, nationals, or organizations; transnational actors; or South Koreans affiliated with any of these entities (NIS Act, Article 4(1)(3); Regulation on Cybersecurity Duty, Article 3(1)(b)). Third, the NIS takes preventive and responsive measures against cyberattacks and threats on public entities (NIS Act, Article 4(1)(4); Regulation on Cybersecurity Duty, Article 3(2)(a)). Fourth, the NIS is entitled to establish and operate a consolidated response governance in which public and private entities jointly work to manage and respond to crises (Regulation on Cybersecurity Duty, Article 6 *bis* (4)). In the event of a crisis, the NIS's National Cyber Security Center (NCSC) serves as the Cyber Threat Task Force (CTTF) tasked with responding; in times when there is no active crisis, the agency functions as the National Cyber Risk Management Unit (NCRMU).

In the context of South Korea's proactive cyber defense, Article 6 *bis* of the Regulation on Cybersecurity Duty must be highlighted. This article was newly introduced in the revised Regulation on Cybersecurity Duty in 2024. According to paragraph three of Article 6 *bis*, the director of the NIS may take necessary steps to proactively identify, deter, and block activities against national security and interests. Such measures under this provision may include tracking and neutralizing foreign and North Korean bases. This provision provides a legal basis for the NIS's proactive cyber defense.

South Korea's Cyber Command also assumes cybersecurity tasks, mostly those related to national defense. The Cyber Command was established under the MND to take control of these duties in 2011 (**Presidential Decree on Cyber Command**, Article 1; the Cyber Command was originally established in 2010 under the Defense Intelligence Command of the Ministry of National Defense. In 2011, the Cyber Command became a unit directly subordinate to the Ministry of National Defense, per the Presidential Decree on Cyber Command enacted in that year). The Cyber Command's duties include planning and executing cyber operations and related cybersecurity needs; developing and establishing frameworks necessary for cyber operations; and collecting, analyzing, and utilizing cyber threat intelligence (Presidential Decree on Cyber Command, Article 2). In addition, the Defense Counterintelligence Command under the MND supports cyber defense and information warfare (**Presidential Decree on the Defense Counterintelligence Command**, Article 4(5)).

South Korea's governmental structure for cybersecurity is illustrated in the graphic below.

Figure 1: South Korea's National Cybersecurity Implementation Framework



Note: MOE refers to the Ministry of Education; KERIS refers to the Korea Education and Research Information Service; MSIT refers to the Ministry of Science and ICT; KISA refers to the Korea Internet and Security Agency; MOFA refers to the Ministry of Foreign Affairs; ROK JCS refers to the ROK Joint Chiefs of Staff; MOIS refers to the Ministry of the Interior and Safety; KILD refers to the Korea Local Information Research and Development Institute; MOHW refers to the Ministry of Health and Welfare; HCSC refers to the Health and Welfare Cyber Security Center; FSC refers to the Financial Services Commission; FSI refers to the Financial Security Institute; MND refers to the Ministry of National Defense; and DAPA refers to the Defense Acquisition Program Administration.

Source: 2024 National Cybersecurity White Paper.

South Korea's Cooperation with the United States for Proactive Cyber Defense

THE U.S. APPROACH AND DEFEND FORWARD

The crux of proactiveness in the United States' cyber defense is reflected in the "Defend Forward" posture. In 2018, the year after President Donald Trump began his first term in office, the DOD's **cyber strategy** introduced Defend Forward, which represented a new approach: the idea of moving as close as possible to the origin of an adversary's activity as a way of defending against it. Defend Forward was first introduced in the 2018 vision document of the U.S. Cyber Command: **Achieve and Maintain Cyberspace Superiority: Command Vision for US Cyber Command**. According to the document, the United States will defend forward to disrupt and stop malicious cyber operations–including activities below the level of armed conflict–at their origin. The United States emphasizes that although Defend Forward involves activities on the adversary's network and not the U.S. network, **this is still a defensive activity**, not an offensive one.

Defend Forward is inextricably linked to the concept of persistent engagement. The United States introduced the philosophy of persistent engagement in recognition of the fact that Cyber Command needs to engage with enemies on an ongoing basis in order to disrupt or impair their capabilities. The goal of persistent engagement is to identify and stop overseas cyber threats before they reach the U.S. network. Persistent engagement is designed to ensure that Cyber Command's Cyber National Mission Force takes and maintains the initiative to succeed in **the daily competition** with enemies.

The spirit of Defend Forward and persistent engagement is reflected in a **metaphor** from General Paul Nakasone, former commander of U.S. Cyber Command: "Our naval forces do not defend by staying in port, and our airpower does not remain at airfields. They patrol the seas and skies to ensure they are positioned to defend our country before our borders are crossed. The same logic applies in cyberspace."

The Biden administration continuously adopted Defend Forward under Pillar II ("Disrupt and Dismantle Threat Actors") of its **2023 National Cybersecurity Strategy**. The strategic tasks in Pillar II aim to mobilize all powers to prevent malicious cyber actors from threatening national security and public safety. The United States elaborated that it would expand private sector participation in neutralizing malicious cyber activities and promote cooperation with international partners. The **DOD** signaled that, in line with the 2023 National Cybersecurity Strategy, it will continuously defend forward by disrupting the malicious cyber activities and degrading their supporting ecosystems. (In the same year, General Nakasone **stated that** "There was a huge inflection point in 2018 with the Defend Forward [strategy]. I don't see, necessarily, a huge change in the strategy coming out.")

ROK AND U.S. CYBER DEFENSE APPROACHES: DIFFERENCES AND COMMONALITIES

There are both shared features and divergences between the proactive cyber defense approaches of the ROK and the United States. In order to identify possible areas for cooperation between the two countries, these commonalities and differences need to be analyzed.

Differences

First, the U.S. and South Korean approaches have different backgrounds. One of the underlying reasons for the United States' paradigm shift toward a proactive posture is the **failure** of the U.S. cyber deterrence strategy prior to 2018. In early cybersecurity strategy formulations, the United States primarily perceived acts that reached the use-of-force threshold as severe cyber threats. However, the malicious cyber operations to that point—such as the 2014 Sony Hack, the OPM breach, and the DNC hack—had been below the level of use of force. Minor but frequently occurring cyber incidents, meanwhile, had been neglected but were having cumulative and erosive impacts on national security. Recognizing this threat landscape, the United States devised the strategies of **Defend Forward** and persistent engagement in order to contest daily competition in cyberspace. In contrast, South Korea's embrace of a proactive stance is not rooted in such reflection. Rather, South Korea took note of the inherent nature of cyber threats. In short, the hyper-connectedness of cyberspace makes complete prevention and defense against cyber threats too constrained.

Whatever the origin of South Korea's approach, it is evident that the major threats the country has experienced are not at or above the level of use of force. For instance, in May 2024, one terabyte of data from South Korea's Supreme Court was stolen by Lazarus, North Korea's hacking group. Yet physical and tangible damage—which would normally be calculated to assess whether an incident justifies use of force—was not caused. However, significantly sensitive personal information was **leaked**, including information on resident registration, marriage, and medical certificates. These types of damage could have a knock-on impact that could threaten national security. Accordingly, South Korea's cyber defense posture must be calibrated to adequately disrupt such low-level activities.

Second, leadership frameworks for defending proactively also differ between the two countries. In the United States, a single leader serves as the director of the National Security Agency (NSA) and the commander of the U.S. Cyber Command. This dual-hatted leader coordinates Defend Forward operations by integrating intelligence. However, the roles of the South Korean NIS and Cyber Command are not integrated for the purpose of proactive cyber defense. Although the NIS's National Cyber Security Center (NCSC) can operate a consolidated response system in which public and private entities can cooperate to manage and respond to crises (Regulation on Cybersecurity Duty, Article 6 *bis* (4)), this framework is primarily crisis-based, requiring a certain threshold to operate. In addition, the NIS and Cyber Command are entitled to engage in proactive defense separately under national law, although cybersecurity intelligence can be shared between them (Regulation on Cybersecurity Duty, Article 5). As a result, who takes the lead in proactive defense and how the authorities cooperate is not well-defined in South Korea.

Commonalities

In both countries, intelligence collection on cyber threat sources is key for successful proactive defense. **Gathering intelligence**–thereby gaining insights on adversaries' weaknesses, intentions, and capabilities–is a crucial step for defending forward as close as possible to the origin of adversary activity. In its **2024 strategy**, South Korea also highlighted an intent to bolster reconnaissance and intelligence on the sources of cyberattacks. Preemptively catching indications of malicious activities by detecting and analyzing sources is underlined as one of the subtasks of proactive cyber defense. By proactively discovering adversaries' malware and tactics and degrading their capabilities to conduct malicious cyber operations, South Korea and the United States could prevent such activities at the source before reaching their networks.

If threat hunting is limited within one nation's border, the success of proactive defense is limited as well. A proactive defense posture thus necessitates partnering with foreign countries. Indeed, the United States' Defend Forward requires the country to conduct activities **outside of U.S. networks**–both in allies' and partners' networks and in those of adversaries. Thus, the U.S. Cyber Command views partnerships as an integral component of Defend Forward. In this vein, hunt forward operations–defensive cyber operations conducted at the invitation of a host nation–must be highlighted. Upon invitation, the U.S. Cyber Command's Cyber National Mission Force deploys a team to a host country to observe and detect malicious cyber operations there. As of March 2023, hunt forward teams had been deployed on **at least 47 missions** in more than 20 countries. With a view toward enhancing capabilities to collect and analyze threat intelligence, South Korea is **planning** to expand the exchange of threat intelligence with foreign intelligence agencies. Compared to the United States' rich experience in partnering with other countries for proactive cyber defense, including in hunt forward operations, South Korea has limited experience in this regard.

OPERATIONALIZING COOPERATION FOR PROACTIVE CYBER DEFENSE

The ROK-U.S. Alliance and Proactive Cyber Defense

At this moment, many uncertainties hang over the alliance between South Korea and the United States, as well as the paths of their respective national cybersecurity strategies. President Trump has commenced his second term in the White House and is reshaping his country's cybersecurity resources. South Korea is currently standing in the fog of uncertainty created by this political transition. Many have cast doubts on President Trump's willingness to promote U.S. alliances, including the partnership with South Korea. Furthermore, experts have been raising concerns that the absence of leadership in South Korea will put the ROK-U.S. alliance in peril.

Nevertheless, the following two principles cannot be reversed. First, the principle that the ROK-U.S. alliance applies to cyberspace must stand. Fortunately, South Korea and the United States still seem to share a common understanding that their alliance—which has lasted over 70 years—must be sustained. The foreign ministers from Seoul and Tokyo and the U.S. secretary of state met in February 2025 and discussed the necessity of enhancing the strength of their countries' alliances to ensure peace and prosperity. In addition, the United States reaffirmed its commitment to strengthening extended deterrence cooperation through **the ROK-U.S. and Japan-U.S. alliances**. In this vein, the **Strategic Cybersecurity Cooperation Framework** (SCCF), a legacy of President Yoon and President Biden, must be underscored. On April 26, 2023, the two presidents created the SCCF, signaling their agreement that the ROK-U.S. alliance applies to cyberspace. Whatever the cooperation framework, South Korea and the United States must consider this a cardinal principle.

Second, the proactive posture in cyber defense must not be abandoned. Strategic thinking evolves as cyber threats evolve; accordingly, defense has been evolving from reactive to proactive as countries adapt to the nature of cyberspace. In the words of cybersecurity experts Eric Talbot Jensen and Sean Watts, "cyberspace's **structural feature** of interconnectedness and its core condition of constant contact creates a strategic necessity to operate continuously in cyberspace." This means, as **General Nakasone** has put it, that we must not just "wait for cyber attacks to affect" our networks. In effect, it is hard to imagine that the United States and South Korea would abandon their proactive postures and reassume reactive postures, since this would go against the evolution of strategic thinking.

Laying Out South Korea's Priorities

Based on the previous analysis of the similarities and differences between the two nations' proactive approaches, this paper suggests five major considerations for South Korea to prioritize in its cooperation with the United States. Some of these are intended for both countries, while others are priorities specifically on the South Korean side.

First, the two nations need to think about a suitable cooperation framework for proactive cyber defense. Under the SCCF, the two countries undertook discussions of how the **Mutual Defense Treaty** between the United States and the Republic of Korea (MDT) applies in cyberspace. When it comes to the two countries' cooperation on proactive cyber defense, however, the MDT's role would be limited. That is because the provisions under the MDT largely address armed attack situations. The treaty contains only six articles that strengthen the two countries' efforts for collective defense. Article I outlines the two countries' commitment to the peaceful settlement of disputes and non-use of force, echoing the corresponding principles under the UN Charter. Articles II and III touch upon the two countries' cooperation when one or both are threatened by an armed attack. Article IV regulates the right to deploy U.S. forces in the territory of South Korea. The final two articles contain miscellaneous provisions on ratification, entry into force, and termination of the treaty. As illustrated earlier in this paper, proactive defense posture has been introduced in national policy mainly due to cyber threats occurring below the use-of-force threshold. Of course, proactive cyber defense is not exclusive to low-level threats, but its necessity is most pronounced at that level. Consequently, South Korea and the United States need to pursue a cooperation mechanism that enables them to proactively defend against malicious operations, including those posed below the use-of-force level.

Second, South Korea and the United States need to define the main threat actors against which they intend to proactively defend each other. According to the **2024 National Cybersecurity Strategy**, South Korea is mainly introducing an offensive response directed at threats from North Korea. Unfortunately, the real threat landscape is a bit different. For instance, pro-Russian cyber actors conducted **distributed denial-of-service (DDos) attacks** against ROK governmental websites, including that of the MND, after North Korea dispatched troops to Russia. In addition, damage caused by **China's cyber operations** has been increasingly acknowledged as severe. Whether or not to explicitly indicate threat actors in a policy document depends upon a nation's strategic calculations. South Korea and the United States, however, must identify and agree upon a common threat actor against whom proactive defense can be meaningfully employed.

To identify common threat actors, South Korea and the United States should be able to assess the feasibility and effectiveness of proactive defense measures against these threat actors, considering diverse elements like infrastructure footprints, geopolitical relations, and technical capabilities. Based on such assessments, South Korea and the United States could pinpoint shared threat actors against which collaborative proactive defense would yield a successful impact.

Third, South Korea and the United States must discuss how to successfully build collective inoculations of their networks. Proactive cyber defense aims to defend against malicious acts before they impact a country's networks; to achieve such a goal, technical capabilities must be geared up well and outputs of technical analysis must be appropriately shared. At times, such technical measures for proactive hunting must be disseminated worldwide. To this end, cybersecurity advisories can be useful. By inoculating their own networks or global networks, the two countries can compete with malicious actors under more favorable conditions. Accordingly, South Korea and the United States must engage in dialogue on how to collaboratively raise their own technical capabilities and share these capabilities with the world for proactive defense.

Fourth, South Korea needs to rearrange its organizational framework for proactive defense and efficient intelligence sharing. Although the U.S. NSA and Cyber Command have different roles in national cybersecurity, they are directed by a single leader. This allows the United States to speedily leverage threat intelligence in cyber operations like Defend Forward. Moreover, the outputs of the command's work during hunt forward operations are appropriately **shared** with the Federal Bureau of Investigation, the Department of Homeland Security, and private companies. Releasing adversaries' malware obtained during hunt forward missions to the cybersecurity community makes that malware less effective because reactive defense can be used to detect and defeat it. In this way, the United States' proactive cyber defense can **inoculate** U.S. networks.

In South Korea, measures for proactive cyber defense are not carried out within one integrated framework. The NIS and Cyber Command are entitled to engage in proactive defense separately under national law. The consolidated response framework led by the NIS's NCSC, in which public and private entities can cooperate, functions primarily on a crisis base. This organizational framework may hinder timely intelligence sharing among relevant agencies and private entities. Considering the advantages of the United States' dual-hat leadership and its extensive experience in intelligence sharing, South Korea's organizational structure must be reexamined and coordinated.

Fifth, the legal limitations of proactive cyber defense must be explored. Proactive cyber defense entails actively detecting and analyzing the sources of malicious cyber activities. Unfortunately, these sources are physically located in other countries' territories and subject to the sovereignty of these states. Even though the international community has not reached a common understanding of how and when a state's territorial sovereignty can be breached through activities in cyberspace, South Korea needs to engage in proactive defense activities within these legal considerations. In this vein, South Korea may gain lessons from the United States' "**away game**" experiences (operations that, like Defend Forward, involve activities outside U.S. networks). The United States' experiences in away games are richer than those of other countries, and some of them are publicly available, with details of successful cases sometimes disclosed. South Korea may reference the United States' legal logic in such situations.

Conclusion

As cyber threats evolve, the tools that states devise in response evolve accordingly. Proactive cyber defense is a tool that is well-adapted to cyberspace's inherent features and threats. South Korea introduced a proactive defense posture in its 2024 National Cybersecurity Strategy, with an ultimate goal similar to the United States' Defend Forward. The concept of proactive cyber defense requires cooperation among states, as it requires tracking traces left by malicious actors globally. Given this landscape, cooperation with the United States—the most experienced country in proactive defense—is imperative for South Korea. In conclusion, this paper, as suggested above, proposes five key areas for the two nations' cooperation to promote proactive cyber defense. South Korea and the United States need to (i) establish a suitable cooperation framework for proactive cyber defense; (ii) define the main threat actors against which they intend to proactively defend each other; and (iii) discuss how to successfully build collective inoculations of their networks. Furthermore, South Korea needs to: (i) rearrange its organizational framework for proactive defense and efficient intelligence sharing and (ii) explore the legal limitations of proactive cyber defense. ■

***Joohui Park** is a senior researcher on the Cybersecurity Policy Research Team at the National Security Research Institute in the Republic of Korea. **Donghee Kim** is a senior researcher and manager on the Cybersecurity Policy Research Team at the National Security Research Institute in the Republic of Korea.*

This report is made possible by general funding to CSIS and generous support from South Korea's National Security Research Institute.

This report is produced by the Center for Strategic and International Studies (CSIS), a private, tax-exempt institution focusing on international public policy issues. Its research is nonpartisan and nonproprietary. CSIS does not take specific policy positions. Accordingly, all views, positions, and conclusions expressed in this publication should be understood to be solely those of the author(s).

© 2025 by the Center for Strategic and International Studies. All rights reserved.