The Asan Institute for Policy Studies

ISSUE BRIEF Executive Summary

No. 2025-33(S)

National Position of the Republic of Korea on the Application of International Law in Cyberspace: Present and Future

Shin Sohyun
Research Fellow
2025-10-02

Implication of the National Position on the Application of International Law in Cyberspace

1. Contribution to the establishment of customary international law

Customary international law (CIL) crystallizes when state practice attains the status of *opinio juris*. The emergence of *opinio juris* may be evidenced through various manifestations, including international jurisprudence, treaty negotiations, and resolutions or declarations adopted by the United Nations General Assembly. This process of customary law formation typically unfolds over protracted periods, often spanning decades or centuries. Nevertheless, individual states may accelerate this temporal dimension through the articulation of official national positions, thereby expediting the consolidation of customary norms. This phenomenon is particularly salient in areas where normative frameworks struggle to keep pace with rapidly evolving technologies, such as cyberspace. In these contexts, states demonstrate heightened proactivity in articulating their legal positions to bridge the regulatory gap between existing normative structures and technological advancement.

2. National strategic value

The articulation of national positions provides the international community with preliminary information that enables states to gauge mutual understanding and anticipate responses regarding relevant inter-state matters. Formalized position statements serve a strategic

function by offering advance notification of states' thresholds (red lines) and anticipated levels or types of responses to actual or potential inter-state conflicts in cyberspace. The greater the specificity of national positions, the more valuable such *ex ante* information provision becomes in practical terms. However, states may also deliberately adopt ambiguous positions or eschew position-taking altogether—decisions that often reflect strategic calculations. The thirty-three national position statements published by July 2025, including that of the Republic of Korea, vary in their level of detail but cannot be characterized as comprehensively elaborated versions. While these statements generally address key areas of international law—such as sovereignty, the use of force, and state responsibility—thereby enabling an understanding of the broader framework, considerable *lacunae* remain.

3. Limitation of the national position statement

The publication of national position statements represents an ongoing process in the evolution of CIL, constituting not a singular determinative act but rather a continuous development that may evolve in response to successive changes. Such evolution may occur when states and international organizations modify their positions in accordance with shifting international dynamics, or when emerging technologies revolutionize the means and methods available to states. Nevertheless, inherent limitations persist. First, national position statements are merely declaratory, indicating how the issuing state interprets international law and intends to apply it when relevant circumstances arise, without necessarily guaranteeing definitive implementation. Second, questions may be raised regarding whether international norm-setting is possible through position statements from approximately forty states, less than half of the 193 UN member states. In response to this challenge, institutions including the NATO Cooperative Cyber Defence Centre of Excellence (NATO CCDCOE) and the UN Institute for Disarmament Research (UNIDIR), along with regional international organizations (ASEAN, OSCE, OAS, among others), have undertaken initiatives to encourage states' development and publication of positions via guidelines and training programs for practitioners. Third, the national position statements published by July 2025 predominantly articulate general positions on the applicability of broad categories of international law, while the specific application of international law to actual or potential scenarios in cyberspace remains subject to interpretative reservation.

Critical Analysis of the National Position of the Republic of Korea

The Government of the Republic of Korea maintains the fundamental position that international norms and CIL generally recognized by the international community, including the UN Charter, should apply equally to cyberspace. The Korean Government has articulated six domains of public international law as applicable to cyberspace: sovereignty and the principle of non-intervention, the prohibition on the use of force, the right to self-defence,

the law of state responsibility, international humanitarian law, and international human rights law.

1. Sovereignty and non-intervention

The Korean government takes the position that the principle of sovereign equality and its derivative principles—namely, the peaceful settlement of disputes, the prohibition of the threat or use of force, and the principle of non-intervention in domestic affairs—are deemed applicable to state activities in cyberspace. Based on the territorial jurisdiction inherent in sovereignty, states exercise jurisdiction over cyber infrastructure located within their territory, persons conducting cyber activities within their territory, and such cyber activities themselves. The Korean government considers that a sovereignty violation occurs when another state gains unauthorized access to or intrudes upon its cyberspace or infrastructure. However, it has not definitively articulated whether such violations constitute wrongful acts of sufficient gravity to warrant countermeasures or the invocation of state responsibility, or whether they merely represent breaches of the sovereignty principle.

2. Prohibition of the use of force and self-defence

The Korean government takes the position that the prohibition of use or threat of force and the right of self-defence apply with equal effect to activities conducted in cyberspace. The determination of whether cyber activities constitute a use of force requires a comprehensive assessment of factors, including the consequences, character, actors, and targets of such conduct. *Prima facie*, specific cyber activities that produce physical effects comparable to those resulting from a kinetic use of force under international law may be characterized as a use of force. Furthermore, an armed attack represents the gravest form of the use of force. The Korean government also needs to consider in the future whether the loss of original functionality can lead to the use of force. Future position statements should explicitly clarify that the exercise of self-defense in response to cyberattacks need not be confined to cyber means alone but may encompass kinetic responses. Additionally, it is necessary to consider whether the right of self-defense may be invoked against cyber-armed attacks perpetrated by non-state actors, such as terrorist organizations.

3. State responsibility

The Korean government determines attribution when cyber activities amounting to internationally wrongful acts occur through a comprehensive analysis based on available evidence, incorporating technical and legal analysis of the relevant activities as well as an assessment of intent. The law of state responsibility concerning attribution and due diligence also applies to cyber activities. States with well-developed cyber infrastructure and advanced cyber capabilities, such as South Korea, consequently bear heightened due diligence obligations, necessitating inter-ministerial policy coordination that reflects the nation’s specific circumstances.

4. International human rights law

The Korean government maintains that international human rights law applies online as it does offline. Fundamental human rights in cyberspace, including the right to privacy, freedom of expression, the right to access information, non-discrimination, and prevention of hate speech, must be guaranteed for all persons, including women and vulnerable groups. In the future, position statements may advance beyond declaratory levels to articulate that states, when pursuing legislation or policies governing cyberspace, should undertake assessments to ensure compliance with international human rights law, including examination of potential restrictions on fundamental rights.

5. International humanitarian law

The Korean government takes the position that international humanitarian law applies when armed conflict arises from cyber activities. The fundamental principles of international humanitarian law, including the principle of distinction, proportionality, and precautions, must be observed. Given that cyberattacks possess inherent characteristics requiring clandestine and surprise execution to achieve strategic objectives, it is necessary to further examine whether implementing precautions in cyberattack is feasible for civilian-protection purposes.

Recommendations for the Future National Position

While the Korean government's initial official position statement may be considered somewhat belated, it has actively participated in and engaged with relevant international organizations' discussions and cyber-related matters in the international community. Following this deliberately measured initial national position statement, more proactive articulation and participation should be sustained. The format of such articulations need not take the form of comprehensively updated national position statements. When deemed necessary in specific areas, national positions may be developed through various modalities, including speeches by the Minister of Foreign Affairs or position announcements during discussions at the forthcoming permanent "Global Mechanism on Developments in the Field of ICTs in the Context of International Security and Advancing Responsible State Behavior in the Use of ICTs." The government may modify its positions on the aforementioned principal areas of international law or articulate more evolved interpretations. The articulation of national positions must also be reflected in the concrete practice of the Korean government. Through such alignment, the Korean government's official pronouncements can garner the trust of the international community.

About the Author

Dr. Shin Sohyun is a research fellow in the Centre for Foreign Policy and National Security at the Asan Institute for Policy Studies. Her research mainly focuses on the international norm change and progress in the new spaces: cyberspace and outer space following the development of emerging technologies such as ICT, AI, space technology and quantum computing, etc. Dr. Shin has interests in interdisciplinary and socio-legal research combining new technologies and law and policy relating to armed conflict, military operations, weapons, cyber espionage and intelligence as well as disaster, environment and human rights. She was the founding member of Sejong Institute Cybersecurity Centre(2020-2022) and organised 'Cybersecurity Forum'. She worked as a research fellow of Korea University Institute of Cyber Security & Privacy. Dr. Shin published "The Regulation of State's Hostile Disinformation Operations in Cyberspace", "Space Security and International Law", and "Cyber Deterrence and US Defence Forward Strategy in International Law", etc.

This article is an English Summary of Asan Issue Brief (2025-29).
('사이버 공간에서의 국제법 적용에 관한 한국 정부 입장의 현재와 미래')