www.ijarp.com ISSN 2456-9992 Page: 01-15

International Journal Advanced Research Publications

Case Study

Volume: 02
Issue: 07

THE IMPACTS OF CYBER WARFARE ON INTERNATIONAL RELATIONS: A CASE STUDY OF THE UNITED STATES AND NORTH KOREA

***Glory Ochuwa Obidah, Popoola Olusegun Victor, Demawu-cole Abidemi Alhameed Abe Feranmi Blessing**

Espam Formation University, Sacuoba Anavia, Porto-Novo Republic of Benin.

Article Received: 09 June 2026, Article Revised: 29 June 2026, Published on: 19 July 2026

***Corresponding Author: Glory Ochuwa Obidah**
Espam Formation University, Sacuoba Anavia, Porto-Novo Republic of Benin.

Doi: https://doi-doi.org/101555/ijarp.8211

ABSTRACT

This article examines how cyber operations attributed to the Democratic People's Republic of Korea (DPRK) have affected international relations, using the United States–North Korea relationship as a longitudinal case from the 2014 Sony Pictures attack to the financial-theft, ransomware and illicit information-technology worker campaigns documented through early 2026. The term cyber warfare is used cautiously: most observed activity remains below the legal threshold of armed conflict and is better understood as persistent grey-zone competition. A qualitative process-tracing design links cyber incidents to public attribution, sanctions, criminal indictments, asset seizures, diplomatic coordination and alliance adaptation. The study finds that DPRK cyber activity has produced five durable effects. It has broadened the bilateral security agenda beyond nuclear weapons; converted private firms and cryptocurrency platforms into foreign-policy theatres; strengthened United States–Republic of Korea–Japan cyber diplomacy; intensified the use of law-enforcement and financial instruments as tools of statecraft; and exposed the weakness of conventional deterrence against a highly insulated, risk-tolerant actor. However, the operations have not compelled major United States policy concessions or generated a decisive strategic victory. Their principal international-relations effect is cumulative: persistent friction, higher defensive costs, deeper coalition coordination and continuing contestation over attribution, sovereignty and responsible state behaviour. The article concludes that an effective response must combine resilience, rapid multilateral attribution, financial disruption, private-sector governance and calibrated diplomatic signalling rather than relying on retaliation alone.

KEYWORDS: Cyber Warfare; International Relations; North Korea; United States; Cyber Deterrence; Sanctions; Cryptocurrency; Grey-Zone Conflict.

1. INTRODUCTION

Cyberspace has become a consequential arena of international politics because it permits states to impose costs, obtain intelligence, and generate revenue without crossing borders in a conventional sense. Yet the vocabulary is routinely abused. A malicious intrusion is not automatically warfare, and the strategic effects of cyber operations are often less dramatic than alarmist accounts suggest [16–20]. This distinction is central to the United States–DPRK case. North Korean operations have destroyed data, stolen funds, threatened expression and targeted critical sectors, but they have generally remained below the threshold that would trigger a conventional military response. They therefore occupy the space between espionage, crime, coercion and armed conflict. The 2014 compromise of Sony Pictures Entertainment brought this problem into United States foreign policy. The Federal Bureau of Investigation attributed the destructive intrusion to the North Korean government, citing similarities in malware, infrastructure overlap, and links to prior attacks [1]. The incident was politically distinctive because a foreign state was accused of using cyber means against a private company to punish and influence speech. Subsequent United States actions—sanctions, indictments, cryptocurrency seizures, public advisories and coalition diplomacy—turned cyber attribution into an instrument of statecraft [3–14]. Meanwhile, DPRK activity shifted from retaliation and espionage toward revenue generation through bank theft, virtual-asset heists, ransomware and fraudulent remote employment.

This article asks three questions: How have DPRK cyber operations changed the substance of United States–North Korea relations? Through what mechanisms are technical incidents converted into diplomatic and strategic effects? Why has the expanding United States response imposed costs without terminating the behaviour? The argument is that cyber operations have not revolutionised the balance of power or produced decisive coercion. Instead, they have institutionalised a persistent form of asymmetric competition. Their importance lies in cumulative effects: agenda expansion, alliance coordination, financial securitisation, public–private interdependence and a chronic deterrence problem.

2. Literature Review and Analytical Framework

Cyber-conflict scholarship is divided between revolutionary and restraint-oriented perspectives. Early strategic writing emphasised low entry costs, anonymity and vulnerability

in networked societies [25,26,28]. More sceptical scholars argue that cyber operations rarely substitute for conventional force, struggle to create durable political control and usually function as supplements to broader power [16–18]. Empirical studies similarly show that cyber incidents can alter short-term interstate interaction, but effects depend on the type of operation and the political objective [19,20]. Recent work moves beyond the binary question of whether 'cyber war' exists and examines how cyberspace changes statecraft, institutional dependence and strategic competition [22,23,27]. Three concepts organise this study. First, asymmetric leverage explains why a materially weaker and internationally isolated state invests in cyber capabilities. North Korea can exploit highly connected adversaries while exposing relatively little domestic digital infrastructure to reciprocal attack [15,29]. Second, the stability–instability logic suggests that nuclear and conventional deterrence may reduce the likelihood of major war while encouraging limited provocations below that threshold [2]. Third, weaponised interdependence explains how control over financial networks, digital platforms, exchanges, and legal jurisdictions becomes a form of coercive power [23]. The United States can sanction, seize and indict through network centrality, while the DPRK seeks to bypass that centrality through cryptocurrency theft, laundering and overseas IT labour.

The dependent variable is not merely technical damage. It is a change in international relations across five dimensions: bilateral hostility and agenda-setting; diplomatic attribution and signalling; economic statecraft; alliance and coalition formation; and norms governing sovereignty, private actors, and responsible state behaviour. The proposed causal sequence is incident → harm → attribution → policy conversion → international-relations outcome. Attribution is the pivotal bridge. Without credible attribution, states struggle to justify sanctions or collective action; with it, they can impose costs, construct coalitions and frame conduct as unacceptable, although attribution does not guarantee deterrence [1,21,24].

3. METHODOLOGY

The research adopts a qualitative single-case study with longitudinal process tracing from November 2014 to January 2026. The case is analytically useful because it combines an extreme asymmetry of conventional power with persistent cyber interaction, extensive public attribution and multiple response instruments. Evidence was drawn from United States government attribution statements, criminal complaints and indictments, Treasury sanctions notices, CISA and FBI advisories, State Department diplomatic records and peer-reviewed

scholarship. Events were coded by operational objective, target, attribution status, United States response and international-relations effect.

Process tracing is appropriate because the principal task is to identify mechanisms rather than estimate an average treatment effect. The analysis tests whether observable changes followed cyber incidents in official framing, policy instruments, coalition behaviour and bilateral relations. Triangulation reduces dependence on any single agency. Nevertheless, public evidence has limitations: intelligence sources remain classified; legal allegations are not identical to judicial findings; state attribution may serve strategic communication; and North Korean internal decision-making is largely inaccessible. Accordingly, the paper distinguishes official attribution from independently proven fact and avoids treating every intrusion associated with a security-industry label as direct evidence of state command.

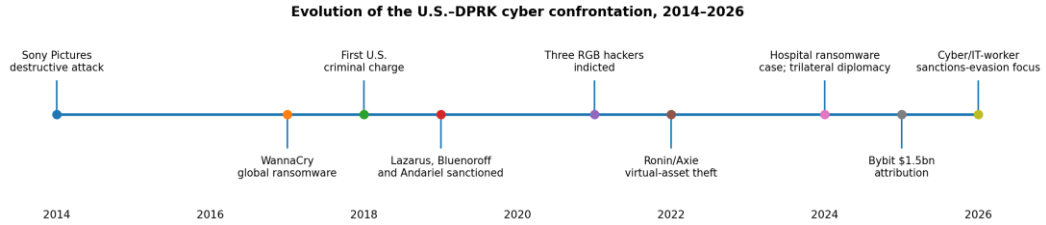

Figure 1. Selected milestones in the U.S.–DPRK cyber confrontation. Sources: FBI, DOJ, Treasury, CISA and Department of State records [1,3–14].

4. Evolution of the Cyber Confrontation

Table 1. Selected incidents, official responses and international-relations significance.

Episode	Operational character	U.S./allied response	International relations affect
2014 Sony Pictures attack	Destructive malware, data theft and coercive threats linked to film distribution	FBI public attribution; executive and sanctions response	Moved a private entertainment company into national security policy; raised censorship and attribution controversies
2017 WannaCry; 2018 Park charge	Global ransomware and related alleged RGB operations	Public attribution and first criminal charge against a DPRK programmer	Shifted response from political accusation toward evidence-based law-enforcement attribution
2019–2021 financial campaigns	Bank theft, SWIFT manipulation and cryptocurrency operations	Sanctions on Lazarus, Bluenoroff and Andariel; indictment of three military hackers	Integrated cyber activity into sanctions enforcement and transnational financial governance
2022–2023	Blockchain-company	Joint advisories, wallet	Linked cyber theft more

Episode	Operational character	U.S./allied response	International relations affect
virtual-asset theft	targeting and major virtual-asset thefts	identification, mixer sanctions and financial disruption	explicitly to sanctions evasion and weapons financing
2024 health-sector ransomware	Ransomware against U.S. hospitals allegedly funding espionage	Indictment, reward, asset seizure and joint cyber diplomacy	Demonstrated convergence of criminal revenue, intelligence collection and critical-infrastructure harm
2025–2026 Bybit and IT-worker schemes	Large virtual-asset theft and fraudulent remote employment	FBI attribution, coordinated forfeiture actions, allied statements and sanctions-evasion diplomacy	Expanded cyber security into labour markets, corporate due diligence and multilateral sanctions compliance

4.1 The Sony Attack: Coercion, Expression and Public Attribution

The Sony incident established the basic political grammar of the case. The attack disabled systems, exfiltrated proprietary and personal data and was accompanied by threats connected to the distribution of The Interview. The FBI publicly concluded that the North Korean government was responsible [1]. Haggard and Lindsay characterised the episode as an extension of limited North Korean coercion into global cyberspace. They noted the unprecedented presidential-level attribution of a cyberattack to a nation-state [2]. The political target was broader than Sony's network: the operation sought to influence expression and commercial decision-making within the United States. The response demonstrated both the value and fragility of attribution. Public naming allowed Washington to frame the incident as unacceptable state behaviour and justify additional sanctions. However, technical experts questioned whether the publicly disclosed evidence was sufficient, illustrating a recurrent dilemma: governments may possess classified evidence that cannot be released without compromising intelligence capabilities. The credibility of attribution therefore depends on a mixture of technical indicators, intelligence confidence, allied support and subsequent legal evidence. The 2018 complaint against Park Jin Hyok strengthened the official narrative by connecting the Sony operation to WannaCry and bank theft through a detailed prosecutorial account [3].

4.2 From Political Retaliation to Revenue Generation

The confrontation subsequently widened from destructive retaliation to the systematic acquisition of financial assets. United States authorities alleged that DPRK military hackers targeted banks, cryptocurrency businesses, automated teller networks and blockchain

platforms across multiple jurisdictions [4–8]. Treasury's 2019 designation of Lazarus Group, Bluenoroff and Andariel located these actors within the Reconnaissance General Bureau and treated cyber operations as state-controlled instruments rather than ordinary transnational crime [5]. The 2021 indictment of three military hackers alleged a broad programme combining revenge, espionage and theft [4]. This shift matters for international relations because stolen digital assets can offset the effects of sanctions. Cyber theft thereby becomes part of the political economy of coercion: sanctions reduce lawful access to foreign currency, while cyber operations create illicit alternatives. Treasury linked major virtual-asset thefts and laundering infrastructure to the DPRK, while CISA and FBI advisories described persistent targeting of blockchain firms [7,8]. In February 2025, the FBI attributed the approximately $1.5 billion Bybit theft to North Korean TraderTraitor actors [11]. A January 2026 United States statement further framed cyber theft and fraudulent IT work as violations and evasions of United Nations sanctions [14]. The implication is not that each stolen dollar can be traced to a specific weapons programme, but that cyber-enabled revenue weakens the intended bargaining leverage of economic isolation.

4.3 Ransomware, Espionage and Illicit IT Work

The DPRK portfolio also blurred the line between state security operations and criminal enterprise. A 2024 United States case alleged that an Andariel actor used ransomware proceeds from attacks on hospitals to finance intrusions against defence and technology organisations [9]. Fraudulent remote IT worker schemes added another layer: individuals allegedly used false or stolen identities to obtain employment, generate revenue, access corporate systems, and sometimes facilitate extortion or data theft [13]. These practices internationalise what would otherwise appear to be domestic corporate-security issues. Hiring verification, contractor governance and cryptocurrency compliance become components of sanctions implementation and national security.

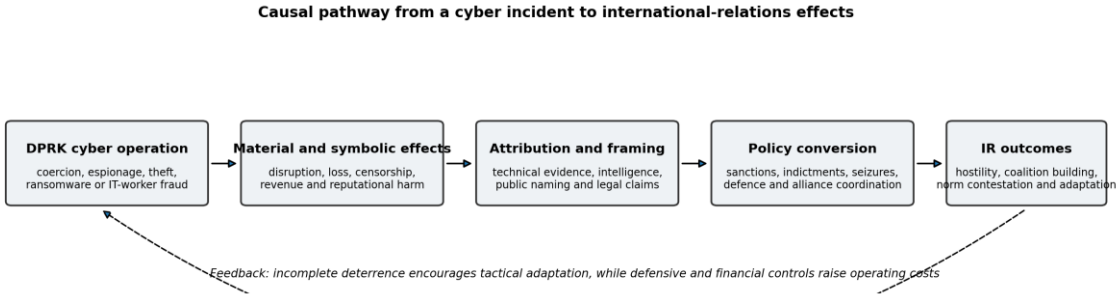

Figure 2. Analytical mechanism linking DPRK cyber operations to international-relations outcomes.

5. Findings: Impacts on International Relations

5.1 Expansion of the Bilateral Security Agenda

The first impact is agenda expansion. United States–North Korea relations have traditionally centred on nuclear weapons, ballistic missiles, sanctions, conventional deterrence and human rights. Cyber activity now connects each of these domains. Destructive attacks raise homeland security concerns; espionage affects defence planning; theft undermines sanctions effectiveness; ransomware threatens critical services; and IT worker fraud implicates labour and corporate governance. Cyber policy is therefore no longer a technical annex to Korea policy. It is a cross-cutting component of deterrence, non-proliferation, finance and diplomacy. This expansion increases policy complexity. A military response may be disproportionate to a financially motivated intrusion, while a purely criminal response may understate state sponsorship. The United States has consequently developed a mixed toolkit comprising diplomatic condemnation, sanctions, indictments, rewards, forfeiture, advisories and partner capacity-building. This hybrid response is evidence that cyber conflict disrupts the traditional separation between war, crime and intelligence.

5.2 Attribution as Diplomatic Signalling and Coalition Construction

Public attribution is both an evidentiary claim and a diplomatic act. It identifies an alleged perpetrator, communicates confidence, reassures domestic audiences and invites partners to align. The 2014 FBI statement transformed a corporate breach into an interstate controversy [1]. Later indictments supplied names, organisational affiliations, infrastructure and alleged operational histories, increasing the reputational and legal costs of denial [3,4,9]. Yet attribution remains probabilistic and politically contested. Excessive certainty unsupported by releasable evidence can damage credibility; excessive caution permits deniability. The United States increasingly addresses this problem through collective attribution and diplomatic working groups. Meetings with the Republic of Korea and Japan in 2024 focused specifically on DPRK cyber activity, information sharing and coordinated countermeasures [10]. Joint statements in 2025 framed cryptocurrency theft as a shared regional and global threat [12]. Coalition attribution does not merely add voices; it distributes intelligence burdens, harmonises sanctions and reduces opportunities for attackers to exploit regulatory fragmentation.

5.3 Economic Statecraft and the Securitisation of Digital Finance

The third impact is the securitisation of cryptocurrency and digital-finance governance. Virtual assets were initially discussed primarily in terms of technological and regulatory innovations. In the DPRK case, exchanges, bridges, mixers, wallet providers and blockchain

analytics have become nodes in sanctions enforcement. Treasury designations and seizures aim to interrupt laundering pathways, while advisories pressure firms to improve know-your-customer controls and operational security [7,8]. This is an application of network power: the United States uses legal jurisdiction, financial centrality and private-sector cooperation to constrain an adversary [23].

However, the relationship is adaptive rather than one-sided. As controls improve, actors shift chains, use mixers, exploit decentralised protocols, recruit insiders or obtain legitimate-looking employment. The result is a regulatory security dilemma in which defensive measures increase firms' compliance costs and may displace rather than eliminate illicit activity. Cyber-enabled sanctions evasion therefore reduces the coercive efficiency of economic pressure, even when seizures recover a portion of assets.

Table 2. Principal international-relations effects identified by the case study.

Dimension	Mechanism	Observed consequence
Bilateral relations	Cyber added a permanent field of confrontation alongside nuclear and missile disputes.	Wider agenda, greater mistrust and more frequent low-level interaction
Deterrence	Low operational exposure, deniability and limited DPRK digital dependence weaken retaliation threats.	Persistence despite sanctions, indictments and public attribution
Economic statecraft	Theft and fraudulent employment create revenue while U.S. network power enables seizures and sanctions.	Continuous adaptation between evasion and financial disruption
Alliance politics	Shared threats incentivise U.S.–ROK–Japan information sharing and diplomatic coordination.	Cyber becomes an institutionalised area of trilateral security cooperation
International norms	Operations against private firms, hospitals and digital platforms test sovereignty and proportionality.	Greater emphasis on responsible state behaviour but limited enforcement consensus
Public–private relations	Victims and key intelligence holders are often private organisations	Corporate security, disclosure and compliance become foreign-policy functions

5.4 Alliance Adaptation and Minilateral Diplomacy

Cyber threats have reinforced minilateral cooperation among the United States, the Republic of Korea and Japan. This cooperation is strategically significant because the three states possess complementary intelligence, financial-regulatory and technical capabilities, but historically faced political constraints on security coordination. DPRK cyber activity supplies a practical, recurring problem around which cooperation can be institutionalised without

requiring agreement on every regional issue. Working groups, joint advisories, and coordinated sanctions can improve the speed of attribution, victim notification, and asset tracing [10,12]. The broader consequence is that a bilateral cyber confrontation produces regional institutional effects. North Korean activity may generate revenue or intelligence tactically, yet it also encourages tighter coordination among Pyongyang's principal adversaries. This is a strategic externality often omitted from assessments focused solely on immediate financial gains.

5.5 Norms, Sovereignty and the Role of Private Actors

The Sony episode exposed the normative ambiguity of state coercion directed at a private speaker. Later attacks on hospitals and cryptocurrency businesses further complicated the public–private boundary. In conventional security, governments are the principal defenders and targets. In cyberspace, private firms own much of the infrastructure, monitor crucial telemetry, and bear the upfront costs. They also make decisions about whether to disclose, pay, patch, freeze, or delist, which affect diplomacy and sanctions enforcement. This distribution of responsibility creates governance problems. A state can condemn an operation as unacceptable without a universally accepted rule specifying the required response. International law applies to cyber operations, but disagreement persists over sovereignty, thresholds of prohibited intervention, due diligence and proportional countermeasures. The DPRK case therefore illustrates a wider normative deficit: states increasingly attribute and sanction malicious conduct, but enforcement remains fragmented and heavily dependent on coalition power rather than universal agreement.

5.6 Why Deterrence Remains Incomplete

The continued pace of activity indicates incomplete deterrence. Conventional deterrence assumes identifiable decision-makers, credible threats, valuable assets at risk and a relationship between imposed costs and behavioural restraint. Each condition is weakened here. DPRK networks are relatively insulated; operators can work through foreign infrastructure; sanctions are already extensive; cyber tools are reusable and deniable; and the regime may value revenue and intelligence more than reputational standing. Indictments restrict travel and expose tradecraft but have little immediate incapacitating effect on actors unlikely to enter United States custody. This does not mean responses are useless. They can recover funds, harden targets, constrain intermediaries, clarify norms and increase operating costs. The error is to evaluate every measure by whether it permanently stops all attacks. The more realistic objective is cumulative denial: reducing success rates, shrinking laundering options, disrupting infrastructure, protecting high-risk sectors and preventing tactical gains

from becoming strategic leverage. Consistent with restraint-oriented cyber scholarship, the case shows that cyber operations are persistent instruments of competition rather than reliable tools for compelling fundamental policy reversal [16–22].

6. DISCUSSION

The evidence supports a middle position between cyber alarmism and dismissal. North Korean operations have not produced the kind of decisive strategic effects associated with major warfare. They have not forced Washington to recognise the DPRK's nuclear status, withdraw forces or terminate sanctions. The Sony operation did not permanently suppress the film. Yet the cumulative consequences are substantial. The United States has altered sanctions practice, prosecution strategy, diplomatic coordination, private-sector guidance and alliance institutions in response. Cyber operations therefore matter less as isolated shocks than as repeated transactions that reshape the architecture of international security.

The case also reveals a paradox of asymmetric cyber power. North Korea benefits from the openness and financial innovation of advanced economies while limiting reciprocal exposure at home. However, the same operations provoke deeper coalition coordination and justify tighter financial surveillance. Tactical effectiveness can therefore generate adverse strategic adaptation. The balance depends on whether illicit revenue and intelligence gains exceed the long-term costs imposed by disruption, exposure, and coalition-building—a calculation that cannot be resolved from public data alone.

A second contribution is conceptual. Calling the entire pattern "cyber warfare" obscures important differences among coercion, espionage, theft, ransomware, and labour fraud. These activities have different legal thresholds, victims and policy remedies. A first-class international relations analysis should not collapse them into a single dramatic label. The more accurate description is persistent, state-directed cyber competition below armed conflict, with occasional destructive and coercive features.

6.1 Small-State Power, Regime Survival and Strategic Substitution

The case qualifies conventional assumptions that international influence follows aggregate material power. North Korea cannot match the United States in economic scale, global finance, intelligence reach or conventional force projection. Yet, it can exploit digital access to impose recurring costs at a distance. This is not parity. It is strategic substitution: cyber capabilities enable a weaker state to pursue selected objectives that would be prohibitively expensive to pursue through conventional means. Revenue theft partially compensates for financial isolation; espionage reduces information disadvantages; destructive malware draws

political attention; and remote-worker schemes insert state-linked activity into ordinary commercial relationships. The power gained is narrow and opportunistic, but it is politically useful because it supports regime survival without requiring open military confrontation.

This form of power is also relational. DPRK effectiveness depends on characteristics of the target environment: dense connectivity, valuable data, global payment networks, rapid innovation and uneven corporate security. The United States' openness is a source of prosperity and international influence, but it expands the attack surface. Conversely, North Korea's restricted domestic connectivity limits some retaliatory options. The asymmetry is therefore not simply that one side is technologically stronger. The stronger side is more dependent on systems that must remain accessible, while the weaker side can accept isolation and operational risk. International relations theory should consequently distinguish between capability possession and exploitable dependence.

6.2 Escalation, Crisis Stability and Cross-Domain Risk

Although most operations remain below the level of armed conflict, they are not automatically escalation-proof. A destructive attack on hospitals, financial clearing systems or military networks could be misread as preparation for a broader campaign. Attribution delays create a temporal problem: leaders may face public pressure before technical confidence is mature, while covert retaliation can generate a cycle neither side openly acknowledges. Cross-domain responses further complicate proportionality because a cyber incident may be answered through sanctions, arrests, financial seizures, diplomatic pressure or non-cyber capabilities. The absence of an agreed ladder makes signalling less transparent than in conventional deterrence.

The United States has generally chosen calibrated instruments, which suggests an effort to impose costs while avoiding military escalation. North Korea, for its part, appears to exploit this restraint by operating below thresholds likely to trigger a response. This interaction can be stable at the level of major war yet unstable at lower levels: frequent operations, reciprocal disruption, and cumulative mistrust become the norm. Risk reduction, therefore, requires more than stronger defence. It requires communication about protected critical functions, careful language in public attribution and channels through which unintended effects can be clarified during a wider Korean Peninsula crisis.

6.3 Limitations and Future Research

The findings should be interpreted within four limitations. First, the public record overrepresents detected and politically salient incidents; failed operations and quiet diplomatic exchanges remain invisible. Second, official United States sources are

indispensable for understanding policy but may reflect prosecutorial and strategic objectives. Third, the analysis cannot directly measure how stolen revenue is allocated inside the DPRK or identify the marginal effect of cyber income on weapons development. Fourth, a single case cannot establish that the same mechanisms operate identically for other cyber powers. Future work should build event-level datasets that separate attribution confidence, operational objective, financial value, target sector and policy response. Comparative cases involving Iran, Russia and non-state proxies could test whether insulation and sanctions pressure produce similar behaviour. Firm-level research is also necessary because organisational hiring, disclosure and custody practices increasingly influence interstate outcomes. Finally, greater attention should be paid to policy effectiveness: which combinations of seizures, sanctions, technical disruption and allied coordination reduce operational success rather than merely demonstrate political resolve?

7. Policy Implications

A credible policy should combine six elements. First, resilience must take priority over symbolic retaliation: segmented networks, offline backups, privileged access controls, secure software development, and rapid incident reporting reduce the expected value of attacks. Second, public attribution should be evidence-led, tiered by confidence and coordinated with allies. Third, financial disruption should target laundering services, facilitators, infrastructure and fraudulent employment networks while avoiding assumptions that sanctions alone will change regime strategy. Fourth, governments should institutionalise public–private information sharing with liability protection and clear disclosure protocols. Fifth, high-risk organisations—healthcare providers, defence contractors, cryptocurrency firms and remote-hiring platforms—require tailored controls rather than generic awareness campaigns. Sixth, cyber risk-reduction channels should be incorporated into broader Korean diplomacy to reduce misperception and establish crisis communication, even when political relations are strained.

Policy evaluation should use realistic metrics: assets frozen or recovered; infrastructure disrupted; victim losses prevented; time from detection to allied attribution; compliance improvement; and reduction in successful access. Counting indictments or sanctions without measuring operational effect encourages performative policy. Conversely, demanding complete cessation sets an impossible standard. The aim is persistent constraint and resilience, not a final cyber victory.

8. CONCLUSION

Cyber operations have changed United States–North Korea relations by creating a durable arena of confrontation that intersects with nuclear diplomacy, sanctions, finance, intelligence and alliance politics. The Sony attack demonstrated the coercive and symbolic potential of a state-sponsored operation against a private company. Subsequent bank thefts, cryptocurrency heists, ransomware, and fraudulent IT work transformed cyber activity into an instrument for revenue generation and sanctions evasion. United States responses evolved accordingly—from public attribution and sanctions to indictments, forfeiture, private-sector advisories and trilateral diplomacy. The central finding is qualified. DPRK cyber activity is strategically significant, but it is not equivalent to conventional war and has not delivered decisive coercion. Its impact is cumulative and institutional: it intensifies mistrust, expands the security agenda, strengthens regional cooperation, securitises digital finance and forces private organisations into foreign-policy roles. The persistence of operations despite repeated penalties demonstrates the limits of punishment-based deterrence against an insulated and adaptive adversary. International stability therefore depends on a layered strategy that combines resilience, collective attribution, financial disruption, law enforcement, alliance coordination, and calibrated diplomacy. The practical task is not to abolish cyber competition—an unrealistic objective—but to deny strategic advantage while controlling escalation.

REFERENCES

1. Federal Bureau of Investigation. (2014, December 19). Update on Sony investigation.
2. Haggard, S., & Lindsay, J. R. (2015). North Korea and the Sony hack: Exporting instability through cyberspace. AsiaPacific Issues, 117, 1–8.
3. U.S. Department of Justice. (2018, September 6). North Korean regime-backed programmer charged in conspiracy to conduct multiple cyberattacks and intrusions.
4. U.S. Department of Justice. (2021, February 17). Three North Korean military hackers were indicted in a wide-ranging scheme to commit cyberattacks and financial crimes across the globe.
5. U.S. Department of the Treasury. (2019, September 13). Treasury sanctions North Korean state-sponsored malicious cyber groups.
6. Cybersecurity and Infrastructure Security Agency et al. (2020). Guidance on the North Korean cyber threat (AA20-106A).

7. Cybersecurity and Infrastructure Security Agency et al. (2022). TraderTraitor: North Korean state-sponsored APT targets blockchain companies (AA22-108A).
8. U.S. Department of the Treasury. (2023, May 23). Treasury targets DPRK malicious cyber and illicit IT worker activities.
9. U.S. Department of Justice. (2024, July 25). North Korean government hacker charged for involvement in ransomware attacks targeting U.S. hospitals.
10. U.S. Department of State. (2024, September 6). Third United States–Japan–Republic of Korea trilateral diplomatic working group meeting on DPRK cyber activities.
11. Federal Bureau of Investigation. (2025, February 26). North Korea is responsible for the $1.5 billion Bybit hack.
12. U.S. Department of State. (2025, January 14). Joint statement on cryptocurrency thefts by the DPRK and public-private collaboration.
13. U.S. Department of Justice. (2025). Coordinated nationwide actions to combat North Korean remote IT worker schemes.
14. U.S. Department of State. (2026, January 12). The DPRK's violations and evasions of UN sanctions through cyber and IT-worker activities.
15. Kim, M.-h. (2022). North Korea's cyber capabilities and their implications for international security. Sustainability, 14(3), 1744. https://doi.org/10.3390/su14031744
16. Gartzke, E. (2013). The myth of cyberwar: Bringing war in cyberspace back down to earth. International Security, 38(2), 41–73. https://doi.org/10.1162/ISEC_a_00136
17. Rid, T. (2012). Cyber war will not take place. Journal of Strategic Studies, 35(1), 5–32. https://doi.org/10.1080/01402390.2011.608939
18. Lindsay, J. R. (2013). Stuxnet and the limits of cyber warfare. Security Studies, 22(3), 365–404. https://doi.org/10.1080/09636412.2013.816122
19. Valeriano, B., & Maness, R. C. (2014). The dynamics of cyber conflict between rival antagonists, 2001–2011. Journal of Peace Research, 51(3), 347–360. https://doi.org/10.1177/0022343313518940
20. Maness, R. C., & Valeriano, B. (2016). The impact of cyber conflict on international interactions. Armed Forces & Society, 42(2), 301–323. https://doi.org/10.1177/0095327X15572997
21. Borghard, E. D., & Lonergan, S. W. (2017). The logic of coercion in cyberspace. Security Studies, 26(3), 452–481. https://doi.org/10.1080/09636412.2017.1306393
22. Maschmeyer, L. (2021). The subversive trilemma: Why cyber operations fall short of expectations. International Security, 46(2), 51–90.

https://doi.org/10.1162/isec_a_00418

23. Farrell, H., & Newman, A. L. (2019). Weaponised interdependence: How global economic networks shape state coercion. International Security, 44(1), 42–79. https://doi.org/10.1162/isec_a_00351
24. Buchanan, B. (2017). The cybersecurity dilemma: Hacking, trust, and fear between nations. Oxford University Press.
25. Nye, J. S., Jr. (2010). Cyber power. Belfer Centre for Science and International Affairs, Harvard Kennedy School.
26. Libicki, M. C. (2009). Cyberdeterrence and cyberwar. RAND Corporation.
27. Foulon, M. (2024). How cyberspace affects international relations. Contemporary Security Policy. https://doi.org/10.1080/13523260.2024.2365062
28. Kello, L. (2017). The virtual weapon and international order. Yale University Press.
29. Jun, J., LaFoy, S., & Sohn, E. (2015). North Korea's cyber operations: Strategy and responses. Centre for Strategic and International Studies / Rowman & Littlefield.