SEPTEMBER 2025

Mutual Defense in Cyberspace

Joint Action on Attribution

By: Julia V. Brock and James A. Lewis

On the seventieth anniversary of the U.S.-Republic of Korea (ROK) alliance, the leaders of the two countries **declared** that the Mutual Defense Treaty applies to cyberspace. The United States and South Korea agreed to expand the scope of the agreement and promote cooperation in cybersecurity technologies, policies, and strategies, including cyber threat information sharing.

The United States and the ROK have significantly strengthened their cybersecurity cooperation in recent years. South Korea's membership in NATO's Cooperative Cyber Defense Centre of Excellence laid the groundwork for enhanced information sharing, joint exercises, and the development of shared standards. The U.S.-ROK Cybersecurity Working Group, **established** in 2022, has focused on strengthening mechanisms for collaboration and joint defense, as well as defensive strategies. Both countries have also emphasized the importance of international partnerships in addressing cyber threats posed by authoritarian states. The U.S.-ROK Strategic Cybersecurity Cooperation Framework, signed in April 2023, further solidified this commitment by increasing information sharing and joint response efforts.

Washington and Seoul are actively engaged in countering cyber threats, particularly those from the Democratic People's Republic of Korea (DPRK). The Counter Ransomware Initiative (CRI), the U.S.-ROK-Japan Trilateral Summit, and the ROK's 2024 National Cybersecurity Strategy each highlight the shared goal of disrupting the DPRK's malicious cyber activities and protecting critical infrastructure. Recent memoranda of understanding (MOUs) between the United States and the ROK have further strengthened cooperation in areas such as computer emergency response team **communications** and supply chain **resilience**.

Current Cooperation Structures

The overarching structure for the U.S.-ROK alliance is the **2023 Strategic Cooperation and Coordination Framework** (SCCF). The SCCF provides a diplomatic mechanism to facilitate discussions between the two countries on a range of issues, particularly those concerning security, military cooperation, and regional challenges. The SCCF aims to enhance bilateral coordination, improve

strategic alignment, and address concerns related to the Korean Peninsula, North Korea, and other regional security matters.

The framework reflects the growing importance of cybersecurity and is an important component of the broader U.S.-ROK alliance. By working together, the two countries hope to deter cyberattacks, protect critical infrastructure, and promote a secure and stable cyberspace. The core areas of collaboration include the following:

1. **Intelligence Sharing:** This encompasses detailed information about North Korean cyber operations, emerging threats, attack patterns, and potential vulnerabilities. Washington and Seoul maintain secure channels for information exchange and conduct joint threat analysis. They share technical indicators, malware signatures, and attribution data in order to build a comprehensive understanding of the cyber threat landscape.
2. **Critical Infrastructure Protection:** The agreement establishes protocols for protecting energy grids, financial networks, transportation systems, and healthcare infrastructure. Both nations conduct vulnerability assessments, develop resilience strategies, and coordinate incident response plans. They share best practices for infrastructure security and collaborate on supply chain security.
3. **Cybercrime Cooperation:** Both countries share investigative resources, forensic capabilities, and information about criminal activities. They coordinate efforts to combat ransomware attacks, financial fraud, and data breaches. Joint investigation teams tackle cross-border cyber incidents, and streamlined processes facilitate rapid information exchange about emerging threats and criminal techniques. For example, the work of the CRI provides a collective approach for attribution and accountability.
4. **Joint Attribution:** Joint attribution—tracking and identifying the perpetrator of a cyberattack—by the United States and the ROK (and perhaps also including Japan, Australia, and other Five Eyes partners) may have an inhibiting effect on an opponent, particularly if linked to measures to create accountability, such as sanctions, indictment and other measures of retorsion.
5. **Capacity Building:** Collaborative programs improve both nations' cybersecurity capabilities. These include joint cyber defense exercises, personnel exchanges, and shared training programs. Technical expertise is exchanged in areas such as malware analysis, incident response, and network defense. The countries also collaborate on research and development projects for new cybersecurity technologies.
6. **International Cooperation:** The United States and South Korea work together in international forums such as the United Nations to promote responsible state behavior in cyberspace beyond bilateral relationships, and should continue to do so. They also advocate for common security standards, coordinate positions on cyber governance issues, and support regional capacity-building efforts. A multilateral approach involving other like-minded nations, including Australia, Japan, and the United Kingdom, would reinforce these efforts. The ROK relationship with the NATO Cooperative Cyber Defense Centre of Excellence is one such avenue for cooperation.

The SCCF included implementation mechanisms through a Joint Cyber Coordination Committee that oversees progress and adapts strategies as needed. Senior-level dialogues ensure continuous

alignment of objectives and approaches. Annual reviews assess the effectiveness of cooperation and identify areas for enhancement. Both countries can agree to conduct joint cyber exercises under the umbrella of the SCCF.

The SCCF also included provisions for addressing emerging technologies like artificial intelligence (AI), quantum computing, 5G/6G networks, and the **Internet of Things**. The agreement allows for changes to accommodate new threats and technological developments in the cyber domain, and emphasizes sustainable, long-term cooperation while maintaining the ability to respond rapidly to immediate threats. This comprehensive approach strengthens both nations' cybersecurity postures while contributing to broader regional stability in the Indo-Pacific. It also represents a significant step forward in establishing trusted partnerships for addressing evolving cyber challenges in an increasingly interconnected world.

Following the adoption of the SCCF, both nations are working to enhance their collaborative cyber defense capabilities. South Korea's 2024 **National Security Strategy** emphasizes developing its cyber workforce and strengthening international partnerships. This cooperation is especially crucial given North Korea's extensive cybercrime operations, which directly support the country's missile and nuclear programs. While bureaucratic differences have historically complicated U.S.-ROK cyber collaboration, both nations are committed to improving intelligence sharing and technical cooperation.

South Korea's Cyber Threat Landscape

South Korea is located at one of the most important intersections for geopolitical rivalry, and therefore is a target for cyberattacks. The country's primary adversaries in cyberspace include North Korea, China, and Russia.

NORTH KOREA

North Korea is South Korea's most dangerous adversary. Pyongyang has significantly improved its capabilities and expanded its cyber operations over the last decade, using cybercrime as a major source of funding. UN reports indicate that North Korean hackers **conducted** almost 60 cyberattacks on cryptocurrency companies between 2017 and 2023, stealing around $3 billion in total, **including** $1.7 billion in 2022 alone. These cyber activities now account for about **half** of North Korea's foreign currency income and may **fund** as much as 40 percent of its weapons of mass destruction programs, making cybersecurity a strategic priority. DPRK hacker groups have targeted South Korean digital infrastructure, including satellite facilities, courts, and defense contractors.

North Korea primarily employs cyberattacks for specific, calculated purposes such as financial gain, intelligence gathering, or disrupting South Korean infrastructure. While the regime has demonstrated the ability to launch sophisticated attacks, these are typically targeted and aimed at causing disruption rather than widespread destruction. North Korea is likely to continue its current strategy of using cyberattacks as a tool of coercion and intimidation. By launching smaller-scale attacks, the regime can signal its capabilities and influence regional dynamics without risking a full-scale conflict. However, if South Korea, the United States, and other allies further improve their cybersecurity defenses, North Korea may find it increasingly difficult to obtain funds and achieve its objectives through cyber operations.

CHINA

China's cyber operations against the ROK are multifaceted and ongoing. While specific details about these operations are often classified, public reports and cybersecurity research **suggest** several key areas of focus, including espionage and intelligence gathering. Chinese state-sponsored hackers have targeted South Korean government agencies, military installations, and defense contractors to steal sensitive information related to national security, military capabilities, and diplomatic strategies. Chinese hackers have also targeted South Korean **companies**, particularly those in high-tech sectors like semiconductors and electronics, to steal intellectual property and trade secrets.

China's cyberattacks against the ROK threaten South Korea's national security, economic interests, and democratic values. State-backed hackers have used social media platforms to spread disinformation and propaganda aimed at influencing public opinion in South Korea. This includes spreading false narratives, promoting pro-China sentiments, and undermining trust in democratic institutions. China has developed sophisticated cyberwarfare capabilities, including the ability to launch large-scale cyberattacks that could disrupt critical infrastructure and government systems. The South Korean government and private sector must continue to invest in cybersecurity defenses to protect against these threats.

RUSSIA

Russia has also used cyber actions against the ROK, primarily for intelligence purposes. Russia is believed to have engaged in cyber espionage against South Korean government agencies, defense contractors, and other sensitive sectors. The goal is typically to gather intelligence related to national security, defense technologies, **arms sales**, and geopolitical **dynamics** involving North Korea (especially given North Korea's decision to send troops to support Russia's invasion of Ukraine). Russian cyber actors often use techniques such as phishing emails, malware, and other types of cyber intrusion to infiltrate South Korean networks.

Threats to the United States

The United States has also been targeted by North Korea, China, and Russia. Given these threats, both Washington and Seoul share a strong interest in countering these cyber operations to protect their infrastructure and impede Pyongyang's nuclear weapons program. Despite the real threat from North Korea, however, China poses the greatest cyber threat to the United States. China leads the world in espionage-related hacking against the United States. China is also active in other intelligence areas, such as the use of clandestine agents and satellites, but communications espionage is the centerpiece of Beijing's intelligence program. China has had major successes against the United States, most recently with an **operation** commonly known as Salt Typhoon. This is only the latest Chinese cyberattack, and it has affected more than two dozen countries.

Salt Typhoon should not be seen as an isolated incident, but as part of a larger Chinese campaign to systematically exploit global telecommunications networks. An earlier campaign commonly known as Volt Typhoon saw China pre-position malicious code on U.S. critical infrastructure networks. Salt Typhoon may have also been used in pre-positioning malicious code on telecommunications **networks**. Pre-positioning goes **beyond** espionage and is often a precursor to attack.

Additionally, China has constructed a broad global signals intelligence surveillance system, and it appears that the country has a comprehensive **strategy** for cyber espionage and communications intelligence. Its initial focus was on commercial and technological espionage, as well as conventional politico-military spying. In the last decade, Beijing has expanded its efforts in both scale and scope to include preparing for disruptive actions against critical infrastructure.

Unfortunately, the international cybersecurity situation is unlikely to improve anytime soon. Defensive measures alone will be inadequate to protect the national interests of both the United States and the ROK. This means that Seoul, working in collaboration with Washington, will need to develop stronger capabilities to support what it **calls** "offensive cyber defense." Attribution is the first step.

Attribution

As stated previously, cyber attribution is the process of tracking and identifying the perpetrator of a cyberattack. Raising specific instances with the state responsible and asking for explanation and cessation is a possible first step, albeit not with North Korea, which has refused to engage with the ROK. However, attribution for diplomatic purposes will be more effective when accompanied by persuasive evidence (and adequacy, discussed later) and when carried out by many nations. Attribution can be done in both private and public engagement.

Cyber attribution is seen as essential by many countries, and the difficulties of attributing cyberattacks are often exaggerated. The demand by political leaders for high accuracy in attribution can constitute a significant burden and can make it difficult to respond to malicious cyber actors. While attribution in cyberspace is challenging due to the ability of opponents to exploit the anonymity it affords, a combination of techniques can allow for accurate attribution. The SCCF does not explicitly outline specific procedures for cyber attribution, but it does provide a framework for cooperation that can support attribution efforts. By sharing intelligence and information, collaborating on investigations, and taking advantage of both countries' technical capabilities, the United States and South Korea can work together to improve their ability to attribute cyberattacks.

CREATING AN ATTRIBUTION FRAMEWORK

Attribution is not primarily a matter of technical capabilities (although a lack of capacity can be an impediment). For international relations, political attribution (a decision by one government to assign responsibility for an act) is more important. Decisions on attribution are primarily political and require a sound foundation in intelligence and analysis; many countries prefer to avoid public attribution, and the current level of information sharing among states is **inadequate** to support a collective approach. Creating a **framework** of technical and factual attribution combined with the political decision to act would be one way to draw attention to the political requirements for action.

States can use the 2015 UN Group of Governmental Experts (GGE) **norms** as a framework for action. Reducing the number, scope, and risk of malicious cyber actions will require mechanisms for cooperation and common understandings of attribution, proportionality, and managing any risk from responsive action. One norm of the UN Open-Ended Working Group (OEWG) **states** that "in case of [information and communication technology (ICT)] incidents, States should consider all relevant information, including the larger context of the event, the challenges of attribution in the ICT environment and the nature and extent of the consequences." The document also notes that attribution

"is a complex undertaking, and a broad range of factors should be considered before establishing the source of an ICT incident." This approach can guide thinking on situational awareness and increased accountability.

DEFINING CREDIBLE ATTRIBUTION

Using legal precedent complicates and confuses the discussion of attribution. Political attribution is in the domain of sovereign states, not the courts. The evidentiary standards are different and incompatible. Most importantly, political attribution by states does not involve identifying the culpable individual beyond a shadow of a doubt. It involves identifying the state responsible for the action, or from whose territory the action originated.

Identifying the responsible state is the central element for decisionmaking in political attribution. Political attribution builds on the responsibility **agreed** upon by all UN member states to observe their commitment to ensure that malicious actions do not emanate from their territory, to cooperate with a victim state when asked for help, and to ensure they take action against the malicious actor. If that malicious actor is unable or unwilling to take action, the victim state is permitted to take action itself (consistent with international law), either collectively or individually.

Credible attribution and proportionality in any response based on that attribution are essential ingredients for a politically acceptable response to malicious cyber action. The factors that states should consider in attributing an attack and in using attribution as a tool to increase accountability and stability in cyberspace include the following:

- precedent (e.g., previous attacks);
- technical indicators (and having best practices such as logging in place before an incident);
- the target (criminals are unlikely to go after military targets);
- probable intent;
- effect (i.e., what data was exfiltrated, what services were disrupted);
- external sources of information (e.g., allies or the private sector); and
- supporting intelligence from human or technical sources.

States can use multilateral, regional, bilateral, and multi-stakeholder platforms to share best practices and information on the attribution of different types of ICT threats and incidents. Coordinated attribution of malicious activity will require better information sharing between partners and, perhaps, new mechanisms for sharing and harmonization. These include evidentiary standards and information-sharing mechanisms for coordination of any collective attribution.

Attribution in the context of accountability is not primarily technical. It is primarily political and requires a sound basis of intelligence for political decisions. However, as stated above, the current level of information sharing among states is inadequate. Creating a framework of technical and factual attribution, combined with the political decision to act, would be beneficial. Other factors help determine the degree of rigor required for attribution, such as whether the attribution is tied to a responding action, or whether the conclusion of an effort at attribution will remain internal or be made public.

> *Attribution in the context of accountability is not primarily technical. It is primarily political and requires a sound basis of intelligence for political decisions.*

It is not necessary to identify the individual responsible for a malicious cyber action. It is only necessary to identify from whose territory the attack emanated. It is, of course, valuable and reassuring to identify the individuals responsible, but this can make the task more difficult and is not necessary for political attribution. The fundamental point is state responsibility for cyber actions taken from their territory. This level of attribution does not satisfy the requirements of a court, but courts have little or no jurisdiction in a conflict between countries.

Two objections to this approach are (1) the risk of "false flag" operations and (2) the need for sufficient evidence to persuade a public audience. The first is overstated. Few false flag operations can withstand scrutiny. And while it may be more satisfying for a public audience to identify an individual culprit, it is no more necessary than identifying the pilot who flies over a border.

The desire for a high degree of certainty in attribution before taking any action reflects exaggerated concerns over the potential risk of escalation and a desire to avoid unintended consequences. It can also cause unnecessary delays. Escalation risk from attribution is also generally overstated—there has been no incident of escalation in the 30-year history of cyberattacks. The risk is manageable using the tools of **diplomacy**.

CHALLENGES TO JOINT ATTRIBUTION

There are several significant challenges in conducting joint cyber attributions. Technical asymmetries create coordination difficulties. The United States and South Korea have different technical capabilities, tools, and methodologies for attribution. While both countries have sophisticated cyber capabilities, their systems and approaches may not always align seamlessly, potentially leading to gaps or inconsistencies in attribution analysis.

Classification and information sharing structures can affect collaboration. Each country has their own national security classification systems and restrictions on sharing sensitive intelligence. This can limit the depth and speed of information exchange needed for comprehensive attribution. Sometimes critical technical indicators or intelligence sources cannot be fully shared due to classification concerns. Different legal structures affect how evidence can be collected and used. The United States and South Korea operate under distinct legal systems with different standards for digital evidence, privacy protections, and admissibility requirements, which complicates efforts to build legally sound attribution cases that would hold up in both jurisdictions.

Political considerations sometimes create divergent priorities. While both countries share concerns about North Korean cyber activities, they may have different diplomatic sensitivities about attributing attacks to other state actors, particularly China. South Korea's geographic proximity and economic ties to China may influence its willingness to publicly attribute attacks.

Operational security risks increase with joint attribution. Coordination between two countries inherently increases the number of people and systems involved, creating more potential points of compromise. This can make it harder to maintain operational security during sensitive attribution investigations. The United States and South Korea might have different timelines and thresholds for when they feel confident enough to make attribution claims. One partner might prefer faster public attribution while the other wants more conclusive evidence before making statements.

As stated previously, attribution is the first step in an offensive cyber response by defenders—the term mentioned in the ROK's 2024 cyber strategy —and involves several considerations that must be carefully weighed. These considerations include navigating the political and legal complications surrounding attribution claims, relying on appropriate evidentiary standards to make credible attributions (standards that differ from those used in courts and the legal system), and determining both the accountability of actors and whether a response is warranted (along with defining what constitutes proportionality). Additionally, organizations must consider their target audience when making attribution claims, and whether that audience is technical, public, political, or diplomatic in nature. There are also important questions about accountability and an appropriate role of and reliance on the private sector in attribution efforts.

Joint attribution requires significant technical resources and personnel from both countries. Differences in available resources or competing national priorities can affect the depth and sustainability of collaborative attribution efforts, and any effort to create accountability. When undertaking joint attribution efforts, there are three key considerations: technical, legal, and political. The mechanics of information sharing pathways need to be formally defined. The underlying intelligence infrastructure also requires joint assessment—including data collection systems, threat intelligence platforms, forensics tools, analytical capabilities, and communication channels—and the levels at which collaboration should occur must all be identified. Organizations must also determine the appropriate degree of transparency and capabilities sharing between the different parties involved in making attribution claims.

Joint attribution would be the gold standard and the foundation for states to implement and create accountability. The United States faces several significant challenges in conducting joint cyber attribution with South Korea, despite the two countries' long alliance and shared security interests. One of the main challenges is the disparate development of technical capacity across the world to conduct the necessary analysis of incidents to determine the culprit. Besides support for technical development, a key consideration is the need for trust and transparency for joint attribution. Given the sensitive nature of the information, governments have been reluctant to share details of their technical attribution capabilities.

Attribution for creating accountability is not the same as attribution required by a court. In international affairs, attribution must provide sufficient information to persuade decision makers and both domestic and global audiences on the source of a malicious cyberattack. An overly legalistic approach cedes advantage to opponents. This is not a criminal proceeding, and it is essential to recognize that political attribution involves assessing the culpability of a state, not an individual. Attribution is difficult, but after decades of hostile action, waiting for more data to justify a response would be irresponsible. The difficulty of attribution should not be an excuse for inaction.

> *Besides support for technical development, a key consideration is the need for trust and transparency for joint attribution. Given the sensitive nature of the information, governments have been reluctant to share details of their technical attribution capabilities.*

Attribution creates the conditions needed to validate an action in response to a malicious cyber act. This does not require identifying the individuals responsible, but rather the state responsible for the attack or for failing to observe its obligations under international law. Credible attribution are essential ingredients for a politically acceptable response to malicious cyber action.

KEY CRITERIA FOR JOINT ATTRIBUTION

The mechanics of information sharing pathways for attribution need to be formally defined for successful joint attribution. The underlying intelligence infrastructure also requires assessment, including data collection systems, threat intelligence platforms, forensics tools, analytical capabilities, and communication channels. Organizations must also determine the appropriate degree of transparency and capabilities sharing between the different parties involved in making attribution claims. Criteria for attribution include the following:

1. identifying the likely violators of South Korean or U.S. sovereignty, judging by their public actions and statements;
2. asking whose strategic interests are served by a cyberattack and violating sovereignty (this can be determined from publicly available information, internal assessments, and consultations with allies and partners);
3. previous incidents pointing to a particular state as the responsible actor;
4. similar or simultaneous violations in other states with attributed sources;
5. allies or friendly nations supplying supporting information;
6. evidence that an incident is part of a larger campaign;
7. technical indicators or other intelligence that points to a perpetrator (e.g., using information from a national source, a commercial firm, or an ally or partner); and
8. accurate past assessments of attribution by the relevant national services.

There is still a tendency in cybersecurity to overvalue technical aspects of attribution. This is not the kind of attribution required by a court of law. There are no judges in cyberspace, impartial or otherwise, and the evidentiary standards required in court are profoundly inappropriate for relations among states. Attribution of the source of a malicious cyber act will remain a national decision and any agreement on collective action must recognize this. A sovereign state has the right to decide who has attacked it. States will not give up that right. Attribution remains the prerogative of states, and a collective response will depend on agreement among states.

Recommendations for an Offensive Cyber Defense

Offensive cyber defense has four elements: adequate attribution capabilities, a menu of proportional responses, a framework for collective action, and the political will to act. It is also useful to find ways to engage in diplomacy with opponents directly (if not always publicly). South Korea has shifted its cybersecurity strategy to offensive cyber defense. This has involved moving from a primarily defensive posture to a more proactive approach in which the country actively seeks to identify and counter cyber threats before they materialize. This method utilizes offensive capabilities to disrupt potential attackers, particularly in response to threats from North Korea.

Offensive cyber defense should have two objectives. The first is to reduce malicious activity by opponents. The second is to create incentives for opponents to come to the negotiating table. At the moment, China, Russia, Iran, and North Korea have no incentives to either stop their attacks or negotiate. It has been a decade since the last serious cyber talks between potential belligerents, and offensive cyber defense works best if it is a central part of a larger diplomatic strategy engaging allies, third countries, and, ideally, opponents. No cyber defense will be adequate against determined, well-resourced, and inventive adversaries.

> *Offensive cyber defense should have two objectives. The first is to reduce malicious activity by opponents. The second is to create incentives for opponents to come to the negotiating table.*

Offensive cyber defense is outlined in South Korea's 2024 National Cybersecurity Strategy, emphasizing the importance of attribution and retaliation against malicious actors. The ROK's Cyber Command plays a central role in this strategy. Established in 2010, the command oversees both defensive and offensive cyber operations. It is tasked with protecting the nation's digital infrastructure, defending against foreign cyberattacks, and, when necessary, executing offensive cyber operations in response to threats.

Offensive cyber defense includes proactive measures designed not only to protect and defend critical systems from cyberattacks—measures that rely on law enforcement or financial actions—but also to deter or neutralize potential threats before they can cause harm. This concept is part of a broader strategy to strengthen the ROK's cybersecurity posture and resilience. Instead of simply waiting for a cyberattack to occur, the ROK can identify threats early and act to prevent or mitigate them. Monitoring cyber activity, identifying vulnerabilities, and responding quickly to malicious actions will all be necessary to preventing cyberattacks. Offensive cyber defense includes the ability to conduct counterattacks on adversary networks, either to disrupt or disable their operations or to prevent further escalation of cyber threats. Examples include hacking back, disrupting the attackers' infrastructure, or causing damage to their systems. Below are four strategies the ROK could consider for its offensive cyber defense:

1. **Coordinate offensive cyber defense operations with key allies, including the United States.** As part of the U.S.-ROK military alliance, the two nations share cyber defense capabilities and intelligence. Joint cyber exercises and information sharing help both nations strengthen their cyber resilience and readiness for offensive operations. The ROK has invested heavily in

building sophisticated cyber tools, which may include malware, denial-of-service capabilities, and other advanced technologies designed to disrupt enemy networks. These tools are used to target adversary infrastructure and provide a strategic advantage in the event of conflict.

2. **Create clear legal frameworks to govern offensive cyber defense actions.** In practice, this involves ensuring that offensive operations do not violate international law or provoke unintended escalations. The ROK has been working to define the rules of engagement in cyberspace, making sure that its actions comply with national laws, international norms, and human rights principles, and this would be useful area for further consultation with Washington. One goal of offensive cyber defense should be to change opponent behavior by creating accountability. Absent accountability and consequences for malicious cyber actions, these will continue to increase and will become increasingly destabilizing. This does not have to involve military action or offensive cyberoperations, although these should not be ruled out. There is no accountability in cyberspace, but accountability has always been difficult for the international community.
3. **Develop both capabilities and a willingness to use them.** Even the United States, which has advanced cyber capabilities, has been reluctant to use the full range of these tools, despite the country's **policies** of active defense and "defend forward." While a few other Western nations are exploring the use of offensive cyber operations to create consequences, these operations have been few and have lacked noticeable effect. One reason for the lack of effect may be that responses tend to be episodic one-offs, rather than a set of sustained campaigns. This points to one central issue for creating accountability: Is this a response to an individual action, as would be the case in a law enforcement approach, or is it a response to a sustained opponent campaign? Policymakers have tried the former without success.
4. **Create a menu of response options and proactive measures.** Instead of solely trying to defend or prevent cyberattacks, South Korea aims to actively disrupt cyber operations by identifying vulnerabilities in potential attackers' infrastructure and taking preemptive actions. International cooperation is key, as South Korea also plans to strengthen collaborations with other countries to enhance its offensive cyber capabilities and intelligence sharing, with a focus on attribution.

Next Steps

The ROK revised its National Cybersecurity Strategy in 2024 as part of its active response to evolving economic, technological, and cybersecurity challenges. This revised strategy, which is aligned with UN Group of Governmental Experts requirements, focuses on transparency in cyber policies while ensuring safety and responsible use of cyberspace. The strategy encompasses three main features: (1) clear identification of cyber threats with a more proactive response approach, (2) reinforcement of the ROK's role as a "**Global Pivotal State**" in international cybersecurity cooperation, and (3) establishment of a comprehensive domestic cybersecurity governance framework.

To implement this strategy effectively, the ROK has outlined four crucial next steps:

1. developing detailed implementation plans;
2. communicating the nation's position clearly to the international community;

3. gathering objective data on partner countries' cybersecurity capabilities; and
4. establishing theoretical and practical foundations for more aggressive strategic approaches.

The United States can play a major role in helping South Korea implement its new cybersecurity strategy by offering technical support, sharing best practices, and fostering bilateral cooperation on cybersecurity issues. Washington can assist Seoul in enhancing its cybersecurity infrastructure by providing expertise in advanced technologies such as AI, machine learning, and threat detection systems. The United States, including U.S. tech companies, can collaborate with South Korean counterparts to implement cutting-edge tools for identifying and mitigating cyber threats from state actors including North Korea, China, and Russia.

The United States can also facilitate information sharing between South Korean and U.S. intelligence agencies. By exchanging threat intelligence data on emerging cyber threats and tactics used by adversaries, both countries can develop a more robust defense posture. The United States also has experience in addressing large-scale cyberattacks, such as those targeting critical infrastructure, which South Korea can learn from to bolster its own national resilience. This can include joint cyber exercises, technical seminars, and internships to help South Korea cultivate skilled professionals capable of handling complex cyber challenges.

A potential research agenda for U.S.-ROK cybersecurity cooperation can focus on several key areas, starting with threat intelligence sharing and analysis. Research questions in this area include how to improve the timeliness and accuracy of threat intelligence—especially regarding emerging risks like AI-powered attacks—and identifying effective mechanisms for joint threat analysis and attribution of cyberattacks from both state and non-state actors.

The next focus is on critical infrastructure protection, particularly in sectors like energy, finance, and transportation. Research could explore how to develop a joint framework for securing these sectors through information sharing, joint exercises, and technology cooperation. Additionally, strategies for enhancing the cybersecurity resilience of emerging technologies such as 5G within critical infrastructure should be examined.

The agenda could also emphasize cyber defense technology cooperation, seeking ways for the United States and ROK to collaborate on cutting-edge cybersecurity technologies including AI for threat detection, blockchain for secure data sharing, and quantum-resistant cryptography. Further, it could call for research on the legal and regulatory frameworks needed to facilitate cross-border technology cooperation while ensuring data privacy and national security. Other areas for possible collaboration include building human resources through joint education and training programs, as well as fostering international cooperation to establish norms for responsible state behavior in cyberspace. ■

Julia V. Brock *is the former program manager and research associate for the Strategic Technologies Program at the Center for Strategic and International Studies (CSIS) in Washington, D.C.* ***James A. Lewis*** *is a non-resident senior adviser in the Economic Security and Technology Department at CSIS.*

This report is made possible through support from the National Security Research Institute of Korea.