MARCH 2026

Active Cyber Defense in the Korean Context

James A. Lewis

The Republic of Korea (ROK) faces a uniquely volatile situation in defending its networks, data, and digital infrastructure. Nuclear-armed North Korea (DPRK), unlike other leading state cyberattackers such as Russia, China, and Iran, poses a direct military threat to the ROK and makes use of missile launches, artillery fire, and (in the past) naval activity to threaten, warn, and manipulate ROK and global opinion. Drawing on one example among many, in January 2024, Kim Yo-jong, the sister of North Korean Supreme Leader Kim Jong-un, threatened an "**immediate military strike**" against South Korea in response to any "**slight provocation**." While there is a considerable degree of bluster in statements like these, the risks of taking retaliatory action against the DPRK is higher than in any other cyber conflict. This shapes any calculation of active cyber defense, defined as taking action against opponents rather than relying on attempting to deny them access to networks and data.

The international landscape for cyber defense is complicated, as all major cyberattackers are currently insulated from punitive responses—particularly from democracies, given their fear of escalation. For the ROK, however, cyber defense against the DPRK adds the risk of armed conflict—unconventional, conventional, even nuclear—to the equation. While this risk should not be exaggerated, it means that while the ROK needs a general cybersecurity strategy focused on resilience, it must also have a strategy specific to the DPRK based on active defense.

South Korea must also navigate an increasingly uncertain and hostile international environment characterized by significant instability. Expanding threats to global order include China and Russia, alongside a dangerously unaccountable DPRK. U.S. retrenchment is another factor that increases risk. This volatile landscape creates difficult challenges for South Korea's defense. Adversaries are increasingly engaging in hostile actions. While these actions have so far not involved direct military confrontation, these risks are compounded by opponent perceptions of U.S. weakness and vacillation. In response to these increasing threats, South Korea is reorienting its defense policy and strengthening alliances.

CSIS | CENTER FOR STRATEGIC & INTERNATIONAL STUDIES

New Approaches to Cybersecurity

A critical component of this strategic evolution reflects a larger rethinking of cybersecurity. The ROK is not alone in doing this. Cybersecurity policy is being reoriented in the United States, Japan, and NATO, and concepts have evolved in ways that reflect the experience of cyber conflict. The primary change is that the emphasis on deterrence and defense is being replaced by a new focus on resilience and active defense. This is because hostile actors have not been deterred in cyberspace and defenses are too easily circumvented. New approaches to cybersecurity center on resilience—which assumes that, despite a degree of unpreventable initial success by attackers, defenders can continue providing a sufficient level of key services and recover quickly—and on active defense, which entails the use of coercive means to degrade opponent capabilities, operations, and benefits. Intelligence and espionage underpin active cyber defense.

Cybersecurity is now an integral component of national defense requirements, supported by expanded foreign intelligence gathering using cyber espionage, signals intelligence (SIGINT), human espionage, and open-source intelligence (publicly available information). While the opportunities provided by open-source collection are limited for the DPRK, it can still offer valuable insights.

Deterrence Requires Credible Threats

Cyber deterrence still has some appeal, if only because it allows governments to avoid the risk of taking action against an attacker. Deterrence reflects a defensive and passive orientation, and ultimately a desire to avoid conflict. It appealed to a cyber community more familiar with technical measures than with strategy, and to a strategic community unfamiliar with digital conflict and too oriented toward precedents from nuclear strategy. Whatever merits this defensive orientation may have had in the past, it is no longer adequate for an environment of increasing malicious cyber activity as Russia, China, North Korea, and Iran become more aggressive in cyberspace. Deterrence still makes sense as an ultimate goal, once democracies develop credible threats of punishment for malicious cyber actions, but it is inadequate until that occurs. For now, a failure to take action only encourages opponents.

The chief weakness of cyber deterrence is the lack of credible threat that would lead an attacker to recalculate benefit and risk and decide to forgo action. The DPRK is in many ways shielded from the punitive responses that democratic nations have tried so far, such as sanctions, public announcements, and law enforcement actions. The utility of sanctions in changing cyberattacker behavior is doubtful, since the DPRK already faces an intense and encompassing sanctions regime, which its leaders shrug off as inconsequential. Sanctions and "**name-and-shame**" announcements have little effect against the DPRK. Reactive law enforcement actions can disrupt attacker networks and reduce the DPRK's gains from illicit cyber action, but do not diminish the capabilities of determined opponents. An active cyber defense policy that disrupts opponent cyber operations can provide greater protection.

Elements of Active Cyber Defense

In response to the worsening situation in cybersecurity (itself a reflection of a deteriorating international security situation), a number of countries are considering adopting or have adopted policies for active cyber defense. These responses need not be confined to cyber actions and may involve diplomatic measures, law enforcement tools, and the full range of coercive instruments available to states. Active cyber defense involves both deciding on an appropriate response for a

malicious cyber action and developing adequate offensive capabilities to impose penalties. It requires more than retaliation for a specific incident, and it can use preemptive actions to prevent a cyberattack by damaging an opponent's cyber capabilities.

Active cyber defense reflects a larger adjustment by democratic nations to an increasingly hostile environment. This new environment will require significantly expanded military and intelligence capabilities, including the development of cyber offense capabilities. Active defense builds on expanded intelligence and military cyber capabilities and requires new strategies that comprise, in addition to coercive actions, coordination with allies and partners, an "all-of-government" (i.e., all pertinent ministries, not just those whose primary focus is national security) approach that combines cyber, law enforcement, financial and diplomatic tools, and designing a public narrative to accompany and explain active defense.

Active cyber defense is still ultimately defensive, as the intent is not to conquer or defeat the attacker but to reduce their ability to inflict harm and to benefit from malicious cyber action. Active cyber defense is unlikely to change an opponent's behavior (and will not deter them from malicious cyber actions), but it can disrupt their operations, degrade the returns from their cyber actions, and damage their attack capabilities. To be effective, active cyber defense cannot be limited strictly to actions in the cyber domain. It must go beyond "hacker versus hacker" and reach other key interests of the attacker, such as disrupting financial gain from hacking.

Offensive operations are only one tool among the several that are available. The fundamental elements of active cyber defense are attribution, identification of opponent targets and vulnerabilities, a menu of proportional responses, offensive cyber capabilities integrated with law enforcement and countering financial crime, a framework for collective action with other states, and the political will to act. The ROK, in adopting a policy of active cyber defense, will need to create a menu of response options derived from its capabilities that are both effective and consistent with the rules, norms, and standards governing relations between sovereign states.

Active cyber defense includes offensive cyber capabilities, which involve the ability to infiltrate another state's networks to collect information and, perhaps, to disrupt them. These actions can be preemptive, accessing and neutralizing attacker infrastructure (like command-and-control nodes or attack tools) before they are used in an attack. The ROK and its allies could consider proactive measures that involve action on the opponents' networks to disrupt attacks. While this could create the risk of retaliation or escalation of conflict, it is less risky than the increasingly dangerous cyberattacks carried out by major state opponents.

Additionally, a sophisticated diplomatic strategy is essential for engaging allies and opponents alike to manage the implications of this more active stance. Building active cyber defense on a national basis and in alliance with the United States and other partners requires the ROK to take a number of steps based on the political decision to engage in it. Active cyber defense uses the tools and levers available to states in international relations to counter transgression. Active cyber defense can be limited to those actions that do not violate sovereignty if they rely primarily on law enforcement and diplomatic measures. An initial effort may begin with these limited measures to assess risk, opponent reaction, and effectiveness and begin to build a kind of escalation ladder for responses.

EXTRATERRITORIAL ACTIONS

Extraterritoriality and sovereignty will affect decisions on active cyber defense by delineating the legal authorities required for operations. Active cyber defense could be limited to networks within the jurisdiction of the ROK, or extend to allied networks with their consent. This avoids the complication created by violating the sovereignty of the DPRK or other opponents. Active cyber defense at a minimum will require the ROK to monitor cross-border internet communications to detect signs of cyberattacks, while explicitly following privacy protections and constitutional principles.

The most difficult issue for policymakers involves preemptive cyber actions taken extraterritorially—deciding when it is justified to violate an opponent's sovereignty. Active cyber defense can require preemptive actions taken to prevent and neutralize a potential cyber threat before it can be executed by an opponent. By its nature, this means that active cyber defense can involve a violation of the opposing nation's sovereignty. Preemptive action also creates new requirements for sharing intelligence to deconflict and coordinate active cyber defense. In cases where active defense employs cyberattacks, it also creates an obligation to ensure compliance with international humanitarian law, specifically the requirements of the law of armed conflict regarding distinction and proportionality.

PROPORTIONALITY

Proportionality is one of the most important requirements of the law of armed conflict for active cyber defense. There has been discussion as to whether the proportionality of a response is determined by an individual incident or by a larger malicious cyber campaign, with the discussion moving in the direction of taking the cumulative effect of a cyberattack into account when considering proportionality. For active cyber defense to be most effective in reducing risk, it must be the latter. Active defense should not be based on tit-for-tat responses or limited to reactive actions.

Proportionality does not mean that the force used by each side must be equal. Instead, it requires balancing the necessity for effective action and the requirements of humanitarian protections. The **Geneva Conventions** define a proportional response as one that is not "excessive in relation to the concrete and direct military advantage anticipated." For active cyber defense, this includes actions that directly target those elements that contribute to an opponent's cyber capabilities while posing limited risk of collateral damage to civilian targets. This is a more forward-leaning approach, but it is necessary if active defense is to be effective. The requirement to observe proportionality does not forbid all civilian harm, and proportionality requirements can be met by better intelligence that allows for precise targeting.

Attacking DPRK critical infrastructure is probably of limited utility. The DPRK's leadership is not overly concerned with citizen well-being, and in any case, its critical infrastructure is already limited in its capacity to deliver services and poses less risk given the underdevelopment of the DPRK economy. For example, turning off power to a DPRK facility used for cyberattacks is less likely to affect civilian entities like hospitals, since they are unlikely to depend on the same power source.

However, actions against the DPRK's command-and-control hacking infrastructure and its financial networks could reduce its ability to do harm, and degrading them is a legitimate goal for active cyber defense. Identifying pressure points in the DPRK is essential for active cyber defense. Since it is

unrealistic to expect to change DRPK behavior, the goal for active cyber defense should be to erode DPRK cyber capabilities and reduce their financial returns.

ATTRIBUTION

Attribution is necessary to impose consequences and perhaps ultimately create accountability. Adequate attribution is needed to ensure effectiveness, provide justification for an action to the international community, and to convince political leaders of the need for action. This is not the attribution required by a court, but what is sufficient to persuade decisionmakers that a campaign of response to malicious cyber actions is justified. It first requires identifying the nation responsible for an attack. This requires a careful calculation of what actions will be seen as both justifiable and effective. An **earlier paper** in this series discusses the requirements for attribution.

Attribution can be defined as determining the identity of an attacker. It is primarily an intelligence task. A 2022 report on UN cyberspace norms **notes that** attribution "is a complex undertaking, and a broad range of factors should be considered before establishing the source of an ICT [information and communications technology] incident." Norm 13(b) (proposed by Russia) of the 2015 report of the UN Group of Governmental Experts, the precedent for global cyber norms, **states that** "In case of 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 ability to attribute the source of an attack is critical for increasing accountability in cyberspace and giving meaning to international law and agreed norms. This concept is repeated and expanded in the 2024 **Open-ended Working Group** agreement agreed to by all member states.

The desire for a high degree of certainty in attribution before taking any action reflects concerns over the potential risks of active defense and a desire to avoid unintended consequences. The risk of escalation is overstated—there has been no **incident of escalation** in the 30-year history of cyberattacks. Escalation risk is manageable using the tools of diplomacy. The second risk is more complicated. Deciding how to act upon attribution is a political decision. Active defense is bound by both strategic implications of any action and by the ROK's commitment to international humanitarian law. Policymakers will need common understandings on the degree of certainty needed for attribution of responsibility.

The fact that the DPRK has an authoritarian mode of government does provide a benefit of sorts. First, the risk of "collateral damage" from any ROK active defense measure is lower, as DPRK assets are owned by the state. Second, the threshold for attribution of the source of an attack is much lower when the DPRK is involved. This certainty provides a greater freedom of action for the ROK and others. The North Korean state exercises very tight control over all online activities, including hacking. It can be safely assumed that no cyber action will be undertaken without its approval and involvement. There are no independent cyber actors in the DPRK or its agents deployed overseas. Once the initial question as to whether the source of an attack is North Korea is answered, more specific attribution is unnecessary for active cyber defense.

RESPONSE THRESHOLDS AND FORCE

Active cyber defense need not cross one of the most important thresholds in cybersecurity: the use of force. The emerging consensus is that an attack in cyberspace qualifies as a use of force when it

produces effects equivalent to those of a kinetic armed attack, such as casualties, physical destruction, and the unacceptable disruption of data and services. There is a gray area in deciding when the disruption of services and data rises to a level of damage or destruction equivalent to the use of force, but the simplest approach is to reason by analogy and ask whether the cyber incident creates damage equal to a kinetic attack.

This definition sets a clear threshold. Most malicious actions in cyberspace have involved crime or espionage, not force. This has been a ceiling below which malicious actors in cyber conflict have been content to remain. However, as economic losses from cybercrime and cyber espionage continue to mount unabated, and as the risk of the use of cyberattacks to create harm and damage continues to grow, a forceful response by the victim state is increasingly seen as necessary.

Initially, there was speculation, such as in the 2012–2014 works of **Panetta**, **Lin**, and **Singer and Friedman**, that as states made greater use of offensive cyber operations, there could be escalation to a larger and more damaging conflict. This has not proven to be the case. In more than two decades of malicious cyber action, there has never been an incident that has led to escalation. The likely reason for this is that for attacker nations, cyber operations are part of their larger strategies of avoiding direct military conflict while pursuing their strategic objective by using unconventional means.

Instead, an implicitly observed threshold derived from the use of force determines escalation risk. No cyber action has led to casualties and only a few have led to physical destruction. Financial harm, of which there has been a significant amount, has not triggered a forceful response. Active defense measures that do not cross the use-of-force threshold pose a much lower risk of escalation.

Escalation is managed by not crossing this use-of-force threshold, and through direct and indirect communications with the opponent. A communications strategy requires deciding what and when to tell opponents, allies, and the public, and how to tell them. The goal is to shape opponent perception and calculation of risk since it cannot be assumed that opponents infer intent from actions, and actions that escape notice have no effect.

COUNTERMEASURES AND RETORSION

In international law, countermeasures and retorsion are ways for a state to respond to the unfriendly or illegal acts of another state. An act of retorsion in international law is a measure taken by one state in response to an unfriendly or adverse act by another state. The act itself does not violate international law or customary law, even if the initial act it is responding to was either unfriendly or illegal. Retorsion thus refers to actions that are harmful to another state but are inherently lawful. Because no international laws are being broken, a state is generally free to use retorsion at any time, whether to express political displeasure or respond to a cyber incident. Examples include expelling diplomats or imposing economic sanctions. Retorsion does not require a state to prove an "**internationally wrongful act**" or meet the high legal standard needed for courts.

Countermeasures are more severe. These are actions that would normally be illegal under international law (e.g., hacking another state's networks) but become legally permissible because they are a direct response to a prior "internationally wrongful act." The response must be temporary and proportional to the injury suffered. A state cannot destroy a power grid in response to a website defacement.

Countermeasures require that the target experiences pain or loss. Countermeasures (or reprisals) involve a temporary, justified breach of international law to bring an unlawful state act to an end.

Countermeasures are more likely to be effective against the DPRK than retorsive acts. Effectiveness requires identifying those places where the DPRK has something to lose, not to deter it, but to limit its ability to do further harm. This suggests that the initial targets for coercive countermeasures should be financial. Neutralizing the attacker's resources used to fund hacking operations also reduces the cyber threat. This can include seizing cryptocurrency funds tied to ransomware payments or other illegal activities. Sanctioning entities and individuals involved in the cyber campaign makes it difficult for them to transact globally. Taking down the attacker's phishing and malware delivery domains, along with supporting botnets or proxy networks used to launch cyber actions, can reduce the scale and lessen the anonymity of attacks. While the immediate goal is to impose costs for malicious cyber action, developing neutralizing capabilities can be seen as a step in developing what can be called "cyber superiority" (crippling an opponent's cyber forces and defenders in a conflict, similar to air superiority in traditional warfare) in an actual war.

Superiority in active cyber defense strategy requires degrading attacker command-and-control infrastructure used by the attacker to communicate with their malware installed on the victim's network. This infrastructure is the nervous system for cyberattacks. Disrupting this infrastructure may produce an immediate halt to an ongoing attack and limit an attacker's ability to operate. The infrastructure can include servers (often compromised or rented) in third countries, raising extraterritoriality concerns that may require diplomatic action to address.

An attacker's assets also include the sophisticated, proprietary tools and exploits they have built. These are expensive to develop and maintain. They are also legitimate targets. Neutralizing or disrupting these capabilities inflicts a high cost. Analyzing the attacker's tools to create detection signatures and sharing the information with allies, software vendors, and service providers will force the attacker to invest significant time and money to develop new tools.

Diplomatic Aspects of Active Cyber Defense

Active cyber defense requires and can be strengthened by a robust diplomatic strategy. This involves the following:

- coordinating and ensuring deconfliction at an operational level;
- engaging with national, allied, third country, and even opponent audiences;
- developing and implementing appropriate policy, diplomatic and legal frameworks, and agreements for cooperation; and
- deciding the degree and timing of acknowledgment of active defense actions.

Multilateral coordination is absolutely essential for many active defense measures. Measures like sanctions, public announcements, and many disruptive actions can be amplified by the involvement and participation of like-minded nations. More importantly, disruptive measures need to be accompanied by steps to ensure deconfliction to reduce the risk of inadvertent interference with an operation by a friendly nation.

One benefit of the **Five Eyes** intelligence partnership is that it provides a ready mechanism for coordination among partners. Like-minded nations in Asia are not yet at the point where they could agree to a Five Eyes–style approach involving the United States, South Korea, Australia, and Japan, but existing bilateral channels can be used to coordinate and obtain support.

The disruption of cryptocurrency, money laundering, and the covert financial infrastructure that supports DPRK cyber activities is an important element of active cyber defense and requires multilateral cooperation. (And in some areas, China might be willing to cooperate.) This can be achieved by utilizing and expanding existing bilateral and multilateral efforts, such as Interpol, the Financial Action Task Force, and the **Egmont Group** of financial intelligence units.

One crucial question for policy is whether and when to inform opponents. Not informing them of responsibility for an action may be preferable in some instances, but there will also be instances where signaling an opponent serves to establish redlines and perhaps may ultimately lead to negotiations. Communicating with opponents may at first seem counterintuitive, and it can be achieved indirectly through press leaks and other mechanisms, but active cyber defense is improved by increasing opponent uncertainty about the rewards and consequences of a cyber action.

Russia is unlikely to cooperate in any cybersecurity effort, but there may be more opportunity with China, and a diplomatic strategy should include approaching China. China is increasingly concerned with ransomware and cybercrime, and it is not always supportive of DPRK activities. China tolerates DPRK hacking activities in its territory and, at a minimum, should be asked to take action against DPRK hackers and infrastructure. While China may reject such a request or demand too high a price to accept it, putting China on notice is an essential step and could be done through expanded cooperation with allies and friends, likely Australia and Japan.

China does not appear to assist the DPRK in its malicious cyber activities, although it tolerates them. That said, China is increasingly concerned about cybercrime against Chinese companies and may be willing to discuss measures to reduce cybercrime against commercial entities. Such discussions risk, however, becoming entangled in the larger China-ROK relations and China's expectations of deference. China is a major source of espionage against the ROK. Developing a common approach to China will take time and political-level discussion that goes beyond cybersecurity.

The goal for diplomacy with allies and partners is to achieve a common situational awareness in cyberspace through information sharing, enabling partner nations act on threats. Building shared situational awareness is fundamentally a political challenge. Sharing data may require formal agreements to ensure compliance with ROK law. Both the ROK and the United States will benefit if they can agree on a **Cyberattack Severity Classification Framework** and joint rules of engagement to make coordination easier. The ROK may also benefit from creating liability protections for private sector data sharing similar to the U.S. Cybersecurity Information Sharing Act.

The degree of government cooperation and the timing of coordination efforts also require political-level decisions: Are allies and partners informed of an action in advance, at its onset, or afterward? Existing intelligence, military, law enforcement, and diplomatic channels can be used to facilitate this coordination. Prior agreement on consultations (building on existing agreements) is better than ad hoc notifications and can be built as additions to existing coordination mechanisms.

ALLIES AND PARTNERS

Active cyber defense can be seen as part of a larger shift in defense policy. It treats cyber operations as part of a more robust and comprehensive defense strategy. This proactive approach allows for the preemption of attacks, though this will require the careful integration of new technologies and strict management of escalation risks. To be most effective, this strategy relies heavily on coordination with allies to maintain a common approach to addressing cyberattacks.

The U.S.-ROK alliance has made cybersecurity and information sharing a core pillar of cooperation. Overall, the effectiveness of existing cooperation mechanisms is improving, driven by shared threat perceptions and high-level commitments. Cooperation is based on a tiered structure, from the strategic to the operational.

Coordinated attribution of malicious activity will require better information sharing between partners and, perhaps, new mechanisms for sharing and harmonization of policies. Additionally, creating a framework of technical and factual attribution would help frame the development of active cyber defense actions intended to disrupt opponent cyberattack capabilities. Even with this, however, attribution and proportionality remain sovereign decisions.

INTELLIGENCE SHARING

Active cyber defense blends law enforcement, military, and intelligence activities. Intelligence coordination is essential, if only because the ROK's major opponents rely heavily on their intelligence services—Russia's Main Intelligence Directorate (still referred to as the GRU) and Federal Security Service (FSB), China's Ministry of State Security and People's Liberation Army, and Iran's Islamic Revolutionary Guard Corps—to undertake hostile cyber actions. Decisions on appropriate responses to cyberattacks raise the issue of how to incorporate offensive cyber into national and alliance military doctrine. One such issue for active cyber defense comes from the differing capabilities of the partners. Another is the dilemma of sharing sensitive information. Finally, as discussed later, some active cyber activities may be covert. While the goals of a larger diplomatic strategy can be established, the implementation of that strategy will need to be dynamic and evolve with opponents' reactions.

Law enforcement actions may have greater effect if they target the DPRK's financial operations. The primary incentive for DPRK hacking is financial gain, especially through cryptocurrency, given its anonymity and ease of transfer. North Korea uses cyber-enabled theft, money laundering, extortion campaigns, and crypto theft to fund projects. Crypto thefts often occur from exchanges and wallets where users keep their coins, using a combination of tactics including phishing and malware to gain access. Interdiction (when possible) of the DPRK's fraudulent IT workers and those who enable their remote activities would also damage North Korea's cyber operations.

This makes active cyber defense primarily an intelligence battle. The DPRK's hacking initiatives are orchestrated by the Reconnaissance General Bureau (recently expanded and renamed the Reconnaissance Information General Bureau), North Korea's intelligence agency, with **reportedly** at least 6,000 cyber operatives (organized as "Bureau 121") carrying out operations against banks and cryptocurrency exchanges in at least 17 countries. North Korea funnels funds from cybercrimes to its weapons of mass destruction programs. **Cryptocurrency exchanges** are a favored target for North Korea, **since they allow the DPRK** "to generate income in ways that are harder to trace and subject to

less government oversight and regulation than the traditional banking sector." Ransomware is another preferred DPRK tool. The use of cryptocurrencies and ransomware has become a central element of DPRK cybercrime operations.

Recommended Policy and Operational Measures

The requirements for a new and more effective approach to cybersecurity for the ROK can be summarized as follows:

Legal and Policy Framework

- Develop or revise legal authorities and policies, consistent with international humanitarian law and emphasizing retorsion and countermeasures.
- Define legal authorities required for extraterritorial operations.
- Establish a framework for determining responses, based on the cumulative effect of cyber campaigns rather than isolated incidents.

Intelligence and Attribution

- Expand national intelligence capabilities for cyber espionage using SIGINT, imagery, open-source intelligence, and human intelligence (HUMINT).
- Define the parameters of the "degree of certainty" required for political leaders to authorize action (and avoid court-style evidentiary requirements).
- Map the DPRK's "pressure points," including command-and-control nodes and financial networks.
- Create a shared intelligence pool with the United States and other allies to deconflict ongoing operations.

Operational Capabilities

- Develop and maintain tools to infiltrate and neutralize attacker infrastructure before attacks are launched (preemption). The U.S. Cyber Command's 2018 Joint Task Force ARES is a precedent.
- Expand capabilities to seize cryptocurrency and disrupt illicit money laundering networks.
- Establish mechanisms to share with private sector partners and create legal safeguards for the private sector to share data with the government.

Diplomatic Coordination

- Coordinate with allies and regional partners (e.g., Australia and Japan) for "name-and-shame" campaigns, economic penalties, and, in some cases, offensive operations.
- Strengthen ROK-U.S. joint rules of engagement and create a severity classification framework.
- Design a strategic communication plan to explain and justify active defense measures to the global community.

Conclusion

Successfully implementing the requirements for active cyber defense depends on sustained political will to take new risks. The ROK can set a precedent for future security policy by endorsing active cyber defense and, if implemented effectively, it can reduce losses from DPRK cyber actions. Active cyber defense is not an all-or-nothing proposition, and the legal and policy foundations can be laid and actual implementation carried out on an incremental basis to accommodate political perception of risk.

Will this stop the DPRK or other malicious cyber actors? Not at all. The profits from hacking are too important for Pyongyang to give them up. Russia, the DPRK, and China are hostile to democracies. But active cyber defense can reduce the harm and cost of malicious cyber action. ■

James A. Lewis *is a non-resident senior adviser in the Economic Security and Technology Department at the Center for Strategic and International Studies in Washington, D.C.*

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