MARCH 2026

South Korea's Integrated Cyber Defense Framework

Active Cyber Defense and Reactive Responses

By Sunha Bae

Introduction

Cyberspace is structurally favorable to attackers. There is little cost when they fail and significant gains when they succeed. As a result, traditional deterrence is difficult to achieve in cyberspace, and the imbalance between the risks and rewards of cyberattacks persists. For this reason, **international policy** and **research** have emphasized approaches that make an attacker's calculus less advantageous, generally though strategies that reduce the cost-effectiveness of conducting cyber operations.

The structural advantage that cyberspace provides to attackers affects many states. North Korea, in particular, uses cyber warfare as a core component of its military strategy, persistently engaging in large-scale cryptocurrency theft, exfiltration of defense technology and state secrets, and attempts to disrupt critical infrastructure. In the first half of 2025 alone, North Korean hackers allegedly stole approximately $1.6 billion in cryptocurrency—around **70 percent** of global cryptocurrency theft during that period. Moreover, illicit cyber activities now account for roughly **30 percent** of North Korea's foreign currency earnings and, aside from weapons sales to Russia, constitute its primary source of external revenue—funds that directly support its military buildup.

For South Korea, North Korea's cyber activities represent a core threat to national security and economic stability, extending beyond espionage and illicit financial gain. At the same time, **China** conducts extensive cyber espionage campaigns that target strategic industries such as semiconductors, batteries, and telecommunications, while **Russia** has expanded cyber activities against South Korea alongside deepening political, military, and economic cooperation with North Korea. Emerging threats—including ransomware operations, supply chain intrusions, and AI-driven automated attacks—further underscore the limits of South Korea's traditional posture of passive defense.

CSIS | CENTER FOR STRATEGIC & INTERNATIONAL STUDIES

Although the South Korean government has repeatedly attributed and condemned North Korea's cyber activities, meaningful cost-imposing responses remain limited. Attributing attacks without follow-on measures raises doubts about the state's capacity and erodes the credibility of its deterrent posture. As former U.S. National Intelligence Officer for Cyber Issues Sean Kanuck **noted during a visit to Singapore in 2016**, once the U.S. government formally accused Russia of interfering in the election, it needed to act. Inaction after attribution creates a negative precedent—undermining both retaliatory threats and the credibility of cyber capabilities. The United States responded with diplomatic expulsions, **economic sanctions** on Russian intelligence agencies and affiliated individuals and entities, and, later, disruption of the Internet Research Agency (IRA) network ahead of the United States' 2018 midterm elections. Although these measures did not fully deter or halt Russia's election interference efforts, they helped prevent doubts about the integrity of the 2018 midterm results and heightened domestic and international awareness of election security. Moreover, they contributed to a broader trend in which democracies such as the United Kingdom, Canada, and Taiwan began publicly disclosing and responding to foreign interference in their own elections.

Repeatedly attributing a wide range of cyber incidents primarily to North Korea raises questions about analytical objectivity, particularly in cases where the involvement of other state or non-state actors cannot be entirely excluded. In such circumstances, attribution risks becoming a declaratory act rather than a credible instrument of statecraft. Without tangible follow-on measures, it may instead signal tolerance for continued malicious activity. South Korea therefore needs a more comprehensive and integrated defense framework to address recurring cyber threats. In this context, the concept of active cyber defense (ACD) becomes relevant.

A 2025 CSIS white paper, "**Forging Forward: South Korea's Proactive Cyber Defense and Strategic Cooperation with the United States**," focused on proactive cyber defense, emphasizing the need to detect, disrupt, and block threats before attacks occur. That paper highlighted the limitations of South Korea's traditionally passive posture and underscored the need for a more forward-leaning cyber strategy.

Building on that foundation, this study puts forth an Integrated Cyber Defense Framework that combines ACD with reactive response measures. ACD refers to proactive disruption and persistent engagement as a mode of direct cyber intervention, while reactive response measures encompass sanctions, law enforcement, diplomacy, and technical actions. The proposed Integrated Cyber Defense Framework aims to establish a defense model tailored to South Korea's strategic environment and recommend improvements in institutional foundations, governance, and cooperative structures that will be necessary to implement such an approach.

Conceptualizing South Korea's Integrated Cyber Defense Framework

ACD RESEARCH TRENDS AND CHARACTERISTICS

Before defining the Integrated Cyber Defense Framework, it is necessary to examine how ACD has been defined in existing research and policy discourse. As the most conceptually contested component of the framework, ACD warrants particular attention.

ACD originated from the military concept of active defense and has been subsequently adapted to the cyber domain, with the United States playing a leading role in its early conceptualization at both the

military and policy levels. In the 2011 **Strategy for Operating in Cyberspace**, the U.S. Department of Defense (DOD) formally defined ACD as "synchronized, real-time capability to discover, detect, analyze, and mitigate threats and vulnerabilities." This definition framed ACD as an operational capability distinct from static or purely preventive defense, and it was later reflected in **U.S. Cyberspace Operations Doctrine**, in which ACD was explicitly distinguished from passive cyber defense.

Despite this early institutionalization in U.S. doctrine, the scope of ACD has remained contested. Some scholars define ACD as a **counterpart to passive defense**, encompassing both internal mitigation and actions conducted beyond the defender's own network. Others focus instead on the direct and persistent mode of **intervention**, emphasizing deliberate and direct defensive actions that **disrupt or constrain** adversary operations and shape behavior below the threshold of armed conflict. Another line of analysis situates **ACD in the gray zone** between passive defense and offensive cyber operations. More expansive approaches conceptualize ACD as an overarching framework integrating **reactive, heuristic, and proactive modes** of cyber defense. As a result, ACD lacks a stable and universally accepted definition.

Nevertheless, across these varying interpretations, a common feature emerges: ACD entails an intervention-oriented posture that seeks to dismantle or disrupt threats, rather than merely aiming to strengthen defensive measures or allow attacks to be endured. In this sense, the distinctive feature of ACD lies in its emphasis on deliberate actions that directly shape or constrain an adversary's operations, distinguishing it from traditional passive defense.

Defining an Integrated Cyber Defense Framework for South Korea

Building on this conceptual clarification, this report proposes an Integrated Cyber Defense Framework to structure South Korea's national cyber response around two complementary components: ACD and reactive response. The distinction between these components is not based simply on whether an attack has occurred, but on differences in purpose and mode of intervention. All activities within this proposed framework remain firmly within the domain of defense, not offense.

- Active cyber defense aims to identify, disrupt, and dismantle threats. ACD includes internal measures such as threat hunting, vulnerability mitigation, and honeypot operations, but it also includes external measures such as the disruption of adversary infrastructure and the use of persistent engagement or international coordination to detect and constrain malicious activities.
- Reactive response seeks to minimize damage after an incident, strengthen resilience, and impose consequences on the attacker. It includes detection, recovery, resilience enhancement, sanctions, law enforcement actions, diplomacy, and technical measures to impose costs.

The objective of this framework is to establish a national defense posture in which threats are actively constrained and disrupted while losses are minimized and consequences are imposed on malicious actors. Within this context, the term "offensive," used in South Korea's 2024 **National Cybersecurity Strategy**, is prone to misunderstanding and may be read to imply operations that exceed defensive intent. Likewise, "proactive" alone does not adequately capture the full spectrum of measures needed. Accordingly, within this framework, ACD is defined in a focused sense to reduce conceptual ambiguity and clarify its role as a defensive function focused on disrupting or constraining adversary operations.

Trends in Cyber Defense Among Major Countries

UNITED STATES

Strategy and Governance

The United States has established a strategy that combines ACD and reactive response measures for cyber defense. This approach is guided by the objective of disrupting attacks before they occur, imposing costs after attacks, and recovering quickly.

The DOD defines **ACD** as a form of cyber defense that actively detects and blocks malicious activity before it affects U.S. networks and systems. These activities include **disrupting** or dismantling malicious cyber activities at their source, including actions conducted below the threshold of armed conflict. In other words, U.S. policy considers certain offensive cyber operations as part of active defense when their purpose is to preemptively defend against or weaken attacks targeting U.S. interests.

Since 2018, this ACD approach has evolved into a strategy of persistent engagement, which involves continuously countering adversaries across the cyber domain and, when necessary, operating in foreign networks to disrupt or block adversary infrastructure through defend forward and **hunt forward** operations. The 2020 **Cyberspace Solarium Commission** emphasized deterrence by denial through improved defensive capabilities, as well as cost imposition through continuous responses using all instruments of national power, recommending ACD as a core component of this approach. While the 2023 **U.S. National Cybersecurity Strategy** reaffirmed this approach, the Trump administration's 2026 **Cyber Strategy for America** places greater emphasis on imposing costs on adversaries and adopting a more assertive posture toward malicious cyber actors, while emphasizing the active use of both defensive and offensive cyber operations.

The United States' legal and institutional framework supports this approach. The **National Defense Authorization Act** (NDAA) empowers the DOD to take "appropriate and proportional actions" in foreign cyberspace against "active, systematic and ongoing campaigns of attacks" conducted by key adversaries such as Russia, China, Iran, and North Korea. In addition, **National Security Presidential Memorandum 13** (NSPM-13), published in 2018, although not publicly released, is reported to have streamlined decisionmaking for time-sensitive offensive cyber operations, allowing the DOD to respond more quickly to malicious cyber activity. However, significant or sensitive cyber operations still require **coordination** with the White House and relevant departments. The **FY 2019 NDAA** also requires quarterly congressional reporting on the use of cyber weapons and cyber operations, in order to enhance transparency and strengthen congressional oversight.

The organization responsible for planning and conducting ACD operations is U.S. Cyber Command (USCYBERCOM), within the DOD. USCYBERCOM integrates personnel from military services and intelligence agencies to build cyber defense and operational capabilities, organized into cyber operations, cyber defense, and research and development. Moreover, the United States is currently considering establishing a separate **Cyber Force** to ensure that USCYBERCOM secures sufficient professional personnel and resources to execute long-term cyber strategy. These discussions also encompass the need to cultivate and secure cyber-specialized **legal experts** who can support the planning and execution of complex cyber operations.

In terms of reactive response, resilience enhancement and cost imposition are key. Legally, the Federal Bureau of Investigation (FBI) and the Department of Justice (DOJ) criminally indict malicious actors and publicly disclose their identities to limit their operational freedom. Economically, the Department of the Treasury (USDT) freezes the assets of international hacking groups and their enablers and blocks their access to the global financial system. Diplomatically, the Department of State (DOS) and the White House attribute cyberattacks to specific states together with allies and issues joint attribution and public condemnations, linking these with diplomatic sanctions to degrade relations with the attacking state and increase the perpetrators' international isolation. The Cybersecurity and Infrastructure Security Agency (CISA) and the National Security Agency (NSA) conduct incident response, enhance resilience, protect critical infrastructure, and issue security advisories. Through this integrated approach, the United States brings together technical, law-enforcement, diplomatic, and economic measures to impose meaningful costs on malicious actors.

U.S. Cases

The United States is currently the most active country in conducting both active and reactive cyber responses. Beginning in 2018, it has increasingly publicized ACD operations, strategically signaling its tracking capability and willingness to respond. International cooperation with the European Union, **NATO**, and Five Eyes partners has also steadily expanded.

The United States has utilized a range of tools as a part of its response, such as disrupting infrastructure, taking down hacking groups, attributing attacks publicly, issuing security advisories, enacting sanctions, and issuing indictments of internal and external collaborators. A prominent example is the SolarWinds incident in 2020, when the FBI, NSA, CISA, and the Office of the Director of National Intelligence (ODNI) jointly attributed the attack to the Russian government, followed by diplomatic expulsions by the DOS, sanctions by the USDT, and insider trading indictments by the Securities and Exchange Commission (SEC). In the 2024 Volt Typhoon case involving China-linked actors, the FBI, NSA, and CISA jointly identified the threat and issued a security advisory, while the DOJ indicted the hackers and the USDT sanctioned associated companies and individuals. The FBI and CISA also carried out proactive technical measures to identify and block the infrastructure used in the attack. The United States has also undertaken coordinated international operations against non-state actors such as the Hive ransomware group in 2023, resulting in global tracking, system takedowns, and arrests.

Table 1: U.S. Cyber Response Cases

Year	Entities	Response	Type
2016	**White House**, ODNI, DOS, USDT, DHS, FBI, **CYBERCOM**, NSA	Sanctions on related entities and individuals; expulsion of diplomats; joint attribution and condemnation; disruption of internet access for the IRA, Russia's disinformation organization	Active + reactive
2020	**USDT**, DOJ, FBI, **CYBERCOM**, CISA	Temporary disruption of the Russia-based major botnet Trickbot; joint attribution and condemnation; sanctions and indictments	Active
2020	**White House**, ODNI, DOS, **USDT**, DOJ, FBI, NSA, CISA, **SEC**	In response to the SolarWinds supply-chain attack: Senior political intervention through a presidential-level call urging specific actions; official attribution to Russia's SVR, Russia's civilian intelligence agency; expulsion of Russian diplomats; prohibition of Russian sovereign bond issuance in U.S. financial markets; sanctions on related organizations and companies; coordination with the United Kingdom and others	Reactive
2022	**CYBERCOM**	Deployment of a hunt forward team to Ukraine; pre-incident detection and removal of malicious activity on Ukrainian networks	Active
2022	**DOJ**, FBI, **CISA**, NSA	Court-authorized disruption of the Russian GRU-controlled global botnet Cyclops Blink; joint attribution; security advisory; Five Eyes cooperation	Active
2022	DOS, **USDT**, FBI, **CYBERCOM**, **CISA**	In response to cyberattacks on Albanian government agencies: public attribution to Iran's Ministry of Intelligence and Security; security advisory; sanctions; indictments	Reactive
2023	**USDT**, **DOJ**, FBI, CISA	Infiltration of the Hive ransomware group; acquisition of decryption keys; international coordination to seize and shut down Hive servers and websites; sanctions; joint attribution; security advisory; Five Eyes cooperation	Active
2023	**DOJ**, FBI, CYBERCOM, CISA, NSA	International operation to disrupt and eliminate the Russia-based cyber espionage malware, Snake; joint attribution; security advisory; Five Eyes cooperation	Active + reactive
2023	**DOJ**, FBI, CISA	International disruption of Qakbot malware; seizure of approximately $8.6 million in stolen cryptocurrency; indictments	Active + reactive
2024	**DOJ**, **CISA**, NSA	In response to cyberattacks involving the Microsoft Exchange server exploitation: joint attribution; infrastructure takedown; international coordination	Active + reactive
2024	ONCD, **DOJ**, **USDT**, **FBI**, CYBERCOM, **CISA**, NSA	In response to the Volt Typhoon attack: joint attribution; security advisory; disruption of the Chinese botnet used in the attack; indictments and sanctions against APT 31; Five Eyes cooperation	Active + reactive

Source: Author's analysis.

UNITED KINGDOM

Strategy and Governance

The United Kingdom uses the term ACD in a more limited sense than the United States. The United Kingdom has operated an automated defense system, called the **Active Cyber Defence** (ACD) program, since 2016, which is designed not to neutralize adversaries but to prevent and reduce harm from their cyberattacks and strengthen collective defense across the digital ecosystem. The National Cyber Security Centre (NCSC) states that the ACD program aims to contain damage quickly even when serious attacks occur and improve resilience against routine threats.

However, despite differences in terminology, the United Kingdom's cyber response strategy also combines elements of ACD and reactive measures. The strategy includes the ACD program as well as offensive cyber operations. In 2020, the United Kingdom established the **National Cyber Force** (NCF)—a joint organization of Government Communications Headquarters (GCHQ) and the Ministry of Defence (MOD)—to institutionalize cyber operational capabilities. Unlike the NCSC, which provides and leads domestic cyber resilience, the NCF conducts offensive cyber operations against a wide range of targets, including terrorist groups, hostile states, and criminal organizations. In addition, the United Kingdom announced plans in 2025 to establish a separate **Cyber and Electromagnetic (CyberEM) Command**, which handles defensive, cyber, and electronic warfare missions across military and government domains so that the NCF can focus more specifically on offensive and tactical cyber operations.

However, the United Kingdom does not officially classify these activities as part of ACD. Instead, it designates them as offensive cyber operations or counter-cyber operations. While using the term "offensive," the United Kingdom emphasizes transparency and responsible behavior in cyberspace in accordance with domestic and international law. Although the NCF's operations are conducted covertly, the United Kingdom has publicly explained how the NCF conducts cyber operations to signal clearly that the country has both the capability and the willingness to impose costs on adversaries.

Because the NCF is a joint organization between GCHQ and the MOD, it is subject to both the **Intelligence Services Act** (ISA) and defense-related laws and is overseen by political, parliamentary, and judicial mechanisms. Politically, the United Kingdom established ministerial oversight through the ISA, which legally defines the mission of intelligence agencies. The NCF also requires the approval and direction of the prime minister and relevant ministers, reflecting the principle of ministerial responsibility, which prevents the military and intelligence agencies from independently abusing the power to conduct cyberattacks.

Second, parliamentary oversight is exercised through the Intelligence and Security Committee (ISC), which oversees intelligence agencies. Similarly, the NCF reports its activities to the ISC, enabling Parliament to check executive authority and ensure democratic accountability.

Third, judicial oversight is applied to NCF intelligence operations that require investigative powers, which fall under the authority of the **Investigatory Powers Act** (IPA) and the supervision of the Investigatory Powers Commissioner (IPC). The IPA regulates interception, equipment interference, and bulk data collection; such activities require both ministerial authorization and IPC approval. The United Kingdom also stresses responsible, proportionate, and voluntary adherence to international norms in **NCF** operations, reinforcing the legitimacy of its cyber military and intelligence activities domestically and internationally.

In terms of reactive response, the National Crime Agency (NCA) conducts investigations into and prosecutions of cybercriminals through international cooperation. However, the United Kingdom generally prefers practical **sanctions** over symbolic indictments of foreign-based hackers, as the Crown Prosecution Service (CPS) has high evidentiary requirements and the likelihood of arresting foreign cybercriminals is low. To support sanctions, the United Kingdom established a standalone **cyber sanctions regime** in 2020, designating cyberattacks as a separate sanctionable category. This framework allows sanctions not only on individuals residing in the United Kingdom but also on external enablers and service providers, signaling an intention to affect overseas networks.

The **Foreign, Commonwealth & Development Office** (FCDO) attributes cyberattacks to specific states and issues public statements of condemnation, imposing diplomatic costs on responsible states. In recent years, the United Kingdom has actively coordinated attribution and sanctions with the United States. Joint sanctions by the two countries signal to the international community that cybercrime is a global issue and demonstrate that such attacks are traceable, thereby increasing the deterrent effect on malicious actors.

UK CASES

The United Kingdom possesses offensive cyber capabilities and publicly acknowledges their existence, but publicly released examples of offensive cyber operations are extremely limited. The ACD program includes proactively blocking attacks, removing malicious websites in real time, and shutting down harmful infrastructure, referred to as the **Takedown Service**. Between September 2024 and August 2025, the UK government **reports** removing 12,000 cyber campaigns, stopping 26,000 phishing campaigns, detecting and resolving 79 percent of phishing attacks within 24 hours, and mitigating 50 percent of such attacks within one hour. As of August 2025, **sanctions** had been imposed on approximately 70 individuals and nine organizations, in addition to the cases listed in Table 2.

Table 2: U.K. Cyber Response Cases

Year	Entities	Response	Type
2017	**GCHQ**, **MOD**	Cyber operations against ISIS; disruption of the terrorist organization's online activities, equipment, and networks	Active
2023	**FCDO**	Sanctions on 11 Trickbot/Conti ransomware members; asset freezes and travel bans; indictments by the U.S. DOJ	Reactive
2023	**FCDO**, NCSC, NCA	Public condemnation of Russian cyber interference and hacking targeting political and democratic processes; summoning the Russian ambassador; indictments of related individuals	Reactive
2023	**NCA**	Arrested more than 120 individuals affiliated with the Genesis Market operation; international cooperation with the United States and the Netherlands	Reactive
2025	FCDO, **NCSC**	Sanctions on GRU units—Russia's military intelligence agency—and 18 Russian individuals for continued malicious cyber campaigns	Reactive
2025	**NCSC**	Public condemnation of cyber espionage activities targeting critical infrastructure by a Chinese hacking group	Reactive

Source: Author's analysis.

JAPAN

Strategy and Governance

Japan formally introduced the concept of ACD through a **legal amendment** in May 2025, with full implementation scheduled for 2027. The **law** defines ACD as measures that prevent cyberattacks threatening national security and limit their spread by collecting and identifying information prior to an attack and blocking the attacker. It further authorizes administrative interception for ACD purposes, focusing on cross-border data collection based on the recognition that most cyberattacks originate outside Japan. The law also provides for establishment of an **independent oversight body** to review compliance with privacy and communications secrecy protections.

Alongside these legal and institutional changes, Japan has been reorganizing its relevant organizations to support the transition toward ACD. In July 2025, the National Center of Incident Readiness and Strategy for Cybersecurity (NISC) was expanded and reorganized into the **National Cybersecurity Office** (NCO), which was designated as the control center responsible for coordinating and implementing Japan's shift to ACD. In the December 2025 **Cybersecurity Strategy**, Japan referred to ACD for the first time in a strategic document and emphasized the need to impose costs on malicious actors.

Under the NCO's direction and coordination, the Japan Self-Defense Forces (JSDF) and the National Police Agency (NPA) **serve** as operational units, while the Ministry of Foreign Affairs (MOFA) must be consulted in advance when measures involve foreign systems. Approval procedures have been established to ensure that such measures do not exceed what is necessary and are conducted under fair and appropriate processes. In the event of a sophisticated cyberattack on the government or critical infrastructure, the prime minister can designate the incident as a "specified incident" and authorize the JSDF to respond. Outside of emergencies, the JSDF must obtain prior **approval** from the independent telecommunications information oversight commission. But the law does not explicitly clarify whether such operations can be conducted from overseas locations, and Japan has framed ACD as a defensive—not offensive—measure to avoid controversy over potential violations of international law.

Japan is also strengthening the JSDF's capabilities for ACD. The JSDF Cyber Defense Command (JCDC) was established in March 2022 as a direct reporting unit under the Minister of Defense (MOD), integrating cyber personnel from all three JSDF branches. Japan **plans** to expand the specialized JCDC to 4,000 personnel by 2027—up from roughly 530 in 2022. Including information technology (IT) personnel involved in system acquisition and maintenance, the total cyber-related workforce of the JSDF is projected to reach approximately 20,000 personnel.

However, because the law has not yet entered into full effect, there are limited publicly available cases that demonstrate the Japanese government's operational direction. In addition, Japan's **Defense Capability Build-Up Plan**—one of the country's three major national security strategies—focuses primarily on cybersecurity within the MOD, JSDF, and defense industries; early detection and response to threats; and the development of capabilities to disrupt adversary use of cyberspace. In comparison to the United States and United Kingdom, Japan's emphasis is somewhat limited. **Constitutional concerns** regarding privacy and communication secrecy have also led the May 2025 law to impose strong restrictions and independent oversight on ACD measures, which may make the implementation of operational measures more difficult.

In terms of reactive response, Japan has pursued diplomatic measures such as financial sanctions, joint attribution, and publication of security advisories, as well as law enforcement cooperation through joint investigations and indictments. Criminal investigations are primarily led by the NPA, with additional support from the Japan Cybercrime Control Center (JC3). Japan currently maintains a complete **ban on trade** with North Korea and has imposed asset **freezes** on individuals and entities, including hacker groups. Under the **Foreign Exchange and Foreign Trade Act**, ransom payments to sanctioned actors are also prohibited. Financial sanctions are primarily administered by the Ministry of Finance (MOF).

However, toward China, Japan has generally favored joint attribution, security advisories, and diplomatic warnings based on international cooperation, rather than direct sanctions. Although there is no publicly disclosed national procedure for public attribution, the MOFA has broadly led these efforts and has expressed its intention to expand cooperative and national-level attribution activities.

JAPAN CASES

Japan has relied more heavily on reactive responses such as public attribution, indictments, and sanctions. According to a 2023 report by the German think tank Interface, Japan has used public attribution in approximately **six cases** since 2014, primarily using political and technical attribution. While Japan has not taken a leading role in global joint investigations or ACD operations, recent cases show that it has cooperated with the United States and European countries in joint investigations of cybercriminal organizations and infrastructure takedown operations.

Table 3: Japan Cyber Response Cases

Year	Entities	Response	Type
2024	NPA, **MOF**	Public attribution of the theft of approximately ¥48 billion in Bitcoin from the Japanese crypto exchange DMM, identifying the North Korean hacking group Lazarus; calling for G7 cooperation	Reactive
2021	**NPA**	Public attribution of intrusions into Japan Aerospace Exploration Agency (JAXA) and defense industry firms, identifying a Chinese military-linked hacking group; indictment of a Chinese national	Reactive
2023	**MOFA**	Public attribution and sanctions on three North Korean hacking groups and four affiliated individuals by freezing assets	Reactive
2025	NPA, **NCO**	Public attribution of cyberattacks targeting advanced technology and security-related institutions, identifying the China-linked hacking group MirrorFace	Reactive
2025	**JC3**	Public attribution and multinational cooperation with the United States and European partners to dismantle the infrastructure of the Lumma Stealer malware; joint investigation; coordinated infrastructure takedown	Active + reactive

Source: Author's analysis.

AUSTRALIA

Strategy and Governance

Australia is a country that, like the United Kingdom, openly acknowledges and conducts offensive cyber operations. These operations are carried out by the **Australian Signals Directorate** (ASD), the intelligence agency responsible for cybersecurity, offensive cyber operations, and intelligence collection. The ASD has publicly stated that it has these **capabilities**.

Under the **Intelligence Services Act 2001**, which defines the mandate of intelligence agencies, the ASD holds the authority to prevent and disrupt foreign cybercrime. Based on this legal foundation, the ASD conducts operations that disrupt the infrastructure of foreign cybercriminals, including intrusions targeting overseas networks. Although government authorization is required to conduct such operations, the specific orders and approval procedures vary depending on whether the offensive cyber capability is being used to support military operations, assist law enforcement, or deter and respond to cyber threats. These operations are also subject to the ASD's existing legislative and oversight framework, including independent oversight by Australia's **inspector-general of intelligence and security**, thereby ensuring legal legitimacy and accountability. Australia has also announced ongoing **joint operational plans** between the ASD and Australian Federal Police (AFP) for offensive cyber operations, and has emphasized that the Australian government will counterattack criminals and hackers when cyber incidents occur.

Australia is advancing the **Resilience, Effects, Defence, Space, Intelligence, Cyber, Enablers** (REDSPICE) program, which aims to expand and strengthen the ASD's intelligence, offensive, and defensive cyber capabilities. The government plans to invest approximately $10 billion over 10 years. REDSPICE includes plans to triple Australia's current offensive cyber capability; double continuous cyber hunting activities; employ advanced AI, machine learning, and cloud technologies; and expand global operational reach fourfold.

The ASD originated as a defense signals agency and, broadly speaking, functions as an independent entity within the Australian government's Department of Defence. It is not part of the Australian Defence Force (ADF) chain of command, but **reports directly** to the Department of Defence and supports ADF operations. Within the ADF, there are several cyber-related units, including a Cyber Command responsible for operational cyber activities, a **Cyber Operations Division** responsible for the integrated management and security of military cyber and communications infrastructure, and a Space and Cyber Capabilities Division responsible for capability development and acquisition. This close and clearly defined relationship between the ASD and Department of Defence provides a coherent governance structure for conducting offensive cyber operations.

Investigation and judicial responses are led by the **Australian Federal Police** (AFP), which conducts cybercrime investigations, cooperates with state police and international law enforcement, and carries out prosecutions. Sanctions are designated and announced by the Department of Foreign Affairs and Trade (DFAT) with the approval of the attorney general. In the 2025 **Australian Cyber Response Plan** (AUSCYBERPLAN), law enforcement and attribution were designated as official government response activities. Additionally, in 2021, Australia established a significant cyber incident **sanctions** framework, enabling direct sanctions—asset freezes, prohibitions on providing economic resources, and travel bans—against actors responsible for such incidents.

DFAT leads the **Cyber Rapid Assistance for Pacific Incidents and Disasters** (RAPID) team, which can be immediately deployed to Pacific partner countries that experience cyber incidents to assist with recovery and response, thereby extending Australia's cyber response capability beyond its borders.

AUSTRALIA CASES

Australia is one of the few countries that officially acknowledges possessing offensive cyber capabilities, though publicly disclosed cases remain limited. Since the partial disclosure of the ASD's offensive cyber capabilities in support of military operations in **Iraq and Syria in 2016**, most offensive cyber operations have been conducted covertly. However, as a member of the Five Eyes alliance—alongside Canada, New Zealand, the United Kingdom, and the United States—Australia actively engages in international joint investigations and ACD activities.

Although Australia has generally taken a more cautious approach to public attribution than the United States and the United Kingdom, it adopted a more active posture in 2024. DFAT and the ASD's Australian Cyber Security Centre (ACSC) jointly led international cooperation efforts to attribute and issue **security advisories** regarding China's cyber espionage activities. In 2024, DFAT officially designated China as a cyber threat actor, leading to diplomatic friction with the **Chinese embassy**.

Table 4: Australia Cyber Response Cases

Year	Entities	Response	Type
2018	**DFAT**	Joint attribution and condemnation of the cyber espionage activities of China's state-sponsored hacking group APT 10	Reactive
2020	**Department of Defence**, ASD	Disruption and dismantling of cybercriminal infrastructure during the Covid-19 pandemic	Active
2022	**AFP**	Public attribution of a Russia-based cybercriminal group's responsibility for the Medibank data breach; sanctions	Reactive
2023	**AFP**	Disruption of servers of the Russia-linked ransomware group BlackCat; acquisition of decryption keys; international coordination with the United States and Europe	Active
2024	**DFAT**, **AFP**	Sanctions (asset freeze and travel ban) on Russian leaders of the ransomware group LockBit; jointly conducted Operation Cronos with the United Kingdom and United States to dismantle criminal infrastructure	Active + reactive
2024	DFAT, **ACSC**	Leading role in issuing an international security advisory and guidelines on APT 40	Reactive

Source: Author's analysis.

Singapore

STRATEGY AND GOVERNANCE

In the **Singapore Cybersecurity Strategy 2021**, Singapore announced plans to adopt an active approach to risk identification, risk management, and the defense of its networks. However, Singapore's "proactive response" differs from the approaches of the United States and the United Kingdom to ACD; it focuses not on inflicting direct effects on adversaries but on prevention, early detection, information sharing, and regulatory strengthening. Accordingly, Singapore has incorporated a proactive,

preventive approach into its cybersecurity **regulations** and has imposed stricter legal obligations and incident-reporting requirements on critical infrastructure operators.

The Cyber Security Agency (CSA), under the prime minister's office, serves as Singapore's national cybersecurity authority. In October 2025, the CSA established the **Digital Defence Hub** (DDH) under the Centre for Strategic Infocomm Technologies (CSIT), assigning it missions such as threat hunting, malware analysis, and red team exercises to detect and prevent cyber threats before they cause harm. However, these activities remain focused on preventive and defensive measures.

In addition, the Digital and Intelligence Service (DIS) within the Ministry of Defence of Singapore (MINDEF) leads cyber operations, protects the networks of the Singapore Armed Forces (SAF), and contributes to national cyber resilience. For this purpose, MINDEF established the **Defence Cyber Organisation** (DCO). In addition, Singapore announced on March 3, 2025, plans to restructure DIS into a **Defense Cyber Command** (DCCOM) and Digitalisation Command, with the DCCOM expected to enhance cybersecurity and operational capabilities. However, the SAF's cyber capabilities remain primarily oriented toward defensive functions such as network intrusion detection, protection, and recovery. A 2023 **report** by the International Institute for Strategic Studies noted that although Singapore acknowledges the need for offensive cyber capabilities, concrete discussions about their development remain limited.

Singapore, however, places greater emphasis on reactive measures. It hosts INTERPOL's **Innovation Centre** and actively participates in joint international responses to global cybercrime. The **Singapore Police Force** (SPF) leads cybercrime investigations and cooperation with INTERPOL. As a result, Singapore primarily engages in indirect threat removal through participation in international cooperative operations rather than through independent extraterritorial cyber actions. This approach also appears in **Singapore's attribution practices**. Singapore prefers technical attribution over politically charged public accusations against states.

Singapore also works to strengthen cybersecurity capacity across the Association of Southeast Asian Nations (ASEAN) to close regional security gaps and enhance the overall trustworthiness of regional networks. It leads initiatives such as the ASEAN Cyber Capacity Programme (ACCP) and the **Cyber Capabilities and Capacity Project** (C3DP) within INTERPOL, helping build cyber and law enforcement capabilities in neighboring countries. Singapore's foreign minister has **emphasized** that "cybersecurity is only as strong as its weakest link," underscoring the importance of global cooperation to enhance cybersecurity capabilities, particularly in developing countries.

SINGAPORE CASES

Recent cases illustrate Singapore's active participation in law enforcement cooperation with INTERPOL, as well as the country's increasing engagement in joint responses to cyber incidents. In July 2025, Singapore publicly **attributed**—for the first time—a cyber threat actor linked to China. The minister for home affairs accused the actor known as UNC3886, following Mandiant's naming convention, of conducting an advanced persistent threat campaign targeting critical infrastructure in Singapore. However, the country did not directly name China and avoided using labels tied to Chinese government entities such as Volt Typhoon, instead relying on an unnamed cluster group designation to deliver an indirect message. This approach reflects the position of a small country with deep economic, regional,

and geopolitical ties to China—a strategy of condemning malicious activity and asserting sovereignty while minimizing diplomatic conflict or risk of retaliation.

Singapore has also cooperated with **Thailand**, Hong Kong, **Malaysia**, and others in joint operations targeting Southeast Asian cyber fraud networks, resulting in the arrest of perpetrators, takedown of infrastructure, and seizure and freezing of illicit assets.

Table 5: Singapore Cyber Response Cases

Year	Entities	Response	Type
2023	**SPF**	Conducting Operation Synergia with INTERPOL; takedown of servers; arrests of suspects	Active + reactive
2023	**SPF**	Working with INTERPOL to take down a phishing-as-a-service (PhaaS) platform; arrests of suspects	Active + reactive
2024	**CSA**	Participation in internationally coordinated Operation Secure; disruption and disabling of a global botnet infrastructure; neutralization of approximately 2,700 infected devices in Singapore	Active
2025	**MHA**	Public attribution and condemnation of a cyberattack on national critical infrastructure to state-sponsored APT group UNC3886	Reactive
2025	**SPF**	Investigation of the Cambodia-based online fraud group Prince Group; freezing and seizure of approximately SGD 150 million in assets located in Singapore	Reactive

Source: Author's analysis.

Summary and Implications for South Korea

Major countries' cyber defense approaches increasingly extend beyond traditional passive defense to include more active measures for detecting, disrupting, and blocking threats. While national approaches vary, they generally share a common structure that combines elements of ACD with reactive mechanisms.

The United States represents one of the more forward-leaning ACD models. Through the defend forward and hunt forward concepts, the United States conducts ACD operations beyond its own networks to detect and disrupt threats from foreign environments. This approach seeks to reduce an adversary's operational space and shape behavior through persistent engagement in cyberspace. After an attack, agencies such as the FBI, USDT, and DOS coordinate criminal indictments, sanctions, and diplomatic attribution, forming an integrated system of legal, economic, and diplomatic cost imposition. The United States also extends its cyber defense posture into a cooperative framework with allies and partners, emphasizing information sharing and collective defense and deterrence.

The United Kingdom conducts offensive cyber operations through the NCF, a combined entity of the intelligence community and the military, and officially acknowledges using these capabilities on a "daily and routine" basis. The country clearly classifies such actions as offensive cyber operations, while emphasizing legitimacy and transparency by adhering to principles of proportionality, necessity, and accountability under domestic and international law. The United Kingdom actively uses sanctions–

supported by its independent cyber sanctions framework—and conducts extensive international coordination and joint responses alongside the United States.

Japan recently codified the concept of ACD into law and has actively reorganized its institutions to implement this shift. The NCO serves as the central authority for directing and coordinating ACD, while operational activities are carried out by the JSDF and NPA. An independent oversight body conducts prior review and approval of ACD measures and ensures the protection of communications privacy and personal data. This system is designed to ensure that controversial measures are conducted through legal procedures, thereby securing both legality and public acceptability. Japan has also begun to take a more active posture in public attribution, including direct attribution of cyberattacks to China.

Australia designates offensive cyber operations as an explicit mandate of the ASD and maintains distinct authorization and oversight procedures depending on operational purpose. The ASD operates a standing joint framework with the AFP and supports military cyber operations. Australia is currently making large-scale investments to strengthen the ASD's cyber capabilities and has expanded its reactive posture by pursuing joint sanctions and attributions with partners such as the United States and United Kingdom.

Singapore, as a relatively small state, adopts resilience building and active international cooperation as core strategies to avoid unnecessary geopolitical conflict. It strengthens proactive measures through early threat detection, information sharing, and recovery capabilities, while calibrating public attribution cautiously. At the same time, Singapore clearly signals its national will to respond to cyberattacks and seeks to enhance joint cyber response efforts through multilateral cooperation (e.g., via ASEAN and INTERPOL) as a means of securing deterrent effects.

Across these cases, the designation of "offensive" and "defensive" cyber operations is not uniform. Some states, such as the United Kingdom and Australia, define cyber operations as offensive acts, while others, such as the United States and Japan, frame them as extensions of defensive measures. Despite these differences in terminology and framing, all countries emphasize compliance with domestic and international legal norms, particularly proportionality, necessity, and accountability. To support these approaches, governments are increasing budgetary allocations and investing in the development of specialized personnel and operational capabilities.

Accordingly, South Korea should recalibrate its cyber defense strategy within an integrated framework that combines ACD with reactive response mechanisms. This should not be understood as offensive action aimed at attacking an adversary, but rather as a defensive approach that includes actively identifying and disrupting threats, as well as undertaking reactive measures and resilience-building efforts after an incident. What is needed, therefore, is a coherent strategy in which ACD and reactive response elements operate in a complementary manner, supported by sustained efforts to build the capabilities required to implement them effectively.

Current Status and Directions for Improvement in South Korea

SOUTH KOREA'S CYBER DEFENSE

Strategy and Governance

South Korea first introduced the term "active response" in its 2019 **National Cybersecurity Strategy**. Although the strategy did not define active defense, it included, under the task of developing "comprehensive and active response measures," efforts to prepare response tools consistent with international norms and expand cyber warfare personnel in the event of a significant cyber threat.

The 2024 **strategy** replaced the term "active" with "proactive" and "offensive," signaling the government's intention to move away from a predominantly defensive and reactive posture. The strategy identified "strengthening offensive cyber defense activities" as a major task and outlined detailed measures such as expanding attribution and responsibility assignment, establishing a deterrence strategy, blocking threats proactively, and developing diplomatic and technical tools to counter influence operations.

South Korea has also sought to establish a unified national cyber threat response system centered on the National Intelligence Service (NIS) and the National Security Office (NSO). In 2023, the government established the **National Cyber Crisis Management Center**, led by the NIS and operating under the oversight of the NSO, with participation from relevant ministries.

The legal and institutional basis for South Korea's ACD was largely established through the **National Intelligence Service Act**, in a way similar to the United Kingdom and Australia. The act designates "prevention and response to cyberattacks and threats" as an NIS mandate. This reflects the North Korea–centric threat environment facing South Korea and the fact that North Korea's early cyber activities were more aligned with espionage and asymmetric attacks than with military operations, and were thus addressed by the traditional counterintelligence process at the NIS. The **Regulation on Cybersecurity Services**, a subordinate regulation under the NIS Act, explicitly authorizes the NIS to conduct active cyber defense measures, including the tracking and neutralization of infrastructure located abroad.

As a military organization, the Cyber Command was established in 2011 and reorganized in 2019 into the **Cyber Operations Command** under the Joint Chiefs of Staff (JCS), following the removal of its psychological operations function. North Korea–related **psychological operations** are now performed by the Psychological Operations Group under the Ministry of National Defense (MND). The **Defense Counterintelligence Command** (DCC) supports the military's cyber protection posture and contributes to information operations.

The Cyber Operations Command is responsible for a wide range of tasks, including cyber operations planning and execution, security activities, system development and maintenance, training, information sharing, and threat intelligence collection. Since 2019, each military service—the **army**, **navy**, and **air force**—has established its own Cyber Operations Center responsible for defensive operations and security monitoring. In 2023, the NIS's National Cybersecurity Center (NCSC) and the Cyber Operations Command signed an **MOU** to formalize interagency cooperation.

Public attribution in South Korea is carried out by multiple agencies, including the NIS, National Police Agency (NPA), and Ministry of Foreign Affairs (MOFA), while cybersecurity advisories are primarily issued by the NIS. Investigations and law enforcement related to cyber-enabled national security crimes are led by the NPA and the Supreme Prosecutors' Office (SPO). Although relatively limited in number, sanctions—particularly those related to North Korea—are imposed by the MOFA and enforced by the Ministry of Economy and Finance (MOEF) and the Financial Services Commission (FSC).

SOUTH KOREA CASES

South Korea's responses to cyberattacks have been focused predominantly on North Korea. Until recently, responses to North Korean cyberattacks have consisted mainly of public attribution and statements of condemnation. However, in 2023, South Korea imposed its first independent **sanctions** related to North Korean cyber activities, signaling efforts to shift toward a more active response posture. Recently, attempts have been made to expand responses into coordinated, multiagency actions involving the NIS, NPA, MOFA, and MOEF.

Table 6: South Korea Cyber Response Cases

Year	Entities	Response	Type
2019	**NPA**	Public attribution and condemnation of the Upbit cryptocurrency theft	Reactive
2023	NIS, **NPA**, **MOFA**, MOEF	Joint attribution and sanctions against the Kimsuky hacking group	Reactive
2023	**NPA**	Public attribution and condemnation of cyber activities targeting ROK-U.S. joint military exercises	Reactive
2023	**NIS,** NPA, **MOFA**	Joint attribution and condemnation of North Korean IT workers; sanctions	Reactive
2023	MOFA, **MOEF**	Joint attribution and condemnation of illicit cyber activities involving technology theft; sanctions	Reactive
2024	**NPA**	Public attribution and condemnation of a cyberattack on the court network	Reactive
2024	**NPA**, NIS	Joint attribution and condemnation of cyber activities targeting weapons and military-related technologies; security advisory; international cooperation	Reactive
2024	**NIS**, NPA, SPO, DCC, Cyber Operations Command	Public attribution and condemnation of the attempted theft of defense technology; security advisory	Reactive
2024	MOFA, **MOEF**	Joint attribution and condemnation of North Korean IT workers; sanctions; international cooperation	Reactive
2025	**NPA**	Participation in Operation HAECHI targeting cyber financial crime; sanctions; freezing and seizure of assets; cooperation with INTERPOL	Reactive

Source: Author's analysis.

CHALLENGES AND CONSTRAINTS

Lack of Substantive Post-Attribution Measures

South Korea has experienced persistent cyberattacks from North Korea and has repeatedly issued attribution statements and condemnations. However, legal, economic, diplomatic, and ACD follow-up measures have lacked consistency and specificity.

In the international community, naming and shaming has been widely used as a response option to cyber threats, with an increasing number of states participating in this practice. Yet in many cases, the attributed state simply denies responsibility, and attribution is not followed by substantive measures, thus reducing its effectiveness and credibility. In South Korea, repeated attribution without meaningful consequences risks being perceived as either limited capability or insufficient political will.

This tendency is closely linked to broader strategic considerations. In managing relations with North Korea, the South Korean government has often prioritized nuclear security, crisis management, and inter-Korean stability over assertive cyber responses. Even when cyber operations do not directly escalate military tensions, concerns about destabilizing the broader security environment may lead to calibrated and restrained responses. As a result, cyber policy has at times reflected strategic caution rather than sustained cost imposition.

The 2024 National Cybersecurity Strategy signaled a shift toward a more forward-leaning posture by adopting the language of "offensive" cyber defense. However, publicly observable implementation has remained limited. Although economic sanctions and regulatory measures targeting cryptocurrency exchanges were introduced to curb North Korea's illicit financial gains, their impact has been constrained. North Korean actors have increasingly adapted by shifting to more opaque financial networks, including informal brokers and cryptocurrency mixers operating through **China** and **Russia**, thereby reducing the effectiveness of existing measures.

INSUFFICIENT OVERSIGHT AND AUTHORIZATION MECHANISMS FOR ACD

Major countries that conduct offensive or ACD operations have established clear domestic legal bases as well as pre-authorization and oversight procedures, emphasizing legitimacy and transparency. In South Korea, although the NIS is granted authority for ACD, the legal basis remains a broad delegation framed as "may take necessary measures, such as tracking and neutralizing."

Under current cybersecurity regulations, this authority allows the director of the NIS to identify, deter, and block foreign-based hacking infrastructure that threatens national security or national interest. However, the procedures for authorization, the structure of oversight, and the allocation of responsibility for failures or misuse are not sufficiently specified. The NSO is designated as the control tower for national cybersecurity, but its concrete role in reviewing and approving NIS's ACD measures is neither clearly defined nor operationalized.

This creates dual constraints: On one hand, the NIS director's discretion may be interpreted too broadly; on the other hand, legal and political liability concerns may discourage the agency from employing ACD capabilities. Without an oversight and authorization framework that ensures democratic control and transparency, the legitimacy and trustworthiness of ACD operations remain vulnerable to challenge, hindering their practical use.

Limitations on Military Roles and Authorities

Constraints also exist within the military domain. Although placing the Cyber Operations Command under the JCS reflects an intention to link cyberspace with broader military operations, the traditional mission set of the JCS—focused on land, sea, and air forces—raises the risk that cyber operations may be treated as auxiliary rather than as an independent strategic domain.

Moreover, because cyber operations blur the boundaries between peacetime and wartime, requiring persistent engagement and reconnaissance in the gray zone, the extent to which Cyber Operations Command can conduct ACD measures during peacetime is not clearly established.

Repeated political controversies—such as the **2013** online comment manipulation scandal and Cyber Operation Command's alleged involvement in intelligence activities during the **2024** martial law-related mobilization incident—have also weakened trust in the organization. These controversies led to the **removal** of its psychological operations function in 2019 and reinforced a risk-averse internal culture. This environment discourages the military from more actively implementing ACD. South Korea's constrained military posture therefore stands apart from emerging trends in other countries that are expanding dedicated personnel and capabilities for military cyber operations, and this limitation restricts the military's ability to assume a more active role in ACD.

Insufficient Interagency Cooperation Mechanisms

Gaps remain between the formal interagency cooperation framework and its actual implementation. Although agencies such as the NIS, MND, NPA, MOFA, and financial authorities each perform roles in cyber incident response, it is rare for technical analysis, investigation, prosecution, sanctions, diplomatic action, and ACD measures to form a coordinated set of response measures for a given cyber campaign.

There are also inconsistencies as to which agencies participate in a given case (reflected in Table 6). For example, despite joint investigative coordination by the National Cyber Crisis Management Center regarding North Korea's cyber activities during the 2023 ROK-U.S. joint military exercise, the final announcement was issued solely by the NPA. This may be because the NIS primarily issues security advisories, while the MOFA tends to accompany such cases with sanctions or other diplomatic measures; this resulted in the NPA taking the lead in announcing the investigation results. However, such single-agency announcements make it difficult to view the government's actions as a genuinely integrated national response to North Korea's cyber threats.

In the 2024 defense industry hacking case, the NIS issued a **security advisory**, but it was only months later that the police and the Defense Acquisition Program Administration jointly announced follow-up inspections, which were once again limited to **public attribution** without further substantive measures. Compared with the U.S. model—in which the NSA, CISA, FBI, DOJ, USDT, and DOS coordinate multilayered responses—South Korea's fragmented structure is a limitation.

The 2023 MOU between the NIS and Cyber Operations Command is a step toward closer cooperation, but its necessity highlights the absence of an institutionalized information-sharing and operational coordination system. The two institutions operate under different legal authorities and regulatory frameworks, and they also differ in security classification practices and operational approaches. As a result, institutionalized information sharing and personnel exchanges are difficult to implement.

Given the declaratory nature and limited legal force of the MOU, structural constraints on sustained cooperation remain.

Divergent Threat Perceptions and the Limitations of North Korea's Shift to Overseas Operations

North Korea's cyber operations increasingly target foreign financial institutions, cryptocurrency exchanges, global IT companies, and third-country infrastructure rather than South Korea directly. According to the **2025 Microsoft Digital Defense Report**, only 1 percent of observed North Korean cyber operations targeted South Korea—an especially sharp decline compared to **2023**, when attacks against the United States and South Korea accounted for 50 percent of North Korea's cyber operations. This indicates a structural shift toward overseas operations aimed at acquiring funds, technology, and infrastructure. It creates fundamental constraints for South Korea, as direct control or legal jurisdiction over third-country environments is limited.

However, reduced direct targeting does not imply reduced relevance. Funds and technology acquired overseas are funneled into North Korea's nuclear and missile programs, ultimately affecting South Korea's security environment. Attacks occur abroad, but their consequences cycle back to South Korea.

Moreover, South Korea's international cooperation remains narrowly focused on North Korea, even as China's and Russia's cyber activities increasingly impact South Korea's economic and technological security. Geopolitical and economic sensitivities further constrain South Korea's ability to take direct or unilateral action against major powers.

POLICY RECOMMENDATIONS

Expanding Practical Responses and Building an Operational Track Record

South Korea should expand substantive post-attribution responses within an integrated framework. Attribution should be one of the key elements feeding into a broader integrated response—one that brings together four elements: (1) legal measures (e.g., criminal indictments and joint investigations); (2) economic sanctions (e.g., asset freezes and financial restrictions); (3) diplomatic action (e.g., joint attribution, condemnation, and multilateral forums); and (4) technical measures (e.g., disrupting or dismantling malicious infrastructures, including those located overseas).

Although such measures may not directly alter North Korea's behavior—given its existing isolation and limited sensitivity to reputational costs—they can increase the operational and attack costs on third-country infrastructure, facilitators, financial channels, and IT personnel supporting North Korean operations. Repeated constraints on third-country enablers can raise the risk and burden of maintaining these operations, ultimately reducing their efficiency and impact.

The South Korean government should develop its own response options and strengthen its capabilities to implement both ACD and reactive response measures. Through sustained and tangible implementation, South Korea can build a track record of integrated response that reinforces credibility.

Clarifying Legal Procedures and Oversight for ACD

To conduct ACD operations, South Korea should first establish clear domestic authorization and oversight frameworks. This requires defining the roles of the president and NSO, NIS and MND, and the National Assembly. A multilayered structure should include: (1) top-level authorization, (2) delegated execution with internal controls, and (3) external democratic oversight.

Significant actions with military or diplomatic implications—such as operations affecting foreign critical infrastructure—should require prior approval from the president or NSO. The NSO could ensure that a substantive review is carried out, including an assessment of necessity, proportionality, and domestic and international legality.

Limited ACD operations may remain under the authority of the NIS director, but with clearer scope and conditions. The NIS could execute such measures swiftly while reporting outcomes to the NSO. Distinguishing between presidential/NSO authorization and delegated authority would help balance responsiveness with control.

Oversight should combine internal and external mechanisms. Internally, the NSO could maintain records and conduct reviews of all ACD activities. Externally, regular classified reporting to relevant National Assembly committees could provide minimum democratic accountability.

Defining Roles Across Peacetime, Crisis, and Wartime and Strengthening Military Cyber Capabilities

An integrated cyber response framework should establish sequential role division across peacetime, crisis, and wartime. Intelligence agencies possess comparative advantages in tracking North Korean espionage-oriented cyber threats and overseas infrastructure during peacetime and periods of gray zone confrontation, while the military should lead combined and joint cyber operations during wartime.

In peacetime, the NIS should lead persistent engagement while the military provides operational support. During crisis periods, the National Cyber Crisis Management Center should direct, coordinate, and control the full spectrum of cyber defense activities, with the NIS and MND cooperating under its direction. In wartime, operational control for cyber offense and defense should transition to the military, with intelligence agencies providing continued support. Relevant authorities, missions, and command structures could be codified in law or operational manuals, with clear transition procedures across phases.

Military active and offensive cyber capabilities should also be strengthened. This includes insulating the Cyber Operations Command from political controversies, reinforcing operational units dedicated to attack, active defense, and joint operations, and enabling focus on disruptive actions against adversary infrastructure and military cyber effects. Moreover, actual operational execution requires cultivating legal specialists capable of assessing risks and advising on the lawful conduct of cyber operations. In the long term, limited credible signaling of offensive capabilities may be considered to enhance deterrence.

INTEGRATED USE OF CYBER, LEGAL, DIPLOMATIC, AND ECONOMIC TOOLS (WHOLE-OF-GOVERNMENT RESPONSE)

Effective cyber response requires integrated action rather than isolated, agency-specific measures. Technical analysis, investigative action, prosecution, sanctions, diplomatic actions, and ACD measures should be linked as a unified response to specific attacks or campaigns.

A standardized joint response process should link actions by the NIS, MND, NPA, MOFA, MOEF, and others. The National Cyber Crisis Management Center should strengthen its coordinating function so

that technical assessments, disruption efforts, investigative direction, diplomatic action, and sanctions decisions are not merely shared but strategically integrated. An integrated architecture would allow South Korea to convey consistent messages and impose meaningful costs on malicious actors.

EXPANDING INTERNATIONAL COOPERATION BEYOND A NORTH KOREA–CENTRIC APPROACH

Given that North Korea conducts most of its cyber operations abroad, the room for unilateral South Korean response is inherently limited. In light of this reality, South Korea should gradually expand its extraterritorial ACD activities. To ensure that such actions remain within the bounds of international law, however, the South Korean government should carry them out with the prior consent and cooperation of relevant third-country authorities or through joint operations with the United States and other allies. Building these conditions requires a broad framework of international cooperation that includes joint action, investigative cooperation, capacity-building support, and information sharing with allies and partners.

Moreover, considering the growing impact of Chinese and Russian cyber activities on South Korea's economic and technological security, South Korea should expand its threat perceptions beyond North Korea and increase participation in multilateral and international responses. Such engagement not only builds trust with allied partners and provides an indirect means of responding to Chinese and Russian cyber activities, but also helps strengthen the diplomatic and operational foundations for more coordinated international responses to North Korea's cyber threats.

Cooperation with third countries whose infrastructure and financial networks are exploited by North Korean actors, and where North Korean personnel operate, is also crucial. Recent initiatives—such as the **MOU** with China on voice phishing and online fraud, or the establishment of an **international cooperation mechanism** for cross-border scam response—represent meaningful progress. Providing capacity-building assistance to strengthen the cyber defenses of third countries not only disrupts North Korea's revenue-generation channels but also helps secure third countries' consent and cooperation for expanding ACD measures against North Korean operations conducted on their territory. In particular, given China's role as a key transit environment for North Korean cyber activities—including the movement, laundering, and cash-out of illicitly obtained funds—cooperation with China remains indispensable for effectively addressing these threats.

Ultimately, South Korea should evolve into an active and meaningful contributor to international cyber response efforts. By expanding international cooperation along these lines, South Korea can enhance its ability to counter overseas cyber threats. ■

Sunha Bae *is a senior researcher on the Cybersecurity Policy Research Team at the National Security Research Institute of Korea.*

This report is made possible through support from the National Security Research Institute (NSR) of Korea. CSIS and NSR conducted scholarly research on U.S.-ROK cyber resilience. The analysis presented here was independently authored by researchers at NSR.