JULY 2025

A Cyberattack Severity Classification Framework for the Republic of Korea

By Sunha Bae

Introduction

Despite deterrence efforts, cyber threats continue to escalate, highlighting the need for greater accountability from and cost imposition on malicious actors. The U.S. **2023 National Cybersecurity Strategy** emphasizes imposing costs on malicious actors and reinforcing alliances; the Republic of Korea's (ROK) **2024 National Cybersecurity Strategy** also prioritizes offensive cyber defense and global cooperation. Since 2018, U.S. Cyber Command's "Defend Forward" policy has resulted in 40 **Hunt Forward operations** across 21 countries, exposing threats from major **adversaries**. Similarly, the European Union's updated 2023 **Cyber Diplomacy Toolbox** stresses situational awareness and the importance of holding persistent threat actors accountable.

Attributing cyberattacks and formulating response strategies are inherently political processes shaped by national security priorities, diplomatic relations, and geopolitical **considerations**. Governments must balance deterrence with escalation risks, ensuring proportionality and international legitimacy. It is therefore difficult to establish a single, uniform standard for response. Nevertheless, consistent policy is necessary, as the absence of clear frameworks increases political burdens, delays decisionmaking, and results in inconsistent responses that can confuse allies.

A national framework for classifying cyberattack severity enhances objectivity, guiding policy decisions and facilitating mutual understanding between nations. Although South Korea has shown strong political will to respond to malicious cyber activities, it lacks a clear legal and policy framework for response procedures. To fill this gap, this paper proposes a Cyberattack Severity Classification Framework (CSCF) to objectively assess and categorize cyberattacks, supporting informed decisionmaking.

Purposes of the Cyberattack Severity Classification Framework

- **Support Political Decisionmaking and Strengthen the Framework for Cost Imposition and Accountability:** The CSCF supports the ROK government's political decisionmaking regarding cost imposition and accountability for malicious actors and their state sponsors at the international level. In doing so, the framework helps facilitate sustained international engagement in cyber threat mitigation.

- **Establish a Basis for International Cooperation:** Publicly sharing a national cyberattack severity assessment framework promotes transparency. By aligning with common evaluation criteria, the CSCF supports mutual understanding, helps partners better interpret intent, and strengthens situational awareness, playing a crucial role in advancing international cooperation efforts.

This study, part of a project to enhance ROK-U.S. cybersecurity cooperation, aims to classify cyberattack severity at the national level to support shared understanding and coordinated responses. It reviews government-led models and simplifies criteria around core items for clarity and efficiency. Case studies of state-sponsored cyberattacks in the United States and ROK over the past decade will test the framework's applicability. Although the CSCF is limited by its reliance on public data, it seeks to support cost imposition efforts and to provide a foundation for international cooperation against cyber threats.

National and International Methodologies

UNITED STATES

Presidential Policy Directive 41 (PPD-41): U.S. Cyber Incident Coordination

PPD-41 (2016) aims to enhance national security by managing and coordinating responses to significant cyber incidents. The United States defines a significant cyber incident as a group of related events, rather than a single isolated incident. PPD-41 introduces the Cyber Incident Severity Schema (CISS) to establish a unified federal understanding of incident severity, supporting coordinated national-level responses to significant incidents. CISS outlines six levels–Emergency, Severe, High, Medium, Low, and Baseline–based on the scope of the incidents and their impact on national security and public safety.

Assessment Criteria

- Scope and Impact: Evaluates the level of observed or potential effects on national security, public health, critical infrastructure, the economy, and public confidence

- Observed Actions: Categorizes incidents into preparation, engagement, presence, and effect phases

- Intended Consequence: Assesses attacker intent and potential damage scope

National Cyber Incident Scoring System (NCISS)

Developed by the Cybersecurity and Infrastructure Security Agency (CISA), the **NCISS** provides a consistent method of assessing cyber incidents and prioritizing the response to them across federal agencies. It assigns **risk scores** to incidents, which then guide response priorities and resource allocation. However, the NCISS struggles to assess simultaneous related incidents, relying on expert judgment instead of predefined criteria, which can cause inconsistencies and reduce objectivity in assessments. The NCISS uses the same six-level severity scale outlined by the CISS.

Assessment Criteria

- Functional Impact: Effect on organizational operations
- Observed Activity: Behavior of the threat actor
- Location of Observed Activity: Network areas where malicious activities are detected
- Actor Characteristics: Capabilities and intentions of the threat actor
- Information Impact: Sensitivity of compromised data
- Recoverability: Resources required for incident recovery
- Cross-Sector Dependency: Connections between critical infrastructure sectors
- Potential Impact: Scale and significance of the affected organization

EUROPEAN UNION

NIS Directive 2.0

The NIS Directive 2.0 (2022) establishes a unified framework for network and information security across the European Union. It covers a wide range of critical infrastructure and essential services vital to public safety, economic stability, and national security. Entities are required to assess and report cyber incidents that cause or could cause severe operational disruptions, financial losses, or significant harm to individuals or **organizations**. The scope of critical infrastructure and essential services includes sectors such as energy (electricity, oil, gas, and hydrogen), transport (air, rail, water, and road), banking and financial systems, healthcare, water supply, digital infrastructure (e.g., domain name systems, content delivery networks, and cloud), information and communication technology service management, public administration, and space-related organizations.

Assessment Criteria

- Impact on service operations
- Financial impact
- Impact on other individuals or organizations (material or nonmaterial)
- Importance of affected networks and information systems to the entity’s service delivery
- Severity and technical characteristics of the cyber threat
- Extent of impact on service functionality
- Duration of the incident
- Number of affected service recipients
- Whether the entity has experienced similar incidents previously
- Whether the incident was due to malicious or unlawful acts
- Possibility of cross-border impacts

Cybersecurity Incident Taxonomy (CIT)

The **EU CIT**, proposed by the NIS Cooperation Group in 2018, offers a standardized framework for classifying cybersecurity incidents at strategic and political levels. It aims to enhance coordination of incident response activities across the European Union and facilitate cross-border information sharing and cooperation. According to a 2022 Organization for Security and Co-operation in Europe (OSCE) **report**, many European Computer Security Incident Response Teams (CSIRTs) or relevant bodies are utilizing the EU CIT in their processes. Notably, Estonia has adopted the EU CIT as a national model.

Assessment Criteria

- Attack Target: Sector affected by the cyberattack (e.g., energy, transport, finance, healthcare, water, digital infrastructure, government services)
- Threat Severity: Technical risk level of the threat
- Impact Severity: Societal or economic damage level

Cyber Diplomacy Toolbox (CDT)

The **CDT** is an EU framework designed to prevent, deter, and respond to malicious cyber activities, promoting solidarity and mutual support among member states. The CDT emphasizes the importance of shared situational awareness and information sharing among EU member states, aiming to improve the understanding of the European Union's threat environment and encourage the use of the CDT to support decisionmaking. It strengthens coordinated strategies to counter persistent cyber threat actors, reinforces the international obligation of due diligence, and introduces additional response options.

Assessment Criteria

- Scope
- Scale
- Duration
- Intensity
- Complexity
- Sophistication
- Impact

UNITED KINGDOM

Categorization Model for Cyber Incidents (CMCI)

The United Kingdom's National Cyber Security Centre (NCSC) in 2023 used the **CMCI** to classify cyber incidents based on severity and potential impact. It ensures effective resource allocation and response coordination across sectors, including government, critical infrastructure, businesses, and individuals. The NCSC and National Crime Agency (NCA) oversee assessments. Severity levels are classified into six tiers, similar to the U.S. CISS model, based on the scope of affected targets (e.g., nation, institution, individual) and the level of socioeconomic impact.

Assessment Criteria

- National Security Impact: Disruptions to essential services, potential harm to life or national security
- Scale of Disruption: Level of interference in services or operations
- Economic and Social Impact: Financial losses, data breaches, privacy violations, and social consequences
- Attack Target: Categorizes affected entities such as critical infrastructure, government, enterprises, small- and medium-sized enterprises, and individuals

Cyber Regulations 2020 (CR)

The **Cyber Regulations 2020** were established under the Sanctions and Anti-Money Laundering Act 2018 to counter cyber activities threatening the United Kingdom's integrity, economy, and security. These regulations allow the United Kingdom to impose sanctions on individuals or entities involved in cyber threats, including asset freezes and travel bans. Although the regulation does not explicitly define assessment criteria, it outlines the definition of relevant cyber activity and types of cyber activities, which form the basis of the assessment criteria.

Assessment Criteria

- Intent: Whether the attack aimed to cause harm
- Scope of Impact: Number of affected people or systems
- Target: Whether the attack was on critical infrastructure or essential services

FRANCE

National Cyber Attack Classification Scheme (NCACS)

France's Cyber Review (2018) introduced a cyberattack classification system to enhance threat assessment and response coordination. The **NCACS** highlights the need for a clear understanding of cyberattacks and rapid analysis of attack techniques for proportionate responses. Its classification scheme aims to enhance shared understanding, support decisionmaking, and promote international cooperation on cross-border incidents. The framework prioritizes impact-based evaluations, covering completed or imminent attacks that require urgent responses. Severity levels, compatible with the U.S. CISS, are classified into six tiers based on the scope and impact of cyber incidents. However, the NCACS incorporates international legal considerations, including the possibility of an armed attack under UN Charter Article 51, with the most severe level designated as "possibly assessable."

Assessment Criteria

- Impact: Effect on national interests, security, the economy, and the environment
- Technical Capability: Attack sophistication and methods used
- Intent: Motivations behind the attack
- Target Risk: The affected entity's significance
- Scale: Attack severity and widespread effects

- Repetition: Frequency and relation to past incidents

CANADA

Government Cyber Security Event Management Plan (GC CSEMP)

Canada's Federal Cyber Incident Response Plan differentiates between general and critical incidents, with critical incidents addressed under the **GC CSEMP** (2023). The GC CSEMP ensures coordinated cyber incident management across government systems, led by the Canadian Centre for Cyber Security and the Treasury Board of Canada Secretariat's Office of the Chief Information Officer (TBS-OCIO). It includes the Injury Test, which assesses cyber incident severity and scope, and the Risk Assessment, which evaluates potential exposure. This report focuses on the **Injury Test**, which sorts incidents into four levels based on their scope and severity. Each level is defined by the extent of damage across five areas–public health, financial loss, government services, national security, and reputation–to provide clearer understanding of the attack's severity.

Assessment Criteria

- Severity: Degree of harm across domains such as public health, financial loss, government services, national sovereignty, national security, and reputation
- Scope: Extent of impact in terms of the number of affected individuals, organizations, facilities, or systems; the geographic area (e.g., international, national, multiple sectors, single sector or jurisdiction, individual or small business); and the duration

AUSTRALIA

Cyber Incident Categorization Matrix (CICM)

The Australian Signals Directorate (ASD) developed the **CICM** to prioritize incident response and ensure appropriate measures. Continuously updated, it is used by the Australian Cyber Security Centre to classify and manage cyber incidents effectively, as well as provide annual cyber incident **statistics**. Severity levels are classified into six tiers based on the intensity of cyber effects and the significance of the affected organization.

Assessment Criteria

- Cyber Effect: Evaluates impact based on attack success, persistence, and intent (e.g., disruption to critical systems, broad or localized compromise, coordinated or isolated low-level attacks, or failed attacks)
- Significance: Assesses the importance of affected organizations (e.g., the general public, small to large organizations, educational and research institutions, local to federal governments, critical infrastructure, and national security systems)

CHINA

Cybersecurity Incident Classification Guide

To standardize incident reporting and enhance security, China issued the **Cybersecurity Incident Reporting Administrative Measures Draft (2023)** under the Cybersecurity Law, defining **severity levels** and standardizing response procedures for government agencies, critical infrastructure operators, and network service providers. Similarly to GC CSEMP, severity is classified into four levels whose severity is defined across five dimensions—system disruption, data leakage, social impact, economic loss, and harmful information spread—to support rapid decisionmaking.

Assessment Criteria

- System Loss and Functional Disruption: Network failures affecting critical operations
- Information Leakage and Data Loss: Exposure of state secrets and sensitive information
- Social Impact: Number of affected people and essential service users
- Economic Loss: Direct financial damage
- Harmful Information Spread: Dissemination of illegal or harmful content

SUMMARY AND COMPARISON

Key Characteristics of National Frameworks

The United States assesses cyber incident severity through the CISS framework, integrating PPD-41 and the NCISS. The NCISS uses a quantitative, weighted scoring system to promote consistent assessment practices across the federal government and critical infrastructure sectors. CISA conducts evaluations based on reports from affected entities to ensure consistency.

The European Union classifies incidents via the NIS Directive, CIT, and CDT, sharing core criteria. The CIT, adopted by some member states like Estonia, supports standardized classification and information sharing. Both the NIS Directive and CIT classify attacks on critical infrastructure and essential services as critical threats, clearly identifying relevant sectors and applying broad coverage. One limitation is that these guidelines—particularly the CIT and CDT—are non-binding recommendations, and therefore not applied consistently across all EU member states.

The United Kingdom classifies cyber incidents through the CMCI and Cyber Regulation, which evaluate attack targets as well as economic, operational, and social impact. The sanctions regulation also considers attacker intent (malicious or unlawful) to ensure accountability and cost imposition on threat actors. Similar to the U.S. system, the NCSC and NCA carry out categorization to promote consistent assessment.

France employs cyber incident severity classification to support proportionate responses to malicious activities, emphasizing situational awareness and international cooperation. The NCACS is designed to be compatible with the U.S. CISS, aiming to enhance mutual understanding of cyber threat levels in the context of international coordination.

Canada's GC CSEMP assesses threats and risks using a matrix-based system to determine response levels. Similarly to the United Kingdom, Canada classifies attack targets by scale and considers the transnational scope of incidents.

Australia's CICM prioritizes victim importance and impact, using a simplified approach. The government maintains and updates its matrix, publishing annual statistics on the severity of cyber incidents in Australia to enhance awareness. The 2023 update categorizes impact by scope, focusing on supply chains, shared services, and critical infrastructure. Australia's framework remains adaptive to changing cyber threats.

China has introduced a cyber incident classification guide and is developing supporting legislation. While it is similar to international models in most assessment criteria, China's system emphasizes controlling harmful information, in line with state information policies. The framework includes quantitative standards, enabling rapid identification and reporting of major cyber incidents, though the basis for these standards is not explicitly provided.

Core Criteria

Across countries, cyber incident assessment criteria generally outline three tiers of importance. Core criteria–such as the scope and importance of the target; attacker intent; impacts on operations, the economy, society, and national security; potential loss of life; and scale and duration–are prioritized in most frameworks. Frequently considered but less emphasized are secondary factors like technical capabilities and incident frequency. Finally, other factors–such as infrastructure dependencies, attack success, harmful information dissemination, and recoverability–are selectively used depending on the context and purpose of the assessment.

While national goals vary, many countries acknowledge the value of severity classification frameworks for crisis response, resource allocation, and international cooperation. Notably, models like the European Union's CDT, the United Kingdom's regulatory framework, and France's NCACS show how classification can support accountability and diplomatic engagement.

Table 1: Comparison of Assessment Criteria

Category	Criteria	Countries/Regions
Attack Target	Scope, importance of system/target	United States (PPD-41, NCISS), European Union (NIS, CIT, CDT), United Kingdom (CMCI), France, Canada, Australia, China
	Cross-sector dependency	United States (NCISS)
Attacker Intent/ Capability	Attacker intent (malicious/illegal)	United States (PDD-41, NCISS), European Union (NIS), United Kingdom (CR), France, Canada, Australia, China
	Complexity/sophistication	United States (PDD-41, NCISS), European Union (NIS, CDT), France
Impact and Damage	Economic, functional, informational, social, and national security impact; risks to health and safety	United States, European Union, United Kingdom, France, Canada, Australia, China—all of which include multiple dimensions, with slight variations
	Scale, duration, intensity	
	Frequency	France
	Recoverability	United States (NCISS)
	Spread of harmful information	China

Source: Authors' analysis.

Cyberattack Severity Classification Framework (CSCF)

ASSESSMENT CRITERIA

The CSCF criteria are based on international frameworks and focus on core criteria to improve efficiency and consistency. While international models incorporate a wider range of factors, this framework prioritizes core criteria by grouping them into three main categories–attack target, attacker intent, and impact–comprising a total of seven sub-criteria, all organized into three levels for simplicity.

Attack Target

1. **Scope**

   This assesses scope by affected entity range.

- High: Nationwide or multinational impact
- Medium: Regional or multi-organization impact
- Low: Localized or single-organization impact

2. **Importance of Affected Targets**

   This assesses the criticality and sensitivity of the affected organizations and systems.

- High: Organizations crucial to national security, such as critical infrastructure or government agencies, based on the **critical infrastructure** sectors defined by the U.S. Department of Homeland Security (DHS) and the ROK's **Act on the Protection of Information and Communications Infrastructure**
- Medium: Large-scale private sector organizations, including major enterprises. The criteria for defining large enterprises in the ROK and the United States are as follows (though they may differ by industry in both countries):
  - South Korea: Large-scale enterprises are defined by the Korean government as organizations with total assets exceeding **10 trillion KRW**.
  - United States: Large enterprises are generally defined as those with more than 500 employees or annual revenue exceeding **$47 million**, according to the Small Business Administration (SBA).
- Low: Smaller organizations or those with limited national significance

Attacker Intent

3. **Intent**

   This assesses the goals and motivations of the attacker.

- High: Goal-oriented attackers–including state-sponsored groups or international hacking organizations–conducting long-term operations for political or economic gain
- Medium: Criminal actors pursuing monetary gains
- Low: Opportunistic or unintentional actors with no clear objectives

Impact

4. **Functional Impact**

   This assesses the disruption or degradation of critical functions and services. Time thresholds, such as the recovery time objective (RTO) or maximum tolerable downtime (MTD), are used as benchmarks. The time thresholds may vary depending on the importance of the organization and system.

- High: Significant damage or prolonged interruptions, such as system downtimes exceeding the RTO or MTD
  - South Korea: The RTO for critical government systems can be set within three hours. The Ministry of Interior and Safety in South Korea has set the MTD for government systems at **three hours**.
  - United States: The RTO for national or mission-essential functions is generally set within 12 hours. According to **NIST Special Publication 800-34 Rev. 1** (Contingency Planning Guide for Federal Information Systems), the recovery time for functions that are national, primary, or mission-essential must be within 12 hours to ensure operational continuity.
- Medium: Partial damage or interruptions, such as disruptions contained within the RTO or MTD limit
- Low: Minor or no impact on functions and services

5. **Information Impact**

   This assesses the compromise of data integrity, confidentiality, or availability:

- High: Breach of classified or sensitive information
- Medium: Breach of non-classified or general information
- Low: Minor or no impact on information

6. **Economic Impact**

   This assesses the financial and economic damage caused by cyberattacks. The thresholds used are reference values informed by the U.S. **CISA report** *Cost of a Cyber Incident,* which systematically analyzes financial impacts (with a methodology detailed in Appendix A of this paper).

- High
  - South Korea: Financial loss exceeding 20 billion KRW (approximately $15.7 million) or affected population of more than 10 million individuals
  - United States: Financial loss exceeding $157 million or an affected population of more than 72 million individuals

- Medium
    - South Korea: Financial loss between 5 billion and 20 billion KRW (approximately $4 million to $15.7 million) or affected population of 1-10 million individuals
    - United States: Financial loss between $40 million and $157 million or an affected population of 8-72 million individuals
- Low
    - South Korea: Financial loss below 5 billion KRW (approximately $4 million) or an affected population of fewer than 1 million individuals
    - United States: Financial loss below $40 million or an affected population of fewer than 8 million individuals

7. **Political and Social Impact**

   This considers the implications for national security, reputation, public relations, and societal responses.

- High: Severe impacts, including extensive media coverage, significant social media backlash, substantial drops in presidential approval ratings, or a decline in international trust indices
- Medium: Moderate impacts with notable effects on public perception or international relations
- Low: Minor or localized effects with limited public attention

WEIGHTING OF ASSESSMENT CRITERIA

According to the **Tallinn Manual 2.0**, a cyber operation's classification as a use of force or severe attack depends on scale, effects, and target. And the **UN GGE** and **OEWG**, two international initiatives on cyberspace norms, emphasize that attacks on critical infrastructure pose significant risks and are considered particularly severe.

A **survey** conducted by the OSCE identified impact and damage scale as the most critical criteria for assessing cyberattacks, followed by attack target. Similarly, a 2022 survey by the National Security Research Institute (NSR) in South Korea found that experts ranked attack sector, importance of the damaged system, and damage scale as the top factors influencing cyber severity assessments (detailed in Appendix B of this paper).

This prioritization aligns with a broader consensus that cyberattack assessments should focus on:

- Impact, including social, functional, and economic consequences
- Target, especially when critical infrastructure is affected

The CSCF reflects importance by letting the number of items in each category influence the results.

SCORING AND SEVERITY LEVELS

The CSCF determines severity by assigning scores to assessment criteria, with a maximum score of 35 points. Each criterion is scored on a three-tier scale based on severity: High (4-5 points), Medium (2-3 points), and Low (0-1 point). The framework uses the total score across all criteria to categorize cyber incidents into six severity levels–Normal, Low, Medium, High, Severe, and Critical–aligning with the CISS used in the United States and France. The United Kingdom and Australia also follow a similar six-tier classification model. Using comparable severity levels helps promote mutual understanding of assessment results among nations.

Table 2: Cyberattack Severity Level

Level	Score Range	Details
Normal (White)	0–10	No impact on national security or citizens
Low (Green)	10–15	Minimal impact on national security and citizens; does not affect major functions
Medium (Blue)	16–20	Impact on national security and citizens; includes partial disruption to major functions and resources
High (Yellow)	21–25	Significant impact on national security and citizens; affects multiple major functions and resources
Severe (Orange)	26–30	Severe impact on national security and citizens; includes widespread disruption to major functions and resources
Critical (Red)	31–35	Critical and nationwide impact on national security and citizens, causing extensive damage and disruptions

Source: Authors' analysis.

CUMULATIVE EFFECTS

Cyberattacks from major adversarial states are often parts of broader strategic **campaigns** rather than isolated incidents. These operations typically unfold within the "gray zone," staying below the threshold of armed conflict to avoid direct retaliation. Attackers employ long-term reconnaissance and persistent access, expanding their targets from individual systems to interconnected networks to achieve their strategic objectives.

Assessing cyber incidents in isolation risks underestimating their intent and cumulative effect. To address this, viewing a cyberattack as part of a broader campaign not only strengthens the assessor's ability to make **political attributions** but also provides a deeper understanding of the attacker's strategic objectives and operational patterns. In line with this, U.S. **PPD-41** recognizes that a series of related incidents with cumulative effects may qualify as a Significant Cyber Incident, and NATO's 2021 **Comprehensive Cyber Defence Policy** acknowledges that such activities could, under certain conditions, be classified as an armed attack.

Integrating cumulative effects into the severity assessment process also helps mitigate a key limitation of the CSCF: the potential perception that low-level or sub-threshold attacks will go unaddressed. By accounting for the cumulative effect of recurring or persistent malicious activity, the framework conveys that even seemingly minor incidents may be evaluated and incorporated into broader strategic assessments.

To evaluate cumulative effects, a composite approach should be applied across the assessment criteria. For each criterion, the scope should be aggregated across incidents; the importance of affected targets should be assessed based on the most critical target; intent should reflect the most hostile objective; and impacts should be accumulated to reflect the overall effect.

Case Studies

This paper's case study applied the CSCF to 21 cyberattacks over the past decade, primarily targeting the ROK and United States, focusing on critical infrastructure and state-sponsored hacking activities. The results are presented in Table 3. While the initial assessment covered 21 cases, 2 incidents were re-evaluated by applying cumulative effect, bringing the total to 23 entries in the table. Entries 1 through 8 correspond to the ROK and 9 through 20 to the United States. Entry 21 involves a German target, included for cumulative analysis, while entries 22 and 23 reflect re-assessed cases.

The assessment presents **EuRepoC's** cyber intensity and impact scores as a comparative benchmark to provide context for the CSCF results. Where EuRepoC scores are unavailable, the corresponding table entries are marked as blank. **EuRepoC**, an open-access database supported by EU member state governments, measures cyber intensity based on direct effects and sociopolitical severity, while its impact indicator evaluates broader consequences.

EuRepoC's cyber intensity is categorized into three levels:

- 1-5: Low/Moderate (Green); 6-10: High (Yellow); 11-15: Very High (Red)

Impact is classified into five levels:

- 1-5: Minor (White); 6-10: Low (Green); 11-15: Medium (Yellow); 16-20: High (Orange); 21-25: Very High (Red)

In South Korea, cyberattacks ranged from Medium to High severity according to the CSCF, with cases like the KHNP Hacking (Entry 1) and the Pyeongchang Olympics Hacking (Entry 3) showing notable social and political impact. Although the KHNP Hacking caused limited direct disruption, it triggered public alarm by targeting nuclear facilities, and led to the development of **South Korea's cybersecurity strategy**. It was classified as High severity under the CSCF. However, according to EuRepoC, both cases were rated within the Low/Moderate intensity range.

North Korean hacking groups were responsible for the most severe attacks on South Korea, particularly the 2023 Andariel IT Company Breach (Entry 7) and the 2024 Defense Contractor Breach (Entry 8), both of which targeted military intelligence and defense technology. The Defense Contractor Breach received the highest scores under the CSCF due to its significant informational and social impact. In contrast, according to EuRepoC, Entry 7 was rated as Low/Moderate in intensity and Low in impact, while Entry 8 was assessed as High in intensity but still rated as Low in impact.

The United States, facing more frequent and severe cyber threats compared to South Korea, exhibited higher severity levels in CSCF-based assessments, with attacks classified as Medium to Severe. High-profile cases such as SolarWinds (Entry 13), Colonial Pipeline (Entry 17), Volt Typhoon (Entry 18), and Salt Typhoon (Entry 19) reached Severe under the CSCF due to their impact on national security and critical infrastructure. Additionally, the Hive Ransomware Attack (Entry 14) was rated Severe according to the CSCF, since it caused significant financial and operational disruptions. In contrast, according to EuRepoC, the Hive Ransomware Attack was rated as Low/Moderate in intensity and Low in impact. For the remaining cases, while some were assessed as High in intensity, all were rated Medium or lower in impact.

Cases in which cumulative effect is applicable under the CSCF include the 2022 Defense Manufacturer Attack (Entry 6), and the 2024 Defense Contractor Breach (Entry 8), both by North Korean groups targeting South Korean defense contractors; and the 2024 Diehl Defense Breach (Entry 21) involving a German missile supplier, which also fits this pattern. Though individually limited, their cumulative effect within the "North Korea Defense Breach Campaign" justifies a reclassification to Severe.

The 2015-2016 DNC hacking incidents (Entry 10) in the United States are attributed to Cozy Bear and Fancy Bear as part of Russia's election interference efforts. Along with the post-election spear-phishing attacks (Entry 11) by the same threat actors and with the same political aim, these incidents can be collectively referred to as the "Russian U.S. Election Interference Campaign." When assessed as a broader campaign, the impact increases and may justify a Severe classification under the CSCF.

Overall, the CSCF and EuRepoC showed a similar relative ranking of cases–those rated highly under the CSCF generally also received higher ratings under EuRepoC. However, EuRepoC tended to assign lower absolute intensity and impact scores compared to the CSCF. This alignment in severity levels was slightly closer in U.S. cases, while ROK cases showed some differences, likely due to EuRepoC's EU-centric focus on large-scale impacts. Since political and economic impacts vary by national context, frameworks like the CSCF–which present reference points informed by such context–are better suited to national-level assessment. In particular, because the importance of the attack target is a critical factor in national security considerations, the CSCF has enabled more appropriate severity assessments in such contexts.

Table 3: t

No.	Date	Name	Attributed Country	CSCF Score and Level	Notes (EuRepoC)	
					Intensity	Impact
1	Dec. 2014	KHNP Hacking	North Korea	21	3	-
2	June 2016	Cyber Command Hacking	North Korea	20	3	-
3	Feb. 2018	PyeongChang Olympic Hacking	Russia	21	4	-
4	Jan. 2019	Leak of Foreign Ministry Emails	China	18	4	-
5	May 2021	SNU Hospital Hacking	North Korea	18	4	6

6	Oct. 2022	North Korean Defense Manufacturer Attack	North Korea	23	4	7
7	Dec. 2023	Andariel’s Attack on Korean IT Companies	North Korea	21	4	7
8	Jan. 2024	North Korean Defense Contractor Breach	North Korea	23	6	9
9	2014	Westinghouse Hacking	Russia	20	2	-
10	2015–2016	DNC Email Leak & Election Interference	Russia	23	4	-
11	Nov. 2016	Cozy Bear Post-Election Spear-Phishing	Russia	17	3	-
12	2017	Equifax Data Breach	China	21	4	-
13	2019–2020	SolarWinds Supply Chain Attack	Russia	28	4	15
14	2020	Hive Ransomware Attack	Non-state	26	4	7
15	2021–2023	RedHotel Attack	China	24	1	7
16	2021	Andariel Maui Ransomware Attack	North Korea	23	4	9
17	May 2021	Colonial Pipeline Attack	Russia	26	6	12
18	2021–2024	Volt Typhoon Attack	China	28	6	13
19	2023–2024	Salt Typhoon Attack	China	26	1	5
20	2023–2024	RedJuliett (Flax Typhoon) Cyberattack	China	25	3	7
21	Sept. 2024	Hacking of German Defense Company Diehl Defence	North Korea	15	-	-
22	2020–2024	North Korea Defense Breach Campaign	North Korea	29	-	-
23	2015–2016	Russian U.S. Election Interference Attack	Russia	27	-	-

Source: Authors' analysis.

Conclusion

The CSCF provides a systematic framework for assessing cyberattack severity, thereby enhancing situational awareness and supporting the ROK government's political decisionmaking. It promotes international understanding, facilitates national cost imposition efforts, and supports joint responses. This approach aligns with the strategic goals of the **ROK-U.S. Cybersecurity Cooperation Framework**, which emphasizes countering and deterring malicious cyber activities while holding responsible states accountable.

The CSCF was developed through comparative analysis to identify core criteria and organize them into three categories: impact, target scope, and intent. The framework also offers detailed sub-criteria with reference points based on publicly available data. When applied to cases, high-profile incidents such as the Volt Typhoon and Salt Typhoon were classified as Severe, effectively capturing their national security implications. Moreover, when multiple attacks by the same hacking group with similar objectives were assessed cumulatively as part of a single campaign—such as the North Korea Defense Breach Campaign—the attacks' severity levels increased.

The case study results underscore the need for a national-level classification framework that reflects country-specific contexts. The CSCF is particularly well-suited for evaluating the severity of cyberattacks in South Korea, especially from a national security perspective. Such a framework enhances understanding of domestic cyber incident severity and can serve as a foundation for improving mutual understanding in the context of future ROK-U.S. cybersecurity cooperation.

Cyberattacks have grown in scale and complexity over the past two decades. Unlike traditional military deterrence, deterrence in the cyber domain lacks clear red lines and established response thresholds, and allows a degree of anonymity. As a result, few cyberattacks have led to meaningful consequences, and major threat actors continue to exploit cyber capabilities. Therefore, active national-level responses that impose costs and ensure accountability are essential. Ultimately, response depends on national resolve, operational capacity, and coordinated action among like-minded nations. Nevertheless, continued research is needed not only to support political decisionmaking but also to foster international consensus. In addition, ensuring consistent assessments requires a dedicated agency for ongoing evaluations—as seen in the United States and United Kingdom—highlighting the need for a similar system in the ROK. Such an agency should share assessment results with stakeholders and foster a unified understanding of cyberattack severity. ■

Sunha Bae *is a senior researcher in the Cybersecurity Policy Department of the National Security Research Institute.*

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

This report is produced by the Center for Strategic and International Studies (CSIS), a private, tax-exempt institution focusing on international public policy issues. Its research is nonpartisan and nonproprietary. CSIS does not take specific policy positions. Accordingly, all

views, positions, and conclusions expressed in this publication should be understood to be solely those of the author(s).

Appendix A

ESTABLISHING ECONOMIC IMPACT BENCHMARKS

While the economic impact of cyber incidents is being studied in various fields such as cyber insurance, there is currently no established global standard. To address this gap, this study references the U.S. CISA's Cost of a Cyber Incident **report**, which systematically estimates national-level financial impacts using both commercial and research data. CISA analyzes 12 large incidents, categorizing costs as direct or indirect, and emphasizes relative costs–such as impacts compared to an organization's revenue or a nation's GDP–rather than absolute figures. However, the report acknowledges limitations, including the significant influence of outliers on total cost calculations.

Table A-1: Costs, Cost-to-Revenue Ratios, and People Affected (Large Incident Sample)

Company Affected	Year of Incident	Total Cost ($ million)	Cost-to-Revenue Ratio	Number of People Affected (millions)
Anthem	2015	375.5	0.48%	78.8
Yahoo	2014	350	7.58%	500
Merck	2017	310	0.78%	Unknown
Target	2013	292	0.41%	70
Home Depot	2014	252	0.30%	56
Sony PlayStation	2011	171	0.20%	101.6
Equifax	2017	164	4.88%	145.5
Sony Pictures	2014	43	0.06%	0.047
Experian	2015	20	0.42%	15
Yahoo	2014	16	0.34%	1000
Ashley Madison	2015	12.8	11.74%	37
LinkedIn	2012	4	0.41%	6.5

Source: Cybersecurity & Infrastructure Security Agency, *Cost of a Cyber Incident: Systematic Review and Cross-Validation* (Washington, DC: CISA, October 2020), https://www.cisa.gov/resources-tools/resources/cost-cyber-incident-systematic-review-and-cross-validation.

To analyze the economic costs and number of affected people in typical large-scale incidents while minimizing the influence of outliers, a 25 percent trimmed mean was applied. Based on this method, the trimmed mean for economic costs was calculated at $157 million, with the average number of victims at 71.99 million. Considering the approximate tenfold GDP difference and sevenfold population difference between the ROK and the United States, the threshold for large-scale incidents in the ROK can be estimated at approximately 20 billion KRW in economic cost and 10 million people affected. Therefore, the suggested thresholds for assessing the economic impact of cyberattacks in South Korea—based on financial loss and the number of individuals affected—would be as follows:

- High: Over 20 billion KRW (approx. $15.7 million) and more than 10 million individuals affected
- Medium: 5-20 billion KRW ($4-15.7 million), affecting 1-10 million individuals
- Low: Less than 5 billion KRW (around $ 4 million) and fewer than 1 million individuals

Appendix B

EXPERT SURVEY ON ASSESSMENT CRITERIA IMPORTANCE

An expert assessment using the Analytic Hierarchy Process (AHP) and the Likert method was conducted from October 24-30, 2022, to evaluate the importance of cyberattack assessment items. Experts rated each item on a 1-9 scale; nine detailed evaluation items were considered. Eleven experts in cyber law, policy, and technology (with an average experience of 18 years) participated.

Among detailed items, “importance of the damaged system” and “attack sector” were rated highest, followed by “scale of damage,” “informational impact,” “social impact,” and “attacker intent.” “Functional impact” and “recoverability” ranked slightly lower, while “attack complexity/sophistication” received the lowest importance score. Although item rankings varied slightly, overall results consistently emphasized the significance of attack targets and damage scale over technical capability.

Table B-1: Assessment Criteria Importance

Number	Importance	Ranking
Importance of the damaged system	7.989	1
Attack sector	7.951	2
Scale of damage	7.535	3
Informational impact	7.526	4
Social impact	7.521	5
Attacker intent	6.797	6
Functional impact	6.781	7
Recoverability	6.749	8
Attack complexity/sophistication	5.772	9

Source: Authors' analysis.