NOTE

# Countering North Korea's Hybrid Warfare: A Framework of International Law and Technological Strategies for Digital and Physical Threats

Seawon Inn†



† Seawon Inn is a J.D. Candidate at Cornell Law School.

**Introduction**

In recent months, North Korea's international influence has taken an assertive turn. Reports of North Korea's deployment of troops to assist Russia in the ongoing Ukraine conflict signal a strategic alliance shift and reflect a broader global realignment.[1] This unexpected action has amplified concerns in the international community, bringing renewed urgency to the issue of North Korean sanctions enforcement. Although the direct impact of North Korean troops on the conflict remains uncertain, the gesture itself underscores North Korea's willingness to actively engage in major global conflicts.[2]

In response, Ukraine has urged its allies to impose additional sanctions on North Korea, demonstrating the global significance of Pyongyang's involvement in the conflict.[3] Sanctions have historically aimed to limit North Korea's nuclear capabilities and economic resources by taking measures such as freezing the assets of people involved in its nuclear program and restricting scientific cooperation.[4] However, these have proven insufficient to counter the regime's sophisticated and evolving sanctions evasion strategies, which now include both physical and cyber-based methods. These strategies enable North Korea to sidestep traditional sanctions while financing its military and nuclear programs with relative ease, thus undermining international containment efforts.

Alongside its military support, North Korea has expanded its cyber capabilities and the use of artificial intelligence (AI) to exploit weaknesses in digital finance. Indeed, North Korea has continued to use advanced cyber capabilities to support its economic and military goals, evidenced by a string of cyberattacks on cryptocurrency firms that United Nations sanctions monitors estimate have netted the regime approximately $3.6 billion between 2017 and 2024.[5] These illicit gains, often funneled into North Korea's military programs and overseas operations, exemplify how the regime uses decentralized financial technologies to fund its initiatives, effectively bypassing traditional sanctions. Moreover, such capabilities can allow North Korea to support allied nations, such as Russia, indirectly through intelligence sharing and disruptive operations, extending its influence in ways that sanctions have not managed to curb.

In response to changing landscapes of cyberattacks, many States have been trying to deal with the problem by revising their cybersecurity policies to bolster their defenses against state-sponsored cyberattacks. For instance, South Korea released a comprehensive revised National Cybersecurity Strategy last

1. *See* Andrew Yeo & Hanna Foreman, *What Do North Korean Troop Deployments to Russia Mean for Geopolitics?*, Brookings Inst. (2024).

2. *See id.*

3. *Ukraine calls for sanctions over alleged North Korean involvement in war*, Reuters (Oct. 16, 2024), https://www.reuters.com/world/zelenskiy-says-nkorea-is-de-facto-taking-part-war-russias-side-2024-10-16/ [https://perma.cc/9H28-R9CK].

4. *What to Know About Sanctions on North Korea*, Council on Foreign Rels. (2022), https://www.cfr.org/backgrounder/north-korea-sanctions-un-nuclear-weapons [https://perma.cc/YDK7-UFVR].

5. Michelle Nichols, *North Korea Laundered $147.5 Mln in Stolen Crypto in March, Say UN Experts*, Reuters (May 14, 2024), https://www.reuters.com/technology/cybersecurity/north-korea-laundered-1475-mln-stolen-crypto-march-say-un-experts-2024-05-14/ [https://perma.cc/AJ4E-9TH3].

February, which emphasizes proactive defense mechanisms and international cooperation to combat escalating cyber threats from North Korea's policy adjustments.[6] South Korea's strategy reflects a broader trend toward collaborative digital defense frameworks that seek to address the limitations of unilateral sanctions by creating a more cohesive and responsive international strategy.[7]

This Note argues that conventional sanctions alone are inadequate in addressing North Korea's modernized evasion tactics, which employ a hybrid approach combining military support with AI-enabled cyber warfare. Aggressive, one-size-fits-all sanctions are no longer effective against hybrid threats that adapt to sanctions in real time, often with the help of advanced technological tools. Instead, a collaborative, standardized sanctions framework could offer a more effective approach. By building a global manual, the international community could establish standardized guidelines and processes for sanctions enforcement, enabling States to collaborate effectively to detect and respond to sanctions breaches as they occur. Such a framework would encourage international alignment, facilitating shared responsibilities in monitoring, regulating, and responding to unconventional threats.

Indeed, this suggestion aligns with recent initiatives by multilateral coalitions, such as the United States-led International Counter Ransomware Initiative (CRI), which aims to build collective resilience against ransomware and cyber threats through collaboration among sixty-eight member States.[8] The CRI has emphasized the importance of supporting member nations' cybersecurity capabilities through rapid response assistance and targeted investments in cybersecurity skills.[9]

As conflicts increasingly incorporate digital assets, artificial intelligence, and hybrid warfare tactics, a modernized sanctions framework will be crucial in ensuring that sanctions regimes can respond effectively to nontraditional threats. Addressing North Korea's case specifically offers an opportunity to set a precedent for a proactive, collaborative approach, making it more resilient in the face of technological advances and shifting geopolitical alliances.

## I. Background: The Evolution of Sanctions and Cybersecurity

### A. Sanctions as a Strategic Tool

In economic theory, "sanctions" refer to the deliberate withdrawal or threat of withdrawal of customary trade or financial relations between the sanctioning State (sender) and the targeted State (target).[10] Traditional sanctions

6. Tae Yeon Eom, *AI and Cybersecurity in Digital Warfare on the Korean Peninsula*, Geo J. Int'l Affs. (2024), https://gjia.georgetown.edu/2024/07/10/ai-and-cybersecurity-in-digital-warfare-on-the-korean-peninsula/ [https://perma.cc/ZB4K-N7ZD].

7. *Id.*

8. *International Counter Ransomware Initiative 2024 Joint Statement,* The White House (2024), https://www.whitehouse.gov/briefing-room/statements-releases/2024/10/02/international-counter-ransomware-initiative-2024-joint-statement/ [https://perma.cc/L9JM-ZYPK].

9. *Id.*

10. Vera Rusinova & Ekaterina Martynova, *Fighting Cyber Attacks with Sanctions: Digital Threats, Economic Responses,* 57 Isr. L. Rev. 135, 139 (2024).

include measures like embargoes, tariffs, and export/import restrictions, while financial sanctions may involve freezing assets or halting loans.[11] Despite being predominantly economic or financial, sanctions can also target individuals through measures like travel bans.[12] Modern perspectives view sanctions less as purely economic devices and more as politically-motivated tools aimed at influencing State decision-making, often extending to private actors connected to the target government.[13]

As the nature of global threats evolves, so too has the use of sanctions. States have responded to cyberattacks by implementing sanctions, expelling diplomats, issuing criminal indictments under domestic law, and rarely but sometimes openly announcing that it is "hacking back."[14] From a legal standpoint, State sanctions in response to cyber operations can fall into two categories: countermeasures or retorsions.[15] Countermeasures are actions taken by an injured State to compel the offending state to fulfill its international obligations, provided the cyber operation constitutes a breach of international law.[16] These measures must adhere to principles such as proportionality, reversibility, and notification, and the wrongful act must be ongoing.[17] Retorsions, on the other hand, involve lawful but unfriendly acts taken in response to an unfriendly act and do not require the triggering cyber operation to violate international law.[18] These measures, such as severing diplomatic relations or withdrawing voluntary aid, are considered a freedom rather than a right and are largely unregulated by international law.[19]

Building on these evolving sanction practices, the European Union (EU) has increasingly adopted targeted sanctions to address specific crimes, including cyberattacks, terrorism, and human rights violations.[20] These "smart sanctions" focus on individuals or entities, and often include travel bans and asset freezes, which tend to minimize broader societal impact.[21] For instance, the EU has implemented the Global Human Rights Sanctions Regime, which targets individuals and entities responsible for serious human rights violations, including crimes against humanity, torture, and suppression of freedoms.[22] Similarly, the EU has adopted measures to combat cyberattacks through its cyber sanctions regime, targeting individuals and entities involved in malicious cyber activities threatening EU security. The EU's restrictive measures against

11. *Id.*
12. *Id.*
13. *See id.*
14. *Id.* at 136.
15. *Id.* at 142.
16. *Id.*
17. *Id.*
18. *Id.*
19. Tom Ruys, Sanctions, *Retortions and Countermeasures: Concepts and International Legal Framework*, *in* Research Handbook on UN Sanctions and International Law 19, 24-5 (Larissa van der Herik ed., 2017).
20. Yuliya Miadzvetskaya, *EU Sanctions in Response to Cyber-Attacks as Crime-Based Emergency Measures*, 54 Comput. L. & Sec. Rev. (2024).
21. *Id.*
22. Strategic Communications, *European Union Sanctions*, Dipl. Serv. Eur. Union (2023), https://www.eeas.europa.eu/eeas/european-union-sanctions_en [https://perma.cc/SH3X-LUWW].

cyberattacks, introduced in Council Decision (CFSP) 2019/797 and Regulation (EU) 2019/796, target persons or entities responsible for significant cyber-attacks threatening the EU or its Member States.[23] These measures include freezing assets and banning sanctioned individuals from traveling to the EU.[24] Notably, these sanctions address cyberattacks impacting critical infrastructure, public elections, and essential services like healthcare and banking.[25] This targeted approach reflects a shift toward individualized foreign policy, aligning with evolving legal bases and global trends in sanctions practices.[26]

Sanctions by other actors, including the United States, the United Nations, and individual States, also demonstrate diverse application of this mechanism.[27] While their implementations vary across jurisdictions, these measures are generally framed to ensure accountability while minimizing harm to innocent populations. By continuing to refine and adapt these measures, the international community will be able to better address emerging challenges while upholding the principles of justice and security.

## B. The Rise of Hybrid Warfare and Cyber Threats

### *1. Hybrid Warfare*

The term "hybrid warfare" was first popularized by Frank Hoffman, who defined it as "a range of different modes of warfare, including conventional capabilities, irregular tactics and formations, terrorist acts including indiscriminate violence and coercion, and criminal disorder."[28] Hybrid warfare integrates traditional military strategies with cyber operations, economic coercion, disinformation, and other non-traditional tactics.[29] These methods, often conducted in the gray zone between war and peace, complicate the application of traditional international legal frameworks designed to govern State conflicts.[30]

The concept of hybrid warfare gained significant attention after the 2014 conflict in Ukraine, where Russia's use of hybrid tactics, including disinformation campaigns and covert military operations, exposed the limitations of conventional military doctrines.[31] While Russia's 2008 war with Georgia hinted at early signs of such strategies, international security discussions at the time were dominated by counterinsurgency efforts in Afghanistan.[32] These largely

23. *EU restrictive measures against cyber-attacks*, EUR-Lex (2022), https://eur-lex.europa.eu/EN/legal-content/summary/eu-restrictive-measures-against-cyber-attacks.html [https://perma.cc/N566-KAK4].
24. *Id.*
25. *Id.*
26. *See* Miadzvetskaya, *supra* note 20.
27. *See* Rusinova & Martynova, *supra* note 10.
28. Frank G. Hoffman, Conflict in the 21st Century: The Rise of Hybrid Wars, (Potomac Inst. Pol'y Stud., 2007).
29. *North Korea Cyber Group Conducts Global Espionage Campaign to Advance Regime's Military and Nuclear Programs*, Cybersec. & Infrastructure Sec. Agency [CISA] (July 25, 2024), https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-207a [https://perma.cc/9EVH-RQ4D].
30. *Id.*
31. Andrew Mumford & Pascal Carlucci, *Hybrid Warfare: The Continuation of Ambiguity by Other Means*, 8 Eur. J. of Int'l Sec. 192, 195 (2023).
32. *See id.*

overlooked developments culminated in Russia's innovative use of hybrid warfare tactics in Ukraine, which brought the concept to the forefront of international security discourse.[33] Moreover, the growing prevalence of hybrid warfare is not limited to Russia. Other States and non-state actors have adopted similar approaches, exploiting technological advancements and global interconnectivity to achieve strategic objectives without triggering a formal declaration of war.

One of the defining features of state-led hybrid warfare is its strategic use of ambiguity.[34] Tactics such as cyberattacks, disinformation, and the use of proxies are designed to operate below the threshold of conventional war, complicating their attribution and responses to them.[35] This ambiguity allows State actors to exploit vulnerabilities in liberal democracies, where decentralized decision-making often delays coordinated responses.[36]

### *2. Cyberattacks*

A key dimension of hybrid warfare is the integration of cyber operations, often referred to as the "fifth dimension" of conflict.[37] Cyber weapons provide a means of targeting critical infrastructure, financial systems, and information networks, enabling states to weaken their adversaries without overt military confrontation. For example, in hybrid conflicts, attackers frequently target commercial sectors like banking and telecommunications, where disruptions cause not only immediate financial losses but also reputational harm.[38]

Cyberattacks have thus become a cornerstone of hybrid warfare, utilized by both State and non-state actors to achieve strategic objectives. According to Council on Foreign Relations' cyber operations tracker, thirty-four countries are suspected of sponsoring cyber operations since 2005.[39] Among them, China, Russia, Iran, and North Korea sponsored 77 percent of all suspected operations.[40] In 2019, there were a total of seventy-six operations, most being acts of espionage. One prominent example is North Korea's state-sponsored cyber campaigns, which target critical infrastructure and leverage both cyber espionage and ransomware attacks.[41] These operations not only advance North Korea's military and nuclear ambitions but also serve as a significant source of revenue for its regime.[42] Such strategies exemplify how States can employ cyber tools

33. *Id.*

34. Erik Reichborn-Kjennerud & Patrick Cullen, *What Is Hybrid Warfare?*, Nor. Inst. Int'l Affs. (2016), https://nupi.brage.unit.no/nupi-xmlui/bitstream/handle/11250/2380867/NUPI_Policy_Brief_1_Reichborn_Kjennerud_Cullen.pdf [https://perma.cc/P8KK-PMMC].

35. *Id.*

36. *Id.*

37. *See* David Lonsdale, *Information Power: Strategy, Geopolitics, and the Fifth Dimension* 22 The J. of Strategic Stud. 137 (1999).

38. *See* Mikhael Dobryshin et al., Simulation of the Conflict of the Opposing Sides in the Conditions of the Introduction of Hybrid Warfare with the Use of Cyber Weapons (2023).

39. *Cyber Operations Tracker,* Council on Foreign Rels., https://www.cfr.org/cyber-operations/ [https://perma.cc/BRG9-2JGN].

40. *Id.*

41. *North Korea Cyber Group Conducts Global Espionage Campaign to Advance Regime's Military and Nuclear Programs*, CISA (2024), https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-207a [https://perma.cc/G74M-9BTH].

42. *Id.*

to achieve a range of objectives from destabilizing adversaries to funding State operations.

However, the use of cyber weapons is not limited to state actors. Non-state actors, including terrorist organizations, have long leveraged cyber capabilities to expand their influence and reach. [43] These groups use cyber tools for recruitment, propaganda, and the disruption of adversarial systems, challenging traditional notions of battlefield engagement.[44]

Meanwhile, cyberattacks pose unique challenges that differentiate them from traditional forms of attack, which are generally observable and traceable. Florian J. Egloff and Max Smeets, in their article *Publicly Attributing Cyber Attacks: A Framework*, explore the complexities States face in publicly attributing cyber intrusions.[45] In it, they develop a Public Attribution Framework to assist states in navigating the challenges of such decisions.[46] The authors argue that public attribution is not a straightforward process, but rather involves balancing multiple considerations, including understanding the attributed cyber operation, identifying the threat actor, analyzing the geopolitical environment, assessing allied positions, and considering the legal context.[47] This multifaceted process helps explain why attribution remains contested and why state responses, including sanctions, often lack speed and consistency.

#### *3. The Evolving Threat Landscape*

The complexity of hybrid warfare and cyber operations highlights the inadequacy of traditional responses. Cyberattacks complicate the line between acts of war and criminal activity, making attribution and accountability difficult. This evolving landscape necessitates robust international cooperation and adaptive cybersecurity frameworks to mitigate growing threats.

## II. Challenges with Existing Sanctions Frameworks

### A. Gaps in International Legal Frameworks

As North Korea continues to expand its cyber capabilities, exploiting the vulnerabilities in global systems for strategic and financial gain, the international community faces significant challenges in applying existing legal frameworks to this evolving domain. The contested application of international law to cyberspace highlights critical gaps that undermine efforts to hold States accountable for malicious cyber operations.[48]

---

43. Erik Reichborn-Kjennerud & Patrick Cullen, *What Is Hybrid Warfare?*, Nor. Insti. Int'l Affs. (2016), https://nupi.brage.unit.no/nupi-xmlui/bitstream/handle/11250/2380867/NUPI_Policy_Brief_1_Reichborn_Kjennerud_Cullen.pdf [https://perma.cc/V2LE-E2Y5].
44. *Id.*
45. Florian Egloff & Max Smeets, *Publicly Attributing Cyber Attacks: A Framework*, 46 J. Strategic Stud. 502 (2023).
46. *See id.*
47. *Id.*
48. *See* Rusinova & Martynova, *supra* note 10.

### *1. Traditional Challenges*

Key challenges often come from different understandings of foundational concepts and boundaries in international law. This includes disagreements over whether sovereignty is a binding rule or a principle, with States like France adopting a broad interpretation while others, like the United States and the United Kingdom, limit its scope.[49] Accordingly, the principle of non-interference is widely accepted but remains underinclusive in addressing cyber operations, relying on abstract criteria like coercion and interference in a State's reserved domain, which are often inadequate for the complexities of cyberspace.[50]

The absence of established agreements, coupled with ambiguities in international law, creates a cycle in which States fail to acknowledge the authority of international law over cyber conduct. In their article *Accusations and International Law in Cybersecurity,* Martha Finnemore and Duncan B. Hollis explore the growing trend of States accusing others of misconduct in cyberspace, noting that such accusations rarely lead to behavior change or acknowledgment from the accused.[51] The authors argue that these accusations often lack reference to international law, highlighting its perceived weakness or irrelevance in holding States accountable for cyber operations.[52]

### *2. Emerging Challenges*

If these traditional uncertainties already constrain effective governance, the rise of hybrid warfare poses an even more complex layer of challenges. Current international legal norms, particularly those outlined in frameworks like the United Nations Charter and customary international law, struggle to address the blurred boundaries of hybrid warfare. Traditional notions of state sovereignty and the laws governing armed conflict fail to capture the complexities of cyber espionage and ransomware campaigns. Furthermore, the lack of standardized definitions for acts of aggression in cyberspace, coupled with inconsistent international cooperation, impedes the development of a robust legal regime to effectively combat hybrid threats.

The rise of new technologies, such as blockchain, introduces additional complexities for regulatory frameworks addressing hybrid threats. Blockchain in particular exemplifies the regulatory challenges posed by emerging technologies due to three major issues: decentralization, jurisdictional complexities, and anonymity leading to identification challenges.[53] Specifically, blockchain's decentralized nature complicates enforcement by removing central authority,

49. *Id* at 145-46.

50. *Id* at 146.

51. Martha Finnemore & Duncan B. Hollis, *Beyond Naming and Shaming: Accusations and International Law in Cybersecurity*, 31 Eur. J. Int'l L. 969 (2020).

52. *Id.*

53. For the general discussion of the relationship between blockchain technology relates to regulations, *see* Thomas Richter, *Regulatory Aspects of Blockchains*, *in* International Handbook of Blockchain Law: A Guide to Navigating Legal and Regulatory Challenges of Blockchain Technology and Crypto Assets 91 (2 ed. 2024).

fragmenting jurisdictional determinations and accountability.[54] This decentralization evolves over time, further complicating oversight.[55] Additionally, the transnational scope of blockchain networks lacks clear regulatory anchors, necessitating international cooperation to address the jurisdictional complexities that necessarily arise.[56] Anonymity adds another layer of difficulty, particularly for enforcing anti-money laundering laws and ensuring compliance in financial services.[57] In this context, balancing privacy with effective identification mechanisms remains a critical hurdle,[58] which illustrates the need for globally coordinated and adaptable regulatory frameworks.

The enforcement challenges posed by blockchain technologies underscore that traditional sanctions are insufficient in the face of North Korea's hybrid tactics, which combine military support for conflicts like the one in Ukraine with AI-enhanced cyber warfare and cryptocurrency-based sanctions evasion. Addressing these threats requires more than incremental adjustments. What is needed is a collaborative, standardized sanctions framework, focused on real-time digital tracking, international regulatory coordination, and AI-supported analysis, as a more effective alternative.

### B. North Korea's Cyber Threats: A Multifaceted Challenge

North Korea's cyber program represents a unique and alarming blend of State and non-state actor characteristics. Isolated from the international community and maintaining limited diplomatic relations, its regime has turned to cyber threats as an alternative means to achieve its political, military, and economic objectives.[59] As outlined in South Korea's Institute of Foreign Affairs and National Security (IFANS)' report, North Korea's objectives include: crippling adversaries' statecraft, interfering with military operations, securing finances, instigating social conflict, stealing strategic information, and propagandization.[60] This comprehensive use of cyber threats underscores the regime's strategic reliance on digital tools to assert its influence on the global stage.

#### *1. Capabilities*

North Korea's cyber capabilities have evolved into a formidable instrument of State power, blending espionage, sabotage, and financial crime into a unified strategy that poses significant global risk. The 2024 Annual Threat Assessment by the Office of the Director of National Intelligence (ODNI) highlights the growing danger of North Korea's cyber program, describing it as a

54. *Id.*
55. *See id.*
56. *See id.* (noting "[i]n the case of public blockchains, there is no 'root' in any specific country which could be the starting point to determine jurisdiction and applicable law and no 'anchor' which could serve as a regulatory entry point from the pure technological perspective of the blockchain as such.")
57. *Id.*
58. *See id.*
59. Tae-Eun Song, Inside Pyongyang's Mind: An Overview of the Kim Regime's Persistence in Masterminding Illicit Cyber Activities and ROK's Responses (2023).
60. *Id.* at 2-3.

"sophisticated and agile espionage, cybercrime, and attack threat."[61] According to the report, Pyongyang's cyber forces have matured significantly, enabling them to achieve a variety of strategic objectives against a diverse range of targets, particularly in the United States and South Korea.[62] To this end, it is believed that North Korea has been addressing a large part of its fiscal shortfalls through hacking since 2020.[63] Indeed, according to the National Cyber Power Index (NCPI) of the Belfer Center, North Korea ranks first in financial category of cyber capabilities.[64]

At the core of North Korea's cyber operations is the Reconnaissance General Bureau (RGB), the regime's primary intelligence agency,[65] which reports directly to the State Affairs Commission.[66] Among its divisions, the 3rd Bureau, operating through groups like Andariel (also known as Onyx Sleet and DarkSeoul), exemplifies hybrid warfare in cyberspace.[67] These actors exploit vulnerabilities in public-facing systems and deploy sophisticated tools such as remote access trojans (RATs), custom malware implants, and phishing campaigns to infiltrate sensitive sectors, including the defense, aerospace, and nuclear industries.[68] Additionally, ransomware campaigns targeting U.S. healthcare systems have been linked to funding North Korea's military initiatives, showcasing how cyber operations directly support physical capabilities.[69]

### *2. High-Profile Cyber Operations*

North Korea's cyber activities have become increasingly bold and impactful. Recently, they tend to focus on ransomware attacks that lock or encrypt key systems and demand money, holding those systems as hostages. This reflects a turn of North Korea's cyber operations focus from infrastructure paralysis and information theft to cryptocurrency theft.[70] For instance, the Lazarus Group stole nearly $100 million in cryptocurrency from the platform Harmony Bridge in June 2022.[71] The FBI formally attributed the hack to

61. 2024 ODNI Ann. Threat Assessment of the U.S. Intel. Cmty.

62. *Id.*

63. Taehyun Kim, *North Korea's Complex Strategy to Avoid Comprehensive Sanctions*, 8 Kor. Rsch. Inst. Nat'l Strategy 27, 41(2023).

64. Julia Voo et al., National Cyber Power Index 2022, at 11 (2022), *cited in* Taehyun Kim, *North Korea's Complex Strategy to Avoid Comprehensive Sanctions*, 8 Kor. Rsch. Inst. Nat'l Strategy 27, 41(2023).

65. Andrei Lankov, *On the Great Leader's Secret Service: North Korea's Intelligence Agencies*, NK News (May 1, 2017), https://web.archive.org/web/20180731080639/https://www.nknews.org/2017/05/on-the-great-leaders-secret-service-north-koreas-intelligence-agencies/ [https://perma.cc/YH6Z-AEA9].

66. *Id.*

67. *North Korea Cyber Group Conducts Global Espionage Campaign to Advance Regime's Military and Nuclear Programs*, CISA (2024), https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-207a [https://perma.cc/WB36-B969].

68. *Id.*

69. *Id.*

70. Jahee Kim & Kyungmin Lee, *Revisiting International Legal Response to North Korea's Cryptocurrency Heist: Enhancing Cyber Deterrence through Hacking-Back*, 142 The Q. J. Defen. Pol'y Stud. 33, 40 (2024).

71. *Cyber Operations Tracker,* Council on Foreign Rels., https://www.cfr.org/cyber-operations/ [https://perma.cc/BRG9-2JGN]

Lazarus in January 2023 after the hackers attempted to launder nearly $60 million through cryptocurrency mixers and a series of wallets.[72]

Similarly, Andariel, another RGB-linked group, has been involved in ransomware campaigns that specifically targeted U.S. hospitals and healthcare providers.[73] According to Cybersecurity and Infrastructure Security Agency (CISA), North Korea has launched ransomware campaigns against Healthcare and Public Health Sector (HPH) organizations and other critical infrastructure sector entities.[74] Using custom-developed malware like "Maui," these attacks disrupted critical healthcare services by encrypting networks and demanding cryptocurrency ransoms.[75] The ransomware payments were then laundered through Chinese facilitators, with proceeds used to fund further cyber intrusions into defense and technology organizations globally.[76] These activities, which included attacks on U.S. Air Force bases, NASA, and international defense contractors, resulted in the theft of terabytes of sensitive data, such as old technical data on military aircraft, intellectual property, and limited technical information concerning maritime and uranium processing projects.[77]

### *3. Financing Military Ambitions and Circumventing Sanctions*

Although smart sanctions are the trend worldwide, North Korea presents a notable exception. While UN sanctions against North Korea have been imposed since Resolution 2270 of the 2016 Security Council Regarding the development of nuclear and WMD programs, the nature of these sanctions has changed from "targeted" (or smart sanctions) to "comprehensive sanctions" that hit the entire North Korean economy.[78] When North Korea conducted its fourth nuclear test in March 2016, the international community adopted UNSCR Resolution 2270 to take extreme measures to ban the import of minerals such as anthracite and iron from North Korea and to ban the export of aviation fuel.[79]

However, despite long-term sanctions against North Korea, the North Korean regime still appears to be enduring under strain.[80] Above all, the 'totalitarian resistance' based on the internal characteristics of the North Korean

72. *Id.*
73. *North Korean Government Hacker Charged for Involvement in Ransomware Attacks Targeting U.S. Hospitals and Health Care Providers*, Off. Pub. Affs. (July 25, 2024), https://www.justice.gov/opa/pr/north-korean-government-hacker-charged-involvement-ransomware-attacks-targeting-us-hospitals [https://perma.cc/M9HF-7AC6].
74. *North Korea Cyber Threat Overview and Advisories*, CISA, https://www.cisa.gov/topics/cyber-threats-and-advisories/advanced-persistent-threats/north-korea [https://perma.cc/V7CD-YACQ].
75. *North Korean Government Hacker Charged for Involvement in Ransomware Attacks Targeting U.S. Hospitals and Health Care Providers*, Off. Pub. Affs. (July 25, 2024), https://www.justice.gov/opa/pr/north-korean-government-hacker-charged-involvement-ransomware-attacks-targeting-us-hospitals [https://perma.cc/N7TE-BRFZ].
76. *Id.*
77. *Id.*
78. Kim, *supra* note 63, at 28.
79. *Id.*
80. *Id.* at 29.

system acts as a driving force for North Korea's long-term survival.[81] While comprehensive international sanctions cause enormous damage to the livelihoods of ordinary people, they also serve as an opportunity for the North Korean regime to strengthen its control over the people.[82]

Cyber operations have become central to this survival strategy. Beyond espionage and sabotage, they are critical for financing the regime's economy and military programs. Historically, North Korea has relied on illegal activities such as drug production, wildlife smuggling, and counterfeiting to offset the economic losses caused by international sanctions.[83] However, as sanctions have intensified through methods such as freezing its assets and as access to foreign exchange markets became extremely restricted,[84] conditions exacerbated by border closure during the COVID-19 pandemic, North Korea has expanded its criminal activities into cyberspace.[85]

Since the late 2010s, the theft of virtual assets has become central to North Korea's economic strategy.[86] By 2022, North Korean cybercrime organizations had stolen an estimated $1.65 billion in cryptocurrency, accounting for 43.4% of the global total stolen that year.[87] These funds, combined with revenue from other illegal exports, amounted to $2.3 billion in foreign currency income in 2022, as noted by the UN Security Council Sanctions Committee.[88] To put this in perspective, North Korea's total exports in 2020 were only $142 million, underscoring how cybercrime has become a primary driver of the nation's economy.[89]

### *4. Accountability under International Law*

While North Korea is already heavily sanctioned for its illicit activities, holding the regime accountable for its cyberattacks presents distinct challenges due to the nature of these threats. According to the United Nations Group of Governmental Experts (GGE) on cybersecurity, which reflects State views and practices on cybersecurity issues, International Law Commission's Articles on Responsibility of States for Internationally Wrongful Acts (ILC Articles) provide an important legal framework applicable to cyberattacks by States and non-state actors.[90] The ILC Articles outline that a State's internationally wrongful act consists of an action or omission that is: (a) attributable to the State under international law; and (b) constitutes a breach of an international obligation of the State.[91] Additionally, Article 1 states that "Every internationally wrongful

81. *Id.*
82. *Id.*
83. Song, *supra* note 59.
84. *Id.* at 3.
85. Kim, *supra* note 63, at 41.
86. Song, *supra* note 59.
87. *Id.*
88. *Id.*
89. *Id.* at 4.
90. *See* Kim & Lee, *supra* note 70, at 42.
91. Int'l L. Comm'n, *Responsibility of States for Internationally Wrongful Acts*, 2 Y.B. 76, U.N. Doc. A/CN.4/SER.A/2001/Add.1 2001 at art. 2 [hereinafter Int'l L. Comm'n, *Responsibility of States*].

act of a State entails the international responsibility of that State."[92] Thus, if the cryptocurrency thefts committed by hacker groups such as Lazarus are found to be attributable to North Korea as a State and constitute a breach of its international obligations, then North Korea would bear State responsibility for these internationally wrongful acts.[93]

Since the hacker organizations such as the Lazarus Group, BlueNoroff, and Andariel are de facto State organs of North Korea,[94] their conduct is attributable to North Korea under Article 4 of the ILC Articles, which states that an act is attributable to a State if it is committed by State organs.[95] Additionally, Article 8 of the ILC Articles specifies that acts committed by individuals or groups can be attributed to a State if they are carried out under the direction or control of that State.[96] As evidence consistently points to North Korea's active involvement in directing and supporting these hacker groups, there is a strong basis that North Korea bears State responsibility for its internationally wrongful acts.

## III. Solution: A Comprehensive Framework to Counter North Korea's Hybrid Threats

To effectively address North Korea's hybrid tactics, the international community must implement a forward-looking framework that integrates sanctions enforcement, cybersecurity, and legal innovation. Traditional approaches have fallen short in countering the regime's evolving methods, particularly its sophisticated cyber operations and cryptocurrency exploitation. A modernized solution must combine international collaboration, advanced technological tools, and adaptive legal mechanisms to mitigate these threats effectively.

### A. Collaborative Sanctions Framework

Traditional sanctions, which primarily target physical assets and state-controlled entities, fail to address decentralized and rapidly evolving cyber strategies. Sanctions must evolve to focus on the digital domain, targeting the financial mechanisms North Korea exploits. Thus, the international community should develop a unified sanctions enforcement manual tailored to hybrid threats. This manual should standardize enforcement protocols across jurisdictions, include best practices for monitoring cyber activities and cryptocurrency transactions, and establish channels for real-time collaboration among States and organizations.

Existing treaties, such as the Budapest Convention on Cybercrime, offer valuable guidance for this effort. The Convention's emphasis on cross-border cooperation and harmonized legal approaches serves as a strong foundation

92. Int'l L. Comm'n, *Responsibility of States*, art. 1.
93. Kim & Lee, *supra* note 70, at 42.
94. *See id.* at 46.
95. Int'l L. Comm'n, *Responsibility of States*, art. 4.
96. Int'l L. Comm'n, *Responsibility of States*, art. 8.

for updated enforcement strategies.[97] For example, its procedural tools for data preservation and evidence sharing could be adapted to track cryptocurrency theft and other digital crimes.[98]

In addition to enhancing existing frameworks, new international agreements should focus on regulating decentralized technologies, strengthening anti-cybercrime measures, and promoting collaborative enforcement mechanisms. Indeed, the escalating frequency and impact of cyberattacks underscore the urgency of these efforts, making international consensus more achievable.

To bolster these initiatives, the establishment of a coalition modeled on the International Counter Ransomware Initiative (CRI) could serve as a practical and effective solution. With its growing membership and proven track record, the CRI demonstrates the benefits of pooling resources, sharing intelligence, and coordinating rapid responses.[99] [100] A similar coalition focused on North Korea's cyber activities would enable member states to collectively mitigate threats, ensuring a more unified and effective approach to countering hybrid threats.

### B. Leveraging Advanced Technologies for Effective Enforcement

The integration of advanced technologies is essential for combating North Korea's sophisticated hybrid tactics. AI and blockchain-based tools can enhance transparency, traceability, and accountability in sanctions enforcement.

---

97. The Budapest Convention on Cybercrime, adopted in 2001, is the first binding international treaty addressing cybercrime comprehensively, providing a harmonized legal framework for combating offenses such as illegal access, data interference, and computer-related fraud. Developed by the Council of Europe with input from non-member states like the U.S. and Japan, the Convention facilitates international cooperation through mechanisms for extradition, mutual legal assistance, and evidence sharing. *See* Chat Le Nguyen & Wilfred Golman, *Diffusion of the Budapest Convention on Cybercrime and the Development of Cybercrime Legislation in Pacific Island Countries: 'Law on the Books' vs 'Law in Action,'* 40 Comput. L. & Sec. Rev. (2021).

98. *Id.*

99. *See International Counter Ransomware Initiative 2024 Joint Statement*, The White House (2024), https://www.whitehouse.gov/briefing-room/statements-releases/2024/10/02/international-counter-ransomware-initiative-2024-joint-statement/ [https://perma.cc/3G7M-ZWUR] (noting that during the Fourth CRI Gathering, "members reaffirmed [the] joint commitment to develop collective resilience to ransomware, support members if they are faced with a ransomware attack, pursue the actors responsible for ransomware attacks and not allow safe haven for these actors to operate within our jurisdictions, counter the use of virtual assets as part of the ransomware business model, partner with the private sector to advise and support CRI members, and forge international partnerships so we are collectively better equipped to counter the scourge of ransomware.").

100. Since its launch in 2021, the International Counter Ransomware Initiative (CRI) has become the largest global cyber partnership between governments, doubling its membership as ransomware evolved from a niche issue to a significant national security threat worldwide. *See* Adam Dobell, *The International Counter Ransomware Initiative: From Forming and Norming to Performing*, Ctr. for Cybersec. Pol'y & L. (Sep. 24, 2024), https://www.centerforcybersecuritypolicy.org/insights-and-research/the-international-counter-ransomware-initiative-from-forming-and-norming-to-performing [https://perma.cc/Y8YQ-V75L].

### 1. Blockchain and AI-Driven Monitoring

North Korea's reliance on cryptocurrency theft necessitates robust technological countermeasures. While blockchain technology has opened up new revenue for North Korea for illegal cyber operations, it also provides an opportunity to effectively detect illicit activities.[101] One of the most pressing challenges in combating North Korea's cyber tactics is the regime's exploitation of decentralized financial platforms to launder stolen cryptocurrency. Blockchain's tamper-proof ledgers offer a means to track and trace financial transactions with unparalleled accuracy.[102] By recording all transactions immutably, blockchain systems create a transparent and unalterable record[103] which makes it significantly harder for North Korea to obfuscate the origins or destinations of illicit funds.

Meanwhile, AI can play a crucial role in detecting and preventing attacks across various categories. It can identify indicators of emerging threats early, allowing organizations to respond proactively before these attacks are executed.[104] Additionally, AI can analyze patterns to recognize and mitigate existing attack types, using this data to train advanced neural networks like deep learning models.[105]

## C. Building Consensus and Addressing Counterarguments

Despite the clear need for action, achieving global consensus on sanctions and enforcement measures remains a significant challenge. Divergent geopolitical interests among major powers often complicate unified responses to North Korea's threats. For example, while the United States and European nations may push for stricter sanctions and collaborative cybersecurity measures, other influential nations may resist such efforts due to their economic or strategic ties with North Korea. This lack of alignment weakens the potential for a cohesive, global enforcement mechanism.

Regional coalitions and bilateral agreements can provide viable pathways for progress. Regional players such as the United States, South Korea, and Japan share a strong interest in countering North Korea's cyber capabilities and can form the foundation for broader international collaboration. For example, South Korea has already participated in the 'Cyber Flag,' a multinational military joint cyber drill organized by the U.S. Cyber Command, since 2022.[106] The main purpose of this multinational joint training is to integrate

101. Some recent research explores innovative blockchain-based methods to enhance cybersecurity, particularly in detecting and mitigating cyberattacks. *See* Zhiqi Feng, Yongli Li & Xiaochen Ma, *Blockchain-Oriented Approach for Detecting Cyber-Attack Transactions*, 9 Fin. Innovation 81 (2023).

102. Kristian McCann, *Top 10 Uses of Blockchain in Cybersecurity*, Cyber Mag. (Sep. 11, 2024), https://cybermagazine.com/articles/top-10-blockchain-strategies [https://perma.cc/JCN4-PFMX].

103. *Id.*

104. Michele Daryanani, *How AI Influences Cybersecurity*, KPMG, https://kpmg.com/ch/en/insights/cybersecurity-risk/artificial-intelligence-influences.html [https://perma.cc/GY29-6C8K].

105. *Id.*

106. Kim & Lee, *supra* note 70, at 56.

analysis through information fused with multinational defense against cyber threats.[107] Expanding these coalitions to include other countries targeted by North Korea's cyber operations, such as European nations and Southeast Asian states, can strengthen collective defenses.

Critics may also raise concerns about privacy and data security associated with the expanded use of blockchain and AI in monitoring financial transactions. To address these concerns, enforcement mechanisms must include robust safeguards to ensure data is used solely for legitimate enforcement purposes and protected against misuse. Transparency and oversight will be critical to maintaining trust in these systems while achieving enforcement objectives.

## Conclusion

North Korea's hybrid warfare tactics—blending cyber operations, decentralized financial exploitation, and traditional statecraft—underscore the urgent need for a modernized, multidimensional response. The limitations of traditional sanctions, which focus primarily on physical assets and state-controlled entities, highlight the necessity of integrating advanced technological tools, collaborative enforcement frameworks, and adaptive legal mechanisms to effectively counter these evolving threats.

Blockchain technology and AI provide promising solutions for addressing North Korea's sophisticated methods. By leveraging blockchain's immutable audit trails and AI's ability to detect patterns in real-time, the international community can enhance transparency, accountability, and resilience in both sanctions enforcement and cybersecurity. These technologies, when paired with international collaboration and updated legal frameworks, can help disrupt North Korea's financial networks and mitigate its global influence.

At the same time, implementing these measures requires careful consideration of privacy concerns and geopolitical barriers. Mechanisms must be in place to ensure that monitoring efforts respect individual rights, and regional coalitions can serve as the foundation for broader international consensus. If implemented thoughtfully, these measures not only address the immediate challenges posed by North Korea but also establish a robust model for managing emerging hybrid threats worldwide.

As hybrid warfare continues to evolve, the global response must remain equally adaptive, proactive, and united. By adopting a forward-looking approach, the international community can set a precedent for resilience against complex, unconventional threats and ensure a more secure and cooperative global order.

107. *Id.*