ISSN 1738-0154 / eISSN 2713-6728

Terrorizing through Extortionary Means: The Divergent Cases of North Korea versus Hamas

Alexis Jihye Yang*

Key Words: North Korea, Hamas, cyberterrorism, cryptocurrency

|ABSTRACT|

Over the past decade, North Korea has intensified its use of cyber operations, evolving from traditional espionage to sophisticated attacks on global financial systems as a means to circumvent international sanctions and illicitly generate revenue. Unlike nuclear or missile provocations, these cyberattacks often evade significant international condemnation and sanctions, despite their growing impact on civilian infrastructure and financial stability. This research examines the phenomenon of cyberterrorism by state and nonstate actors, comparing how the impact of cyberterrorism by state actors like North Korea diverges from how nonstate actors like Hamas leverage access to cyberspace for financial gain. The study argues that cyberterrorism, traditionally associated with non-state actors, must be reconceptualized to include hostile states that exploit cyberspace for extortion, disruption, and terror. By analyzing the financing strategies of Hamas and the evolving tactics of North Korean cyber units, the paper highlights the nuance between the use of cyberspace by terrorist organizations versus actions that fall under the definition of cyberterrorism. Special attention is given to the exploitation of cryptocurrency markets by both actors, demonstrating how these activities not only cause immediate economic harm but also enable sustained conflict by funding future operations. The article concludes by discussing the broader theoretical and policy implications – in particular, emphasizing the urgent need for international frameworks that address the dual-use nature of cyber operations as tools of both warfare and terrorism.

✣ 『국제관계연구』 제30권 제2호(2025년 겨울호).
http://dx.doi.org/10.18031/jip.2025.12.30.2.71

* Visiting Research Fellow, Ilmin International Relations Institute, Korea University, Seoul, Republic of Korea.

Ⅰ. Introduction

In the last decade, North Korea has increasingly utilized cyber operations to not only conduct espionage operations on its enemies but also conduct strategic attacks on financial markets to circumvent international sanctions and illicitly gain revenue through criminal means. But because the attacks occur within cyberspace, there is less fear, condemnation, and sanctions compared to when conducting nuclear tests and ballistic missile launches. However, not only do we see the nature of cyber-attacks to be aimed towards civilians, but it is also used as a means of terrorizing for politically or ideologically motivated reasons – in other words, attacks take on the nature of *cyberterrorism*.

The purpose of this research is to highlight and identify the different pathways by which both state and nonstate actors can leverage access to cyberspace for hostile purposes, such as securing financing and conducting cyber warfare. States such as North Korea, Russia, China, and Iran use cyberterrorism and cyber warfare to extort financial resources and engage in indirect psychological warfare against states that they deem to be enemies.[1] For this analysis, I will be focusing specifically on the cases of North Korea and Hamas to advance the argument that threats from cyberterrorism and extortionary cybercrimes should not be solely localized to terrorist organizations, but that it is also a means of financial procurement and cyber warfare used by belligerent countries such as North Korea.

The reasoning behind the comparison between Hamas, a renowned terrorist organization, and North Korea, a state actor, demands an explanation upfront. The conceptual definition of cyberterrorism

1) America's Cyber Defense Agency, "Nation-State Threats," https://www.cisa.gov/topics/cyber-threats-and-advisories/nation-state-cyber-actors (Accessed March 24, 2025).

remains vague and disputable, with a lack of agreement in the literature as to whether to define cyberterrorism as restricted to cyberattacks motivated by political or ideological motives or to be inclusive and take on a broader definition that encompasses the use of cyberspace for bolstering terrorist activities in the real world. While much concern over the use of cyberterrorism by terrorist actors was motivated by concerns for the former, this paper goes on to show that the concern over cyberterrorism posing a detrimental impact in the real world is and can actually be carried out by state actors. The illustrative case comparison between Hamas's use of cyberspace and North Korea's use of cyberspace thereby illustrates this point. It goes on to show the necessity of including states as possible actors that carry out detrimental acts of cyberterrorism.

This article will proceed as follows. First, I will review the literature on terrorism to advance the need to reconceptualize the concept of cyberterrorism to encompass state actors. Next, I will provide the background context to Hamas and its sources of financing over the years since its inception. The following section will go on to provide an overview of North Korea's cyber operations, detailing the strategy, tactics, and motives of North Korean cyberattacks over the last decade. I will then follow up with an illustrative assessment of how the trajectories of North Korea and Hamas led to a similar strategy but differing approaches to using cryptocurrency markets, and how this not only results in first-stage casualties but also perpetuates future terror by funding warmongering capabilities. I will conclude by presenting the academic and policy implications of this research.

Ⅱ. Definition of Cyberterrorism

The most straightforward definition of cyberterrorism can be seen as the convergence of cyberspace and terrorism.[2] However, the definition

becomes less straightforward when it comes to determining *what* should be viewed as cyberterrorism. Some definitions view cyberterrorism as a cyberattack motivated by political or ideological motives, while others incorporate the use of cyberspace for "enabling, facilitating, or amplifying" terrorist activities beyond cyberspace.[3] To be more specific, the seven types of cyberactivity defined as cyberterrorism include destroying the machinery of an infrastructure, commandeering controls of nuclear power plants or hazardous waste facilities, using computers to control dams, hacking into power grids, using technology to commit sabotage, initiating protests that involve hacking into government computers, and compromising information illegally accessed through computers.[4]

However, defining cyberterrorism to be to cyberattacks creates a restrictive definition. According to NIST's Computer Security Resource Center (CSRC), cyberattacks are defined as "an attack, via cyberspace, targeting an enterprise's use of cyberspace for the purpose of disrupting, disabling, destroying, or maliciously controlling a computing environment/ infrastructure; or destroying the integrity of the data or stealing controlled information."[5] Conversely, overly broad definitions – such as those that classify any cyber activity enabling terrorist objectives, including fundraising, propaganda, or recruitment – as cyberterrorism risk obscuring the distinction between cyberterrorism and the broader category of terrorist activity conducted in cyberspace.[6]

---

2) Dorothy E. Denning, "Cyberterrorism: The Logic Bomb Versus the Truck Bomb," *Global Dialogue*, Vol. 2, No. 4 (2000), pp. 29-37.

3) Mehmet F. Bastug and Ismail Onat, "Cyberterrorism," *Oxford Research Encyclopedia of Criminology*, March 20, 2024, https://oxfordre.com/criminology/view/10.1093/ acrefore/ 9780190264079.001.0001/acrefore-9780190264079-e-790 (Accessed November 10, 2025).

4) Jonathan Matusitz, "Cyberterrorism: Postmodern State of Chaos," *Information Security Journal: A Global Perspective*, Vol. 17, No. 4 (2008), pp. 179–187.

5) Computer Security Resource Center, "Cyber attack – Glossary," https://csrc.nist.gov/glossary/ term/cyber_attack (Accessed November 24, 2025).

6) Bastug and Onat (2024).

According to Plotnek and Slay, a balanced definition would be a construct that takes into consideration the actor, motive, intent, means, effect, and target. After running a statistical analysis, they propose the following to be the written definition of cyberterrorism:

> "Cyber terrorism is the premeditated attack or threat thereof by non-state actors with the intent to use cyberspace to cause real-world consequences in order to induce fear or coerce civilian, government, or non-government targets in pursuit of social or ideological objectives. Real-world consequences include physical, psychosocial, political, economic, ecological, or otherwise that occur outside of cyberspace."[7)]

However, more recent developments suggest the need to consider state actors as potential perpetrators of cyberterrorism. A notable example emerged in July 2010, when the Stuxnet computer worm incident heightened fears about cyberterrorism as a major national security threat. The virus was a malicious software that attacked widely used industrial control systems built by the German firm Siemens, with a study by U.S. technology company 'Symnatic' showing that the main affected countries as of August 6, 2010, were – Iran, with 62,867 infected computers, Indonesia with 13,336, India 6,552, United States 2,913, Australia 2,436, Britain 1,038, Malaysia 1,013 and Pakistan with 993.[8)] While it was never proven who was to blame, there have been some who have pointed to U.S. and Israeli experts.[9)]

---

7) Jordan J. Plotnek and Jill Slay, "Cyber Terrorism: A Homogenized Taxonomy and Definition," *Computers & Security*, Vol. 102 (2021).

8) *Reuters*, "Factbox: What Is Stuxnet?" September 24, 2010, http://www.reuters.com/article/2010/09/24/us-security-cyber-iran-fb-idUSTRE68N3PT20100924 (Accessed November 24, 2025).

9) *The Washington Post*, "Stuxnet was work of U.S. and Israeli experts, officials say," June 2, 2012, https://www.washingtonpost.com/world/national-security/stuxnet-was-work-of-us-and-israeli-experts-officials-say/2012/06/01/gJQAlnEy6U_story.html (Accessed

Although the Stuxnet worm was designed to infiltrate Iranian computers and slow down their uranium enrichment activities[10], the broader lesson from this event is that cyber threats can effectively target physical assets just as well as conventional weapons can.[11] Another important takeaway from this event is that cyberterrorists are not limited only to non-state actors; states may also be responsible for cyberterrorist events. Among the five main groups that currently use, or are likely to develop, the capacity for cyberattacks are terrorist organizations and states, both of which are increasingly developing offensive and defensive capabilities as a growing part of their force capabilities.[12]

Ⅲ. State Actors as Cyberterrorists

Terrorism is most commonly defined as "violence – or threat of violence – used and directed in pursuit of, or in service of, a political aim." It is ineluctably political in aims and motives, violent – or threatens violence, designed to have far-reaching psychological repercussions beyond the immediate victim or target, conducted by an organization or by a small collection of individuals, and perpetrated by a subnational group or nonstate entity.[13] By extension, cyberterrorism is defined as "the premeditated use of disruptive activities, or the threat thereof,

November 24, 2025).

10) *Business Insider*, "The Stuxnet Attack on Iran's Nuclear Plant Was 'Far More Dangerous' than Previously Thought," November 21, 2013, http://www.businessinsider.com/stuxnet-was-far-more-dangerous-than-previous-thought-2013-11 (Accessed November 24, 2025).

11) LTC Marco De Falco, "Stuxnet Facts Report: A Technical and Strategic Analysis," (Tallinn: NATO Cooperative Cyber Defense Centre of Excellence, 2012), p. 31.

12) Yoram Schweitzer, Gabi Siboni, and Einav Yogev, "Cyberspace and Terrorist Organizations," *Military and Strategic Affairs*, Vol. 3, No. 3 (2011), p. 40.

13) Bruce Hoffman, *Inside Terrorism* (New York: Columbia University Press, 2017), pp. 2-3, 43-44.

against computers and/or networks, with the intention to cause harm or further social, ideological, religious, political or similar objectives, or to intimidate any person in furtherance of such objectives."[14] As such, while terrorism has generally been understood as a strategic tool by collective groups or organizations with low capacity to maximize their political gains, the shift to its use in cyberspace has triggered discussions over expanding the scope of terrorist entities to include state actors.

The use of the term *cyberterrorists* in a Congressional Research Service (CRS) Report somewhat reflects this shift. Theohary and Rollins (2015) define cyberterrorists to be "state-sponsored and non-state actors who engage in cyberattacks to pursue their objectives." They go on to cite the use of the Internet by transnational terrorist organizations, insurgents, and jihadists as a tool to support organizational objectives such as planning attacks, radicalization and recruitment, a method of propaganda distribution, a means of communication, and for disruptive purposes.[15] While these definitions allude to the possibility of state involvement in terrorism in cyberspace, they do not clearly distinguish the primary actor as the state but rather presume the cyberterrorist entity to be the agent that the state may have delegated the act of committing terror to.

This is because "state sponsorship" denotes a particular relationship between terrorist organizations and state actors. In theory, relationships between violent nonstate and state actors fall within a spectrum based on the degree of autonomy the terrorist group has from state support, strategy, and power.[16] In this case, state sponsorship involves the state's

14) Catherine A. Theohary and John W. Rollins, "Cyberwarfare and Cyberterrorism: In Brief," *US Congressional Research Service Report R43955* (2015), p. 2.

15) John W. Rollins and Clay Wilson, "Terrorist Capabilities for Cyber-attack: Overview and Policy Issues," *US Congressional Research Service Report RL33123* (2007), pp.10-11.

16) Kai M. Thaler, "Delegation, Sponsorship, and Autonomy: An Integrated Framework for Understanding Armed Group–State Relationships," *Journal of Global Security Studies*,

deliberate provision of resources and material support to terrorist organizations that enable concrete organizational advantages, going a long way in building group capacity towards fighting and resisting efforts at counterterrorism and counterinsurgency. This may include tangible support such as weapons, money, training, and the provision of safe havens.[17)]

But because the state sponsor tends to have little or nothing to gain from the militant group's success in terms of its core security interests, sponsorship fulfills a secondary "national interest" in providing support, most commonly due to ideological or identity affinity.[18)] These secondary interests include advancing their international political and strategic position, furthering their ideology, and bolstering their position at home.[19)]

Rather, state terrorism would be a more accurate expression for the use of terrorism by state actors. Fundamentally, the only difference would be that the terrorist act is "committed by the state, and to the benefit of the state," where there must be evidence of state involvement through agents or resources of the state. This would include terrorism by proxies employed by the state, so long as it can be shown that they have been trained, armed, or financed by the state.[20)] Another definition provided by Heryanto (2006)[21)] states that state terrorism comprises a

---

Vol. 7, No. 1 (2021), p. 4.

17) Daniel Byman, "Understanding, and Misunderstanding, State Sponsorship of Terrorism," *Studies in Conflict & Terrorism*, Vol. 45, No. 12 (2022), pp. 1031–1049.

18) Here, Thaler (2021) distinguishes "core security interests" to be more central to the state, whereas the "national interest" is more contested.

19) Daniel Byman, *Deadly Connections: States That Sponsor Terrorism* (Cambridge: Cambridge University Press, 2007), pp. 21–52.

20) David Claridge, "State terrorism? Applying a definitional model," *Terrorism and Political Violence*, Vol. 8, No. 3 (1996), p. 52.

21) Ariel Heryanto, *State Terrorism and Political Identity in Indonesia: Fatally Belonging* (New York: Routledge, 2006).

series of state-sponsored campaigns that induce widespread fear throughout the population.[22] This arguably focuses mostly on "internal" state terrorism within one's own country, and pays less attention to the "external" aspects of state terrorism outside of its borders.[23]

Turning to the case of the Democratic People's Republic of North Korea (DPRK, or North Korea for short), their cyber operations largely adopts an asymmetric strategy in its application, Given their main opponents are the militarily and economically superior United States and the Republic of Korea (ROK, or South Korea for short), North Korea has invested in asymmetric capabilities that allow for the projection of power and coercion without triggering a conventional military standoff.[24] However, Kim and Polito (2019) observe that broadly, there have been two main shifts in Pyongyang's cyber operations between 2009 and 2018. First, there has been an increase in cyber-attacks aimed at financial gain, and secondly, there has been a corresponding decrease in the visibility of cyber operations in espionage and information gathering.[25] What this implies is the shift in the focus of cyber-attacks to a broader, civilian audience outside of their borders that induces fear in the general populace.

In addition, taking a closer look at how cyber operations are run in North Korea will provide further evidence to show that there is near-alignment of the state and "affiliated" hacker groups that merits a theoretical reclassification towards state terrorism rather than

---

22) William N. Holden, "Ashes from the phoenix: state terrorism and the party-list groups in the Philippines," *Contemporary Politics*, Vol. 15, No. 4 (2009), p. 378.

23) Kacper Rekawek, "Russian State Terrorism and State Sponsorship of Terrorism," *International Centre for Counter-Terrorism Report* (2024), p. 5.

24) Jenny Jun, Scott LaFoy, and Ethan Sohn, *North Korea's Cyber Operations: Strategy and Responses* (Washington D.C.: Center for Strategic & International Studies, 2015), p. 26.

25) Chong Woo Kim and Carolina Polito, *The Evolution of North Korean Cyber Threats* (Seoul: Asan Institute for Policy Studies, 2019), p. 2.

state-sponsored terrorism. The predominant North Korean government agencies in charge of cyber operations[26] are the Reconnaissance General Bureau (RGB) and the General Staff Department of the Korea Peoples' Army (GSD), with other government units including the State Security Department Bureau 225 and the Defense Commission Psychological Operations Department Unit 204.[27] These agencies are not only tasked with conducting their own cyber operations, but also directly managing the numerous North Korean commercial hacker groups.[28] These groups include well-known names such as the 'Lazarus Group (APT38)', 'BeagleBoyz', 'Adariel', and the 'Kimsuky group'.

To provide empirical evidence in support of this argument, I will be conducting a comparative case analysis of North Korea and Hamas. While the two are dissimilar in the former being a state actor and the latter being a nonstate group actor with a terrorist designation, they have both taken a remarkably similar path in evading sanctions to fund their acts of belligerency by relying on cryptocurrencies – showing the different trajectories of the use of cybercurrency to on one hand, fundraising purpose, while on the other, extorting through cryptocurrency heists that ultimately results in not only the disrupting and disabling of a critical financial institution but also goes to funding subsequent acts of terrorism and belligerency.

---

26) For a more detailed explanation on North Korean government agencies in charge of conducting cyber operations, refer to Bruce Klingner, "North Korean Cyberattacks: A Dangerous and Evolving Threat," *The Heritage Foundation Special Report*, No. 247 (2021), pp. 18-21 and Jun et.al (2015) pp. 35-59.

27) Klingner (2021), p. 5.

28) *The New Yorker*, "The Incredible Rise of North Korea's Hacking Army," April 19, 2021, https://www.newyorker.com/magazine/2021/04/26/the-incredible-rise-of-north-koreas-hacking-army (Accessed March 30, 2025).

Ⅳ. Hamas: Cybercurrency as a Source of Funding

Hamas, an acronym for Harakat al-Muqawama al-Islamiya (Islamic Resistance Movement), is a Sunni Islamist militant movement and one of the Palestinian territories' two major political parties.[29] Founded by Sheikh Ahmed Yassin in 1987 after the first Intifada against the Israeli occupation, it has continued to govern more than two million Palestinians in the Gaza Strip since taking control from Fatah in 2007.[30] They have been designated as a terrorist organization by dozens of countries[31] – although some apply this label only to its military wing. They receive external support from states such as Iran, which provides them with material and financial support, while Turkey is reported to harbor some of their top leaders.

Hamas emerged as an outgrowth of the Palestinian branch of the Muslim Brotherhood. They went on to establish themselves as an alternative to the secular Fatah within the Palestinian Authority (PA), which was set up after the Palestine Liberation Organization (PLO) and Israel entered a peace process and were subsequently tasked to exercise limited control in the West Bank and Gaza. Ideologically positioning itself to be a combination of Palestinian nationalism with Islamic fundamentalism, Hamas has since committed itself to eliminating Israel and establishing an all-Islamic state of Palestine in its place.

Following a forceful seizure of Gaza in 2007 after a breakdown in a Saudi-brokered PA unity government, they have since continued to

---

29) Carol A. Ireland, Michael Lewis, Anthony Lopez and Jane L. Ireland, *The Handbook of Collective Violence: Current Developments and Understanding* (London: Routledge, 2020), p. 239.

30) Jessica Davis, *Women in Modern Terrorism: From Liberation Wars to Global Jihad and the Islamic State* (Lanham: Rowman & Littlefield, 2017), pp. 67-69.

31) These countries include, but are not limited to: Argentina, Australia, Canada, Israel, Japan, Paraguay, New Zealand, the United Kingdom, the United States, and the European Union.

preside over Gaza as the de facto authority amidst deteriorating economic and humanitarian conditions. And while Hamas remains the preferred faction for at least 20% of Palestinians in the West Bank and Gaza (WBG) in most polls, the extent of their domestic popularity remains uncertain.[32] WBG polls taken in late 2023 indicate a boost in Palestinian approval for Hamas in the aftermath of the conflict, but it is uncertain whether this spike in support will persist. This is because Hamas' domestic popularity tended to spike in the wake of past conflicts but would then soon fall back to pre-conflict levels.[33]

It is therefore unsurprising that Hamas is best known for its armed resistance to Israel, apparent from its engagement in multiple wars sporadically from 2008 onward. This vastly differs from the approach taken by the Fatah, its rival party, which dominates the Palestine Liberation Organization (PLO) and rules in the West Bank, which has formally renounced violence – a vow that has not always been upheld during times of high Israeli-Palestinian tensions. Most recently, Hamas launched a massive surprise attack on southern Israel on October 7 of 2023, killing more than 1,200 people (both civilian and military) and taking around 240 more as hostages. In response, Israel has declared war on the group and indicated plans for its military to conduct a long campaign to wipe it out entirely.[34]

Given its designation as a terrorist entity, Hamas is not privy to the official assistance provided to the PLO in the West Bank by the United States and the European Union (EU). Instead, much of the funding

32) An Arab Barometer survey taken just before October 7 found the majority of Gazans to have little or no trust in the Hamas-led government, with Palestinians in the WBG voicing more support overall for Fatah over Hamas.

33) Jim Zanotti, "Hamas: Background, Current Status, and U.S. Policy," *US Congressional Research Service IF12549* (2024).

34) Kali Robinson, "What is Hamas?" *Council on Foreign Relations*, October 31, 2023, https://www.cfr.org/backgrounder/what-hamas (Accessed May 25, 2024).

historically comes from Palestinian expatriates and private donors in the Persian Gulf, in addition to some Islamic charities in the West. Foreign aid generally tends to reach Gaza via the PA and UN agencies. However, the 2006-07 closing of borders by Egypt and Israel has made the movement of goods and people in and out of the territory severely difficult.

To circumvent the blockade, Hamas collected revenue by taxing goods moving through Egypt into Gaza using a series of underground tunnels. Not only did this bring staples such as food, medication, and affordable gas for energy, such as electricity, but it also brought resources such as construction materials, cash, and arms. In 2013, Abdel Fatah al-Sisi became President of Egypt, under whom the Egyptian army was ordered to shut down the network of channels that breached its territory as a part of a counterterrorism campaign against the newly declared Islamic State. In 2018, Egypt started allowing Gaza limited access to commercial goods through its Salah-al-Din border, leading to earnings averaging around $12 million per month[35] from taxes for Hamas.[36]

Another significant source of funding and support comes from surrounding states sympathetic to the Palestinian plight. Some have been consistently forthcoming (i.e., Iran) with their support, while others have, over time, gradually become sponsors. Hamas relied heavily on funding from states such as Iran, Iraq, Syria, and Sudan before their takeover of the Gaza Strip. In the case of Syria, the Assad regime provided decades of support to Hamas up until the Syrian civil war.[37] As for Qatar,

35) This figure represents monthly estimates from 2021.

36) Robinson (2023).

37) United States Department of State, "State Sponsors of Terrorism," August 18, 2011, https://2009-2017.state.gov/j/ct/rls/crt/2010/170260.htm (Accessed July 25, 2025); *The New York Times*, "Hamas Leader Abandons Longtime Base in Damascus," January 27, 2012, https://www.nytimes.com/2012/01/28/world/middleeast/khaled-meshal-the-leader-of-hamas-vacates-damascus.html (Accessed July 25, 2025).

they have more recently been publicly providing Hamas with monthly stipends that help pay for electricity as fuel as well as wages for the public sector – all with Israel's knowledge and acquiescence.[38] Additionally, Qatar has provided safe asylum to top political leader Ismail Haniyeh, along with several other senior Hamas leaders, who now reside in luxury.[39] Furthermore, Qatar has been able to leverage its unique relationship with Hamas to facilitate hostage negotiations in the aftermath of October 7 and has gone on to publicly indicate its openness to reconsidering Hamas's continued presence in Doha.[40]

Alternatively, Hamas started fundraising through cryptocurrency donations starting in 2019. In 2023, the Wall Street Journal reported that cryptocurrency wallets connected to Hamas received about $41 million between 2020 and 2023.[41] In 2020, the U.S. Justice Department announced the seizure of several websites and 150 cryptocurrency accounts linked to the armed wing of Hamas, the Izz al Din al Qassam Brigades. It was revealed by U.S. enforcement actions in 2023 that the Qassam Brigades used Binance, a cryptocurrency exchange, to facilitate fundraising and donations through cryptocurrency transactions as early as 2019.[42] Since its initial cryptocurrency campaign in 2019, Hamas

38) *Reuters*, "Who funds Hamas? A global network of crypto, cash and charities," October 16, 2023, https://www.reuters.com/world/middle-east/hamas-cash-to-crypto-global-finance-maze-israels-sights-2023-10-16/(Accessed May 30, 2025).

39) *CBC News*, "How tiny Qatar hosts the leaders of Hamas without consequences," October 18, 2023, https://www.cbc.ca/news/politics/qatar-hamas-israel-1.6999416 (Accessed June 12, 2025).

40) *Reuters*, "Qatar open to reconsidering Hamas presence in Qatar, US official says," October 27, 2023, https://www.reuters.com/world/middle-east/qatar-told-us-it-is-open-reconsidering-hamas-presence-us-official-says-2023-10-27/ (Accessed June 15, 2025); Devorah Margolin and Matthew Levitt, "The Road to October 7: Hamas' Long Game, Clarified," *CTC Sentinel*, Vol. 16, No. 10 (2023), pp. 1–10.

41) *The Wall Street Journal*, "From Hamas to North Korean Nukes, Cryptocurrency Tether Keeps Showing Up," October 27, 2023, https://www.wsj.com/finance/currencies/most-popular-cryptocurrency-keeps-showing-up-in-illicit-finance-71d32e5e (Accessed April 15, 2025).

continued efforts to generate cryptocurrency donations; in 2021, the U.S. cryptocurrency exchange platform Coinbase identified Hamas as one of several terrorist groups involved in cryptocurrency fundraising, with the Israeli authorities reportedly seizing dozens of cryptocurrency addresses linked to Hamas, PIJ, and other terrorist groups between 2021 and 2023.[43]

V. North Korea's Cyber Operations

If it was Kim Jong-il who initiated North Korea's foray into cyber warfare in the 1980s, it was during Kim Jong-un's reign that Pyongyang truly accelerated and expanded its cyberattacks on a broader spectrum of targets.[44] The disruptive and extortionary tactics of the North Korean cyber-attacks have increasingly expanded their capacity to inflict significant damage to South Korea and its allies. Not only are they believed to have jammed the GPS systems of planes over Incheon Airport,[45] but they have also successfully hacked into South Korean banks, newspapers, and nuclear power plants – not to mention their famous hacking of Sony Pictures in 2014 in response to the regime-critical film "The Interview".[46]

---

42) United States Department of Justice, "Global Disruption of Three Terror Finance Cyber-Enabled Campaigns," August 13, 2020, https://www.justice.gov/archives/opa/pr/global-disruption-three-terror-finance-cyber-enabled-campaigns (Accessed March 29, 2025).

43) Rena S. Miller and Liana W. Rosen, and Paul Tierno, "Terrorist Financing: Hamas and Cryptocurrency Fundraising," *US Congressional Research Service IF12537* (2024).

44) Klingner (2021), p. 3.

45) *The Associated Press*, "North Korean GPS manipulation disrupted dozens of planes and vessels, South Korea says," November 9, 2024, https://apnews.com/article/north-korea-gps-interference-jamming-aircraft-nuclear-2f6a345ffd3bcf2875b04a758658c9c7 (Accessed April 15, 2025).

46) Elizabeth Suh, "North Korea's Cyber Capabilities and Strategy," *German Council on Foreign Relations*, January 7, 2022, https://dgap.org/en/research/publications/north-koreas-cyber-capabilities-and-strategy-0 (Accessed April 15, 2025).

It is no wonder senior U.S. intelligence officials have already assessed back in 2017 that North Korea was one of the top four cyber threats capable of launching "disruptive or destructive cyberattacks" against the United States.[47] More recently, the Office of the Director of National Intelligence's 2024 Annual Threat Assessment[48] has released the following analysis:

> "North Korea's cyber program will pose a sophisticated and agile espionage, cybercrime, and attack threat. Pyongyang's cyber forces have matured and are fully capable of achieving a variety of strategic objectives against diverse targets, including a wider target set in the United States and South Korea."

Pyongyang's cyber activities may generate less reaction and punishment compared to its missiles and nuclear weapons, despite repeated attacks against governments, financial institutions, and industries.[49] But given its ability to disrupt or destroy one or more of the elements comprising cyberspace – such as the information, software, and the physical infrastructure component – and its effectiveness in neutralizing or suppressing the benefits of advanced weaponry and combined arms,[50] it is essential we understand and evaluate the strategical usage of cyber-attacks as an integral part of its military strategy, alongside ground, air, sea and space.[51]

---

47) *Yonhap News Agency*, "U.S. Intelligence Chiefs Pick N. Korea as Major Cyber Threat," January 6, 2017, https://en.yna.co.kr/view/AEN20170106000200315 (Accessed March 14, 2025).

48) Office of the Director of National Intelligence, "Annual Threat Assessment of the U.S. Intelligence Community," February 5, 2024, https://www.dni.gov/files/ODNI/documents/assessments/ATA-2024-Unclassified-Report.pdf (Accessed March 14, 2025), p. 22.

49) Klingner (2021), p. 1.

50) Jun et.al (2015), p. 24.

51) Alexandre Mansourov, *North Korea's Cyber Warfare and Challenges for the U.S.-ROK Alliance* (Washington D.C.: Korea Economic Institute of America, 2014), p. 4.

In evaluating the *modus operandi* of North Korean cyber-attacks, Boo (2017) finds that North Korean cyber-attacks are usually delivered in tandem with traditional security threats, with instructions given to the elites of North Korea's hacking organizations from above to coordinate cyber-attacks with other military provocations, such as the fourth nuclear test.[52] Their strategic use of cyber-attacks has now evolved to take on the form of coercive diplomacy, criminal activities to generate hard currency, and disruptive actions against South Korea and against deployed U.S. forces.[53] One approach North Korea takes to expand political influence is by intervening in other countries' political processes to undermine their political stability or exert influence in the international community. Another approach is to conduct cyber espionage against government organizations and companies to gather critical intelligence in the military, political, and economic sectors to determine and shift their foreign policy and strategy.[54]

To do so, North Korean cyber operations have utilized a range of tactics[55] such as:

- **Spear Phishing or Social Engineering** North Korean cyber actors rely heavily on spear phishing with investment-, job-, and payroll-themed e-mails or social media messages to trick a target company's

52) Hyeong-wook Boo, "An Assessment of North Korean Cyber Threats," *The Journal of East Asian Affairs*, Vol. 31, No.1 (2017), p. 103.

53) James Andrew Lewis, "The Likelihood of North Korean Cyber Attacks," *Center for Strategic & International Studies*, September 7, 2017, https://www.csis.org/analysis/likelihood-north-korean-cyber-attacks (Accessed March 14, 2025).

54) Sang-jung Byun and Junghyun Yoon. *The Evolution of North Korea's Cyber Influence Operations and Its Implications* (Seoul: Institute for National Security Strategy, 2024), pp. 3-4.

55) The Cyber Threat Intelligence Integration Center, "North Korea Tactics, Techniques, and Procedures for Revenue Generation," July 2023, https://www.dni.gov/files/CTIIC/documents/products/North-Korean-TTPs-for-Revenue-Generation.pdf (Accessed March 14, 2025).

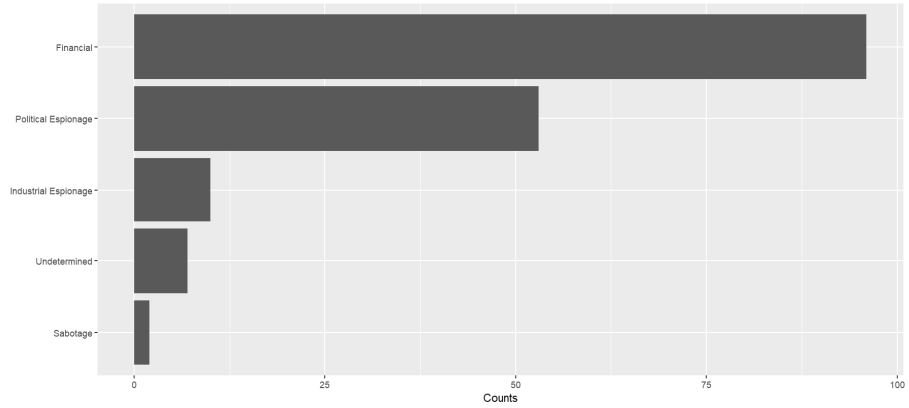
employees into downloading malware that will enable cyber actors to compromise the firm's network, exfiltrate wallet private keys, or hijack transaction validators to undermine the security and integrity of entire blockchains.

- **North Korean IT Worker-Enabled Malicious Access** North Korean IT workers living abroad use privileged access gained as contractors to support the regime's cyber operations by sharing access to virtual infrastructure, facilitating the sale of stolen data, or assisting with money laundering and virtual currency transfer.
- **Software Vulnerability Exploitation** North Korean cyber actors buy vulnerabilities and exploits from brokers or steal them from security researchers for use against unpatched networks. Advanced persistent threat (APT) 37 and the Lazarus Group are the most likely North Korean cyber groups to use software exploits and quickly weaponize zero-day vulnerabilities.
- **Supply Chain Attack** North Korean cyber actors compromise software firms or third-party IT providers to insert malicious code into a company's software and also target cryptocurrency customers through legitimate but compromised applications.

Using these methods, the North Korean cyber operations have successfully carried out strategically motivated attacks that involved cyber espionage to steal information or conduct surveillance, and disrupting or destabilizing networks in critical infrastructure through cyberattacks. Improvements in the scope, scale, and sophistication of cyber operations lead to the progression towards cyberterrorism, revenge attacks, and extortion.[56]

56) Klingner (2021), p. 8.

<Figure 1> Total Number of North Korean Cyber Attacks by Motive, 2014-2024



* Source: Harry and Gallagher (2018)

Figure 1 presents a bar chart that presents the number of all recorded cases of North Korean cyber-attacks between 2014 to 2024 by motive. This clearly shows that overall, attacks that are motivated by financial gain are predominant over other possible motives. Given that this data[57] spans from 2014 to 2024, it captures the early days of Kim Jong-un's reign and, therefore, North Korea's pivotal shift to cyber robbery operations as a way to gain revenue for the heavily sanctioned regime. Beginning with attacks against traditional financial institutions – such as banks, fraudulent forced interbank transfers, and automated teller machine (ATM) thefts – the regime shifted towards targeting cryptocurrency exchanges once the international community started to take notice of their cybercriminal activities.[58]

57) Charles Harry and Nancy Gallagher, "Classifying Cyber Events: A Proposed Taxonomy," *Journal of Information Warfare*, Vol. 17, No. 3 (2018), pp. 17-31.

58) Klingner (2021), pp. 8-9.

VI. Hamas and North Korea: Cryptocurrency Heists

In the case of Hamas, while the Qassam Brigades announced in April 2023 that it would stop accepting Bitcoin donations due to concerns over law enforcement targeting donors, this was not the end of Hamas's attempts to secure funding through cryptocurrency. After the October 7 attacks in 2023, several Hamas-affiliated groups solicited donations in cryptocurrency – most notably "Gaza Now," which raised tens of thousands of dollars since the attacks. Gaza Now was sanctioned by the United States on March 27, 2024.[59]

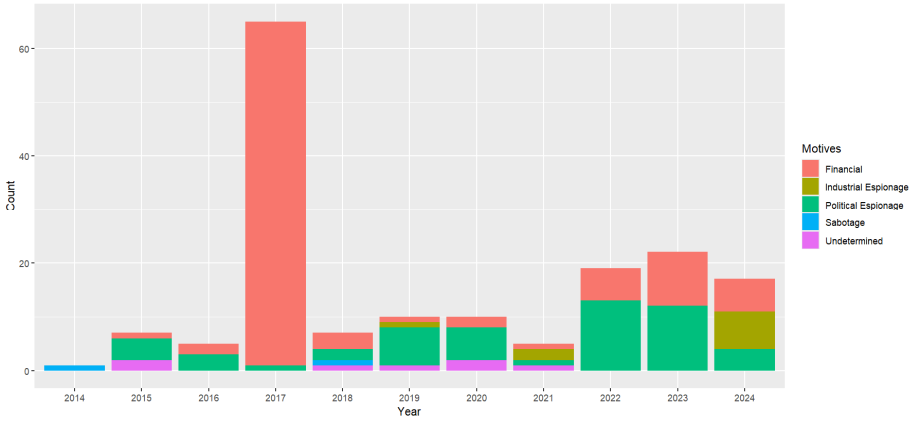
On the other hand, concerns over Hamas hacking and stealing from cryptocurrency exchanges are minimal at best. To date, there has only been one case of Hamas successfully stealing cryptocurrency, and it was from the wallets of a Delhi businessman.[60] Hamas can secure funding through other channels and thus does not need to rely solely on donations. The capacity to hack cryptocurrency exchanges for currency extortion would require far more resources allocated to building cyber capacity than to conducting political violence. Another limitation to a more widespread adoption of cryptocurrency by terrorist organizations is due to the limited acceptability and usability of these currencies in the regions in which terrorist groups operate. Even if a group receives and manages these funds, they cannot easily be used to pay for expenses

59) TRM Labs, "US DOJ Charges Hamas Leaders with October 7 Attacks, Details Hamas' Use of Cryptocurrencies," September 4, 2024, https://www.trmlabs.com/resources/blog/us-doj-charges-hamas-leaders-with-october-7-attacks-details-hamas-use-of-cryptocurrencies (Accessed March 14, 2025).

60) *India Today*, "Stolen from Delhi, sent to Hamas: What Delhi Police's crypto probe found," October 11, 2023, https://www.indiatoday.in/india/story/stolen-delhi-funneled-to-israel-hamas-war-delhi-police-cryptocurrency-probe-bitcoin-hamas-israel-war-2447435-2023-10-11 (Accessed March 14, 2025); *Times of India*, "Cryptocurrency stolen from Delhi lands in Hamas wallets," October 11, 2023, https://timesofindia.indiatimes.com/city/delhi/cryptocurrency-stolen-from-delhi-lands-in-hamas-wallets/articleshow/104327800.cms (Accessed March 14, 2025).

where vendors and members expect cash, either in stable currencies like dollars and euros or in local currencies.[61)]

<Figure 2>Number of North Korean Cyber Attacks by Motive, 2014-2024



* Source: Harry and Gallagher (2018)

This is not the case for state actors like North Korea. Between 2017 and 2023, there have been 58 suspected North Korean cyberattacks on cryptocurrency-related companies that have been valued at approximately $3 billion USD, which the United Nations suspected to help fund North Korea's nuclear weapons program.[62)] More recently, the US Federal Bureau of Investigation (FBI) announced that North Korea was responsible for the theft of approximately $1.5 billion USD in virtual assets from the cryptocurrency exchange 'Bybit', on or about February 21, 2025.[63)]

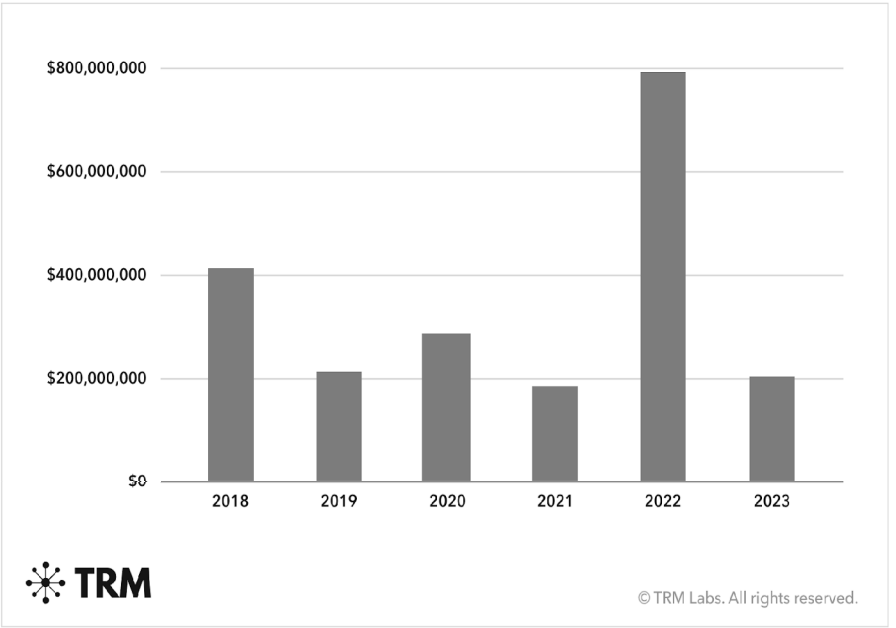
---

61) Cynthia Dion-Schwarz, David Manheim, and Patrick B. Johnston, *Terrorist Use of Cryptocurrencies: Technical and Organizational Barriers and Future Threats* (Santa Monica, CA: RAND Corporation, 2019), p. 13.

62) *Reuters*, "Exclusive: UN experts investigate 58 cyberattacks worth $3 bln by North Korea," February 8, 2024, https://www.reuters.com/technology/cybersecurity/un-experts-investigate-58-cyberattacks-worth-3-bln-by-north-korea-2024-02-08/ (Accessed March 14, 2025).

63) *Reuters*, "FBI says North Korea was responsible for $1.5 billion ByBit hack," February 28,

<Figure 3> Yearly Total in USD Stolen by North Korea, 2018-2023



* Source: TRM Labs (2023)

Although the total amount stolen in cryptocurrency attacks is down from a record-setting 2022, North Korea has maintained its focus on the crypto ecosystem in 2023. Year-to-date, North Korea has stolen USD 200 million in cryptocurrency, accounting for over 20% of all stolen crypto by August of 2023 – in fact, North Korean cyberattacks have been so successful, their hacks in 2023 are 10 times larger than attacks by other actors.[64] Carrying out such large hacks not only provides a means of securing a massive amount of funds, allowing for long-term planning,

2025, https://www.reuters.com/technology/cybersecurity/fbi-says-north-korea-was-responsible-15-billion-bybit-hack-2025-02-27/ (Accessed March 14, 2025); *BBC*, "North Korean hackers cash out hundreds of millions from $1.5bn ByBit hack," March 10, 2025, https://www.bbc.com/news/articles/c2kgndwwd7lo (Accessed March 14, 2025).

64) TRM Labs, "Inside North Korea's Crypto Heists: $200M in Crypto Stolen in 2023; Over $2B in the Last Five Years," August 18, 2023, https://www.trmlabs.com/resources/blog/inside-north-koreas-crypto-heists (Accessed March 14, 2025).

but also allows for North Korea to carry out other cyber operations, particularly in the area of espionage – as we can infer from Figure 2.

Consequently, the North Korean cyber operations have evolved to take on a dual function of asymmetric warfare and state terrorism in cyberspace. As North Korea's cyber proficiencies evolved, they shifted focus from military and infrastructure targets to prioritizing financial targets to evade international sanctions to augment funding for its nuclear and missile programs.[65] Additionally, beyond the first-stage damage incurred by cyber-attacks, the ramifications of such attacks have led to the bolstering of the offensive capacity of the North Korean regime by illicitly acquiring income and funding that they then channel into their Weapons of Mass Destruction (WMD) and ballistic missile programs.

Ⅶ. Implications

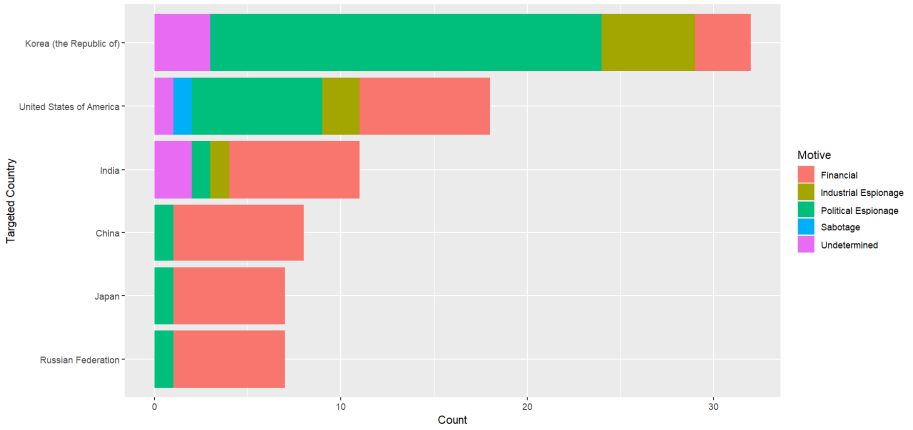
Threats from cyberterrorism and extortionary cybercrimes are not just localized by terrorist organizations; it is also a means of financial procurement and cyber warfare used by countries such as North Korea. The theoretical argument I advance in this paper is that state actors should also be included in defining cyberterrorists because the current definitions of state-sponsored or state terrorism do not adequately encompass the reality of states carrying out acts of cyberterrorism on civilian populations for political or ideological reasons. Not including state actors in the theoretical discussions over cyberterrorism and its actors will result in significant policy ramifications in countering cyberterrorism and, more broadly, global security concerns, as I will lay

65) Klingner (2021), p. 2.

out below.

In the case of North Korea, cyber espionage operations persisted even after commencing cyber robbery operations. North Korea has proven itself to be capable and adept at penetrating government, military, and banking networks, international financial transaction systems, and critical infrastructure targets.[66] Out of the top 5 target countries, South Korea and the United States hold the largest number of cyberattacks. And while the other three ranking target countries have mostly been hit with financially motivated attacks, South Korea and the United States have been hit more with espionage-motivated attacks than financially motivated attacks.

<Figure 4> Top 5 Countries Targeted by North Korea, 2014-2024



* Source: Harry and Gallagher (2018)

This is because cyberattacks have also been used to extract classified information to support North Korea's nuclear weapons program, such as plans relating to nuclear enrichment and blueprints of missile designs and missile defense systems. Those include satellite communication and

66) Ibid., p. 9.

technology, and radar systems such as surveillance radar.[67] In addition to stealing blueprints and other nuclear-related information, North Korea also leverages these hacks to finance and expand its military programs.[68]

The concurrent nature of North Korean cyber operations to tackle both espionage and financially motivated attacks has resulted in a feedback loop of sorts, where illicitly obtained funds from crypto heists are believed to be funneled into North Korea's weapons development programs, including nuclear and submarine capabilities.[69] Given that more than half of North Korea's nuclear weapons have been funded by cyberattacks and cryptocurrency theft[70], it is thereby essential to thwart avenues for extortionary attacks on cryptocurrency markets and exchanges.

> "North Korea is funding its military development – allowing it to pose greater risks to the United States – and economic initiatives by stealing hundreds of millions of dollars per year in cryptocurrency from the United States and other victims. Looking forward, the North may also expand its ongoing cyber espionage to fill gaps in the

---

67) *The Record from Recorded Future News*, "North Korean hacking group targeted weapons blueprints, nuclear facilities in cyber campaigns," July 25, 2024, https://therecord.media/north-korea-andariel-apt45-weapons-systems-nuclear-facilities (Accessed June 6, 2025).

68) Doreen Horschig, "How Are Cyberattacks Fueling North Korea's Nuclear Ambitions?" *Center for Strategic and International Studies,* July 31, 2024, https://www.csis.org/analysis/how-are-cyberattacks-fueling-north-koreas-nuclear-ambitions (Accessed June 6, 2025).

69) Sunha Bae, "Deterrence Under Pressure: Sustaining U.S.-ROK Cyber Cooperation Against North Korea," *Center for Strategic and International Studies*, April 1, 2025, https://www.csis.org/analysis/deterrence-under-pressure-sustaining-us-rok-cyber-cooperation-against-north-korea (Accessed June 6, 2025).

70) *CNN*, "Half of North Korean missile program funded by cyberattacks and crypto theft, White House says," May 10, 2023, https://edition.cnn.com/2023/05/10/politics/north-korean-missile-program-cyberattacks (Accessed June 6, 2025).

regime's weapons programs, potentially targeting defense industrial base companies involved in aerospace, submarine, or hypersonic glide technologies."[71]

However, while many analysts have cited concern over the North Korean cyber capabilities, they are simultaneously also doubtful as to their capacity to provoke a significant security threat to regional or global security. While South Korean experts have continued to sound the alarm about Pyongyang's cyber warfare capabilities,[72] less has been paid attention to its capacity for cyberterrorism and financial extortion. While this is purely reasonable, given the trend of Pyongyang's attacks to more likely conduct cyber espionage against South Korean targets, the lack of attention towards possible cyberterrorist attacks and financial extortion raises concerns over the capacity of South Korea to defend its networks against attacks on its digital financial markets and assets.

In a report by Hewlett-Packard Security Research, the authors stated that "we should not overestimate the regime's advanced cyber capability, yet we should never underestimate the potential impact of North Korea utilizing less advanced, quick-and-dirty tactics like DDoS to cripple their high-tech targets."[73] While Figure 5 illustrates North

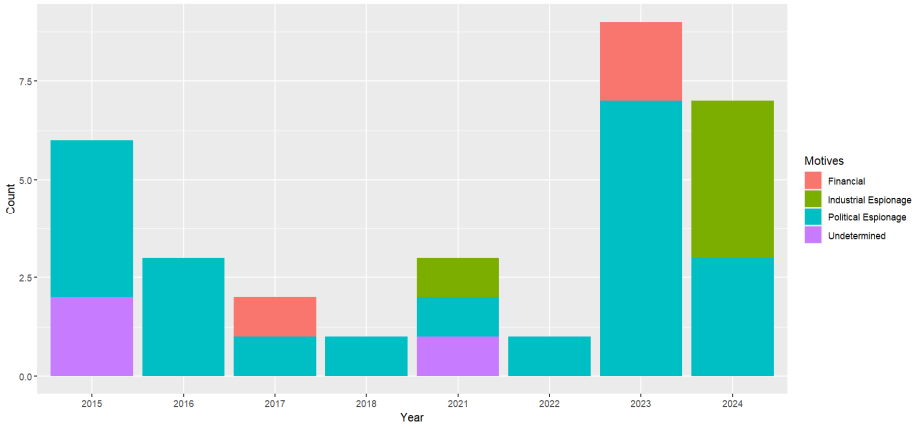
71) Office of the Director of National Intelligence, "Annual Threat Assessment of the U.S. Intelligence Community," March 25, 2025, https://www.dni.gov/files/ODNI/documents/assessments/ATA-2025-Unclassified-Report.pdf (Accessed June 6, 2025), p. 28.

72) For example, the South Korean Defense Security Commander General Song Yeong-geun asserted in 2004 that North Korea's computer hacking capability was so outstanding that it was second only to that of the U.S. Central Intelligence Agency. In June 2012, the ROK Defense Security Commander Bae Deuk-shik agreed with the opinion that "North Korea is the world's third most powerful nation in cyber warfare after Russia and the United States." Mansourov (2014), p. 3.

73) HP Security Research, "Profiling an enigma: The mystery of North Korea's cyber threat landscape," August 2014, *HP Security Briefing Episode 16*, https://time.com/wp-content/uploads/2014/12/hpsr_securitybriefing_episode16_northkorea.pdf (Accessed June 3, 2025).

Korean cyber operations against South Korea to more likely to be motivated by espionage concerns, by no means does this preclude the possibility of the potential for the South Korean crypto markets to be targeted, given that the South Korean market is estimated to be the third biggest cryptocurrency market in the world. This exposes a critical security risk in South Korea's readiness to prepare against cyberattacks on the crypto market by North Korean or other terrorist entities.

<Figure 5> Number of Yearly North Korean Cyber Attacks on South Korea



* Source: Harry and Gallagher (2018)

Another concern with omitting state actors as perpetrators of cyberterrorism and generalizing cyberattacks to cyber warfare is that it obfuscates the potential for civilians to be targeted in cyberspace. While South Korean crypto exchanges accounted for more than nine percent of the global trading volume in August 2021, the Korean Won ranks among the top five most traded currencies for Bitcoin.[74] This not

74) Statistica, "Daily cryptocurrency trading volume on South Korean and global exchanges as of August 3, 2021," June 26, 2024, https://www.statista.com/statistics/1261206/south-korea-trading-volume-on-local-and-global-crypto-exchanges/ (Accessed June 3, 2025); *Bloomberg*, "Upbit Rides Korea Crypto Boom to Top-Five Global Exchange Spot," April 25, 2024, https://www.bloomberg.com/news/articles/2024-04-25/korean-

only increases the cybersecurity risks of the cryptocurrency market being hacked by terrorist entities due to its size and trading volume, but this also leaves worldwide citizens who trade in Korean Won vulnerable to extortionary cybercrimes through means such as phishing scams masked with the intent to fund terrorist activity.

In addressing security concerns relating to cryptocurrency exchanges, the United Nations Panel of Experts recommends the following:

> "20. The Panel encourages Member States to implement the Financial Action Task Force standards, with special attention given to recommendation 15, that to manage and mitigate the risks emerging from virtual assets, countries should ensure that virtual asset service providers are regulated for anti-money-laundering and counter-terrorist financing purposes, and licensed or registered and subject to effective systems for monitoring and ensuring compliance with the relevant measures called for in the Financial Action Task Force recommendations."[75]

Here, the Financial Action Task Force (FATF) refers to the global money laundering and terrorist financing watchdog. It sets international standards that aim to prevent these illegal activities and the harm they cause to society. Their efforts include setting global standards to combat terrorist financing, assisting jurisdictions in implementing financial provisions of the United Nations Security Council resolutions on terrorism, and evaluating countries' ability to prevent, detect, investigate,

---

crypto-boom-upbit-is-now-a-top-global-exchange-by-volume (Accessed November 10, 2025).

75) United Nations Security Council, "Annex 62: Consolidated List of Recommendations," *Report of the Panel of Experts Established Pursuant to Resolution 1874*, August 28, 2020, https://www.securitycouncilreport.org/atf/cf/%7B65BFCF9B-6D27-4E9C-8CD3-CF6E4FF96FF9%7D/s_2020_840.pdf (Accessed June 2, 2025), p. 210.

and prosecute the financing of terrorism.[76] In regard to WMD proliferation financing, the FATF Recommendations require countries and the private sector to identify and assess the risks of potential breaches, non-implementation, or evasion of the targeted financial sanctions related to proliferation financing, and take appropriate mitigating measures commensurate with the level of risks identified.[77]

Additionally, we have seen increased international cooperation to combat cyberattacks by belligerent states. The U.S. National Security Agency, the U.S. Federal Bureau of Investigation (FBI), South Korea's National Intelligence Service, the United Kingdom's National Cyber Security Centre (NCSC), and others released a joint cybersecurity advisory to publicize North Korean activities and encourage critical infrastructure organizations to strengthen their cyber defenses by providing detection methods and mitigation measures.[78] We have also seen ongoing trilateral cooperation between the United States, South Korea, and Japan to respond to North Korea's threats in cyberspace, including cryptocurrency abuses and space launches.[79]

Moving forward, South Korea and the United States, as primary targets of North Korean cyber aggression, will need to continue their cyber defense cooperation and actively identify and develop joint response measures that can impose real pressure on North Korea. In doing so, some strategies[80] to institutionalize practical and active action include

---

76) The Financial Action Task Force, "FATF's global efforts on combating terrorist financing," https://www.fatf-gafi.org/en/topics/Terrorist-Financing.html (Accessed June 16, 2024).

77) The Financial Action Task Force, "Proliferation financing," https://www.fatf-gafi.org/en/topics/proliferation-financing.html (Accessed June 16, 2024).

78) Joint Cybersecurity Advisory, "North Korea Cyber Group Conducts Global Espionage Campaign to Advance Regime's Military and Nuclear Programs," July 25, 2024, https://media.defense.gov/2024/Jul/25/2003510137/-1/-1/0/Joint-CSA-North-Korea-Cyber-Espionage-Advance-Military-Nuclear-Programs.PDF (Accessed June 16, 2025).

79) *Reuters*, "U.S., South Korea, Japan to step up actions on North Korea cyber threats," December 9, 2023, https://www.reuters.com/world/us-skorea-japan-security-advisors-seoul-trilateral-meeting-2023-12-09/ (Accessed June 16, 2025).

coordinated sanctions with global cryptocurrency exchanges, the disruption of laundering pathways, and continued efforts to track and freeze stolen crypto assets should be pursued in tandem as a strategic way forward toward denying North Korea its financial benefits.

On a broader level, international cooperation should be directed towards stymying similar attempts by belligerent states such as China, Russia, and Iran. North Korea is not the only actor using cyber operations to conduct espionage and financially motivated attacks. Regarding China, for example, CrowdStrike's 2025 Global Threat Report finds that targeted attacks in financial services, media, manufacturing, and the industrial sectors rose to 300%.[81] The Russian government engages in malicious cyber activities to enable broad-scope cyber espionage, to suppress certain social and political activity, to steal intellectual property, and to harm regional and international adversaries; while the Iranian government has exercised its increasingly sophisticated cyber capabilities to suppress certain social and political activity, and to harm regional and international adversaries.[82] A more concrete and institutionalized response plan that coordinates between intergovernmental and governmental agencies with financial institutions will go a long way towards defense from cyber-attacks aimed at illicitly extorting digital currency that subsequently goes on to channel funding towards belligerency.

80) Bae (2025).

81) *Cyber Magazine*, "China's Cyber Espionage Surges 150%, Says CrowdStrike," February 28, 2025, https://cybermagazine.com/articles/chinas-cyber-espionage-surges-150-says-crowdstrike (Accessed June 16, 2025).

81) Bae (2025).

82) America's Cyber Defense Agency.

[References]

Boo, Hyeong-wook. "An Assessment of North Korean Cyber Threats." *The Journal of East Asian Affairs,* Vol. 31, No.1 (2017).

Byman, Daniel. *Deadly Connections: States That Sponsor Terrorism* (Cambridge: Cambridge University Press, 2007).

_____. "Understanding, and Misunderstanding, State Sponsorship of Terrorism." *Studies in Conflict & Terrorism*, Vol. 45, No. 12 (2022).

Byun, Sang-jung and Junghyun Yoon. *The Evolution of North Korea's Cyber Influence Operations and Its Implications* (Seoul: Institute for National Security Strategy, 2024).

Claridge, David. "State terrorism? Applying a definitional model." *Terrorism and Political Violence*, Vol. 8, No. 3 (1996).

Davis, Jessica. *Women in Modern Terrorism: From Liberation Wars to Global Jihad and the Islamic State* (Lanham: Rowman & Littlefield, 2017).

De Falco, Marco LTC. "Stuxnet Facts Report: A Technical and Strategic Analysis." (Tallinn: NATO Cooperative Cyber Defense Centre of Excellence, 2012).

Denning, Dorothy E. "Cyberterrorism: The Logic Bomb Versus the Truck Bomb." *Global Dialogue*, Vol. 2, No. 4 (2000).

Dion-Schwarz, Cynthia, David Manheim, and Patrick B. Johnston. *Terrorist Use of Cryptocurrencies: Technical and Organizational Barriers and Future Threats* (Santa Monica, CA: RAND Corporation, 2019).

Harry, Charles and Nancy Gallagher. "Classifying Cyber Events: A Proposed Taxonomy." *Journal of Information Warfare*, Vol. 17, No. 3 (2018).

Heryanto, Ariel. *State Terrorism and Political Identity in Indonesia: Fatally Belonging* (New York: Routledge, 2006).

Hoffman, Bruce. *Inside Terrorism* (New York: Columbia University Press, 2017).

Holden, William N. "Ashes from the phoenix: state terrorism and the party-list groups in the Philippines." *Contemporary Politics*, Vol. 15, No. 4 (2009).

Ireland, Carol A, Michael Lewis, Anthony Lopez and Jane L. Ireland. *The Handbook of Collective Violence: Current Developments and Understanding* (London: Routledge, 2020).

Jun, Jenny, Scott LaFoy, and Ethan Sohn. *North Korea's Cyber Operations: Strategy and Responses* (Washington D.C.: Center for Strategic & International Studies, 2015).

Kim, Chong Woo and Carolina Polito. *The Evolution of North Korean Cyber Threats* (Seoul: Asan Institute for Policy Studies, 2019).

Klingner, Bruce. "North Korean Cyberattacks: A Dangerous and Evolving Threat." *The Heritage Foundation Special Report*, No.247 (2021).

Mansourov, Alexandre. *North Korea's Cyber Warfare and Challenges for the U.S.-ROK Alliance* (Washington D.C.: Korea Economic Institute of America, 2014).

Margolin, Devorah and Matthew Levitt. "The Road to October 7: Hamas' Long Game, Clarified." *CTC Sentinel*, Vol. 16, No. 10 (2023).

Matusitz, Jonathan. "Cyberterrorism: Postmodern State of Chaos." *Information Security Journal: A Global Perspective,* Vol. 17, No. 4 (2008).

Miller, Rena S., Liana W. Rosen, and Paul Tierno. "Terrorist Financing: Hamas and Cryptocurrency Fundraising." *US Congressional Research Service IF12537* (2024).

Plotnek, Jordan J. and Jill Slay. "Cyber Terrorism: A Homogenized Taxonomy and Definition." *Computers & Security,* Vol. 102 (2021).

Rekawek, Kacper. "Russian State Terrorism and State Sponsorship of Terrorism." *International Centre for Counter-Terrorism Report* (2024).

Rollins, John W. and Clay Wilson. "Terrorist Capabilities for Cyber-attack: Overview and Policy Issues." *US Congressional Research Service Report RL33123* (2007).

Schweitzer, Yoram, Gabi Siboni, and Einav Yogev. "Cyberspace and Terrorist Organizations." *Military and Strategic Affairs,* Vol. 3, No. 3 (2011).

Thaler, Kai M. "Delegation, Sponsorship, and Autonomy: An Integrated Framework for Understanding Armed Group-State Relationships." *Journal of Global Security Studies*, Vol. 7, No. 1 (2021).

Theohary, Catherine A. and John W. Rollins. "Cyberwarfare and Cyberterrorism: In Brief." *US Congressional Research Service Report R43955* (2015).

Zanotti, Jim. "Hamas: Background, Current Status, and U.S. Policy." *US Congressional Research Service IF12549* (2024).

〈News〉

BBC. "North Korean hackers cash out hundreds of millions from $1.5bn ByBit hack." March 10, 2025. https://www.bbc.com/news/articles/c2kgndwwd7lo (Accessed March 14, 2025).

Bloomberg. "Upbit Rides Korea Crypto Boom to Top-Five Global Exchange

Spot." April 25, 2024. https://www.bloomberg.com/news/articles/2024-04-25/korean-crypto-boom-upbit-is-now-a-top-global-exchange-by-volume (Accessed November 10, 2025).

Business Insider. "The Stuxnet Attack on Iran's Nuclear Plant Was 'Far More Dangerous' than Previously Thought." November 21, 2013. http://www.businessinsider.com/stuxnet-was-far-more-dangerous-than-previous-thought-2013-11 (Accessed November 24, 2025).

CBC News. "How tiny Qatar hosts the leaders of Hamas without consequences." October 18, 2023. https://www.cbc.ca/news/politics/qatar-hamas-israel-1.6999416 (Accessed June 12, 2025).

CNN. "Half of North Korean missile program funded by cyberattacks and crypto theft, White House says." May 10, 2023. https://edition.cnn.com/2023/05/10/politics/north-korean-missile-program-cyberattacks (Accessed June 6, 2025).

Cyber Magazine. "China's Cyber Espionage Surges 150%, Says CrowdStrike." February 28, 2025. https://cybermagazine.com/articles/chinas-cyber-espionage-surges-150-says-crowdstrike (Accessed June 16, 2025).

India Today. "Stolen from Delhi, sent to Hamas: What Delhi Police's crypto probe found." October 11, 2023. https://www.indiatoday.in/india/story/stolen-delhi-funneled-to-israel-hamas-war-delhi-police-cryptocurrency-probe-bitcoin-hamas-israel-war-2447435-2023-10-11 (Accessed March 14, 2025).

The Associated Press. "North Korean GPS manipulation disrupted dozens of planes and vessels, South Korea says." November 9, 2024. https://apnews.com/article/north-korea-gps-interference-jamming-aircraft-nuclear-2f6a345ffd3bcf2875b04a758658c9c7 (Accessed April 15, 2025).

The New York Times. "Hamas Leader Abandons Longtime Base in Damascus." January 27, 2012. https://www.nytimes.com/2012/01/28/world/middleeast/khaled-meshal-the-leader-of-hamas-vacates-damascus.html (Accessed July 25, 2025).

The New Yorker. "The Incredible Rise of North Korea's Hacking Army." April 19, 2021. https://www.newyorker.com/magazine/2021/04/26/the-incredible-rise-of-north-koreas-hacking-army (Accessed March 30, 2025).

The Record from Recorded Future News. "North Korean hacking group targeted

weapons blueprints, nuclear facilities in cyber campaigns." July 25, 2024. https://therecord.media/north-korea-andariel-apt45-weapons-systems-nuclear-facilities (Accessed June 6, 2025).

The Wall Street Journal. "From Hamas to North Korean Nukes, Cryptocurrency Tether Keeps Showing Up." October 27, 2023. https://www.wsj.com/finance/currencies/most-popular-cryptocurrency-keeps-showing-up-in-illicit-finance-71d32e5e (Accessed April 15, 2025).

Times of India. "Cryptocurrency stolen from Delhi lands in Hamas wallets." October 11, 2023. https://timesofindia.indiatimes.com/city/delhi/cryptocurrency-stolen-from-delhi-lands-in-hamas-wallets/articleshow/104327800.cms (Accessed March 14, 2025).

Reuters. "Factbox: What Is Stuxnet?" September 24, 2010. http://www.reuters.com/article/2010/09/24/us-security-cyber-iran-fb-idUSTRE68N3PT20100924 (Accessed November 24, 2025).

_____. "Who funds Hamas? A global network of crypto, cash and charities." October 16, 2023. https://www.reuters.com/world/middle-east/hamas-cash-to-crypto-global-finance-maze-israels-sights-2023-10-16/ (Accessed May 30, 2025).

_____. "Qatar open to reconsidering Hamas presence in Qatar, US official says." October 27, 2023. https://www.reuters.com/world/middle-east/qatar-told-us-it-is-open-reconsidering-hamas-presence-us-official-says-2023-10-27/ (Accessed June 15, 2025).

_____. "U.S., South Korea, Japan to step up actions on North Korea cyber threats." December 9, 2023. https://www.reuters.com/world/us-skorea-japan-security-advisors-seoul-trilateral-meeting-2023-12-09/ (Accessed June 16, 2025).

_____. "Exclusive: UN experts investigate 58 cyberattacks worth $3 bln by North Korea." February 8, 2024. https://www.reuters.com/technology/cybersecurity/un-experts-investigate-58-cyberattacks-worth-3-bln-by-north-korea-2024-02-08/ (Accessed March 14, 2025).

_____. "FBI says North Korea was responsible for $1.5 billion ByBit hack." February 28, 2025. https://www.reuters.com/technology/cybersecurity/fbi-says-north-korea-was-responsible-15-billion-bybit-hack-2025-02-27/ (Accessed March 14, 2025).

The Washington Post. "Stuxnet was work of U.S. and Israeli experts, officials say." June 2, 2012. https://www.washingtonpost.com/world/national-

security/stuxnet-was-work-of-us-and-israeli-experts-officials-say/2012/06/01/gJQAlnEy6U_story.html (Accessed November 24, 2025).

Yonhap News Agency. "U.S. Intelligence Chiefs Pick N. Korea as Major Cyber Threat." January 6, 2017. https://en.yna.co.kr/view/AEN20170106000200315 (Accessed March 14, 2025).

〈Internet Sources〉

America's Cyber Defense Agency. "Nation-State Threats." https://www.cisa.gov/topics/cyber-threats-and-advisories/nation-state-cyber-actors (Accessed March 24, 2025).

Bae, Sunha. "Deterrence Under Pressure: Sustaining U.S.-ROK Cyber Cooperation Against North Korea." *Center for Strategic and International Studies*. April 1, 2025. https://www.csis.org/analysis/deterrence-under-pressure-sustaining-us-rok-cyber-cooperation-against-north-korea (Accessed June 6, 2025).

Bastug, Mehmet F. and Ismail Onat. "Cyberterrorism." *Oxford Research Encyclopedia of Criminology*. March 20, 2024. https://oxfordre.com/criminology/view/10.1093/acrefore/9780190264079.001.0001/acrefore-9780190264079-e-790 (Accessed November 10, 2025).

Computer Security Resource Center. "Cyber attack – Glossary." https://csrc.nist.gov/glossary/term/cyber_attack (Accessed November 24, 2025).

Horschig, Doreen. "How Are Cyberattacks Fueling North Korea's Nuclear Ambitions?" *Center for Strategic and International Studies*. July 31, 2024. https://www.csis.org/analysis/how-are-cyberattacks-fueling-north-koreas-nuclear-ambitions (Accessed June 6, 2025).

HP Security Research. "Profiling an enigma: The mystery of North Korea's cyber threat landscape." August 2014. *HP Security Briefing Episode 16*. https://time.com/wp-content/uploads/2014/12/hpsr_securitybriefing_episode16_northkorea.pdf (Accessed June 3, 2025).

Joint Cybersecurity Advisory. "North Korea Cyber Group Conducts Global Espionage Campaign to Advance Regime's Military and Nuclear Programs." July 25, 2024. https://media.defense.gov/2024/Jul/25/2003510137/-1/-1/0/Joint-CSA-North-Korea-Cyber-Espionage-Advance-Military-Nuclear-Programs.PDF (Accessed June 16, 2025).

Lewis, James Andrew. "The Likelihood of North Korean Cyber Attacks." *Center for Strategic & International Studies*. September 7, 2017. https://www.

csis.org/analysis/likelihood-north-korean-cyber-attacks (Accessed March 14, 2025).

Office of the Director of National Intelligence. "Annual Threat Assessment of the U.S. Intelligence Community." February 5, 2024. https://www.dni.gov/files/ODNI/documents/assessments/ATA-2024-Unclassified-Report.pdf (Accessed March 14, 2025).

_____. "Annual Threat Assessment of the U.S. Intelligence Community." March 25, 2025. https://www.dni.gov/files/ODNI/documents/assessments/ATA-2025-Unclassified-Report.pdf (Accessed June 6, 2025).

Robinson, Kali. "What is Hamas?" *Council on Foreign Relations*. October 31, 2023. https://www.cfr.org/backgrounder/what-hamas (Accessed May 25, 2024).

Statistica. "Daily cryptocurrency trading volume on South Korean and global exchanges as of August 3, 2021." June 26, 2024. https://www.statista.com/statistics/1261206/south-korea-trading-volume-on-local-and-global-crypto-exchanges/ (Accessed June 3, 2025).

Suh, Elizabeth. "North Korea's Cyber Capabilities and Strategy." *German Council on Foreign Relations*. January 7, 2022. https://dgap.org/en/research/publications/north-koreas-cyber-capabilities-and-strategy-0 (Accessed April 15, 2025).

The Cyber Threat Intelligence Integration Center. "North Korea Tactics, Techniques, and Procedures for Revenue Generation." July 2023. https://www.dni.gov/files/CTIIC/documents/products/North-Korean-TTPs-for-Revenue-Generation.pdf (Accessed March 14, 2025).

The Financial Action Task Force. "FATF's global efforts on combating terrorist financing." https://www.fatf-gafi.org/en/topics/Terrorist-Financing.html (Accessed June 16, 2024).

_____. "Proliferation financing." https://www.fatf-gafi.org/en/topics/proliferation-financing.html (Accessed June 16, 2024).

TRM Labs. "Inside North Korea's Crypto Heists: $200M in Crypto Stolen in 2023; Over $2B in the Last Five Years." August 18, 2023. https://www.trmlabs.com/resources/blog/inside-north-koreas-crypto-heists (Accessed March 14, 2025).

_____. "US DOJ Charges Hamas Leaders with October 7 Attacks, Details

Hamas' Use of Cryptocurrencies." September 4, 2024. https://www.trmlabs.com/resources/blog/us-doj-charges-hamas-leaders-with-october-7-attacks-details-hamas-use-of-cryptocurrencies (Accessed March 14, 2025).

United Nations Security Council. "Annex 62: Consolidated List of Recommendations." *Report of the Panel of Experts Established Pursuant to Resolution 1874*. August 28, 2020. https://www.securitycouncilreport.org/atf/cf/%7B65BFCF9B-6D27-4E9C-8CD3-CF6E4FF96FF9%7D/s_2020_840.pdf (Accessed June 2, 2025).

United States Department of Justice. "Global Disruption of Three Terror Finance Cyber-Enabled Campaigns." August 13, 2020. https://www.justice.gov/archives/opa/pr/global-disruption-three-terror-finance-cyber-enabled-campaigns (Accessed March 29, 2025).

United States Department of State. "State Sponsors of Terrorism." August 18, 2011. https://2009-2017.state.gov/j/ct/rls/crt/2010/170260.htm (Accessed July 25, 2025).

[국문초록]

사이버공간에서의 테러와 재원조달 방법의 암행화: 북한과 하마스의 사례 분석

양지혜 | 고려대학교 일민국제관계연구원 객원연구원

지난 10여 년간 북한은 사이버 작전을 전략적으로 고도화하며, 전통적인 정보수집 활동을 넘어 국제 금융 시스템을 겨냥한 정교한 공격을 수행해 왔다. 이러한 활동은 국제사회의 제재를 우회하고 불법적인 수익을 창출하기 위한 수단으로 활용되고 있다. 핵이나 미사일 도발과 달리, 사이버 공격은 민간 인프라 및 금융 안정성에 심대한 영향을 미치고 있음에도 불구하고, 국제사회의 명확한 비난이나 추가 제재 조치 없이 간과되는 경우가 많다. 본 연구는 북한과 하마스를 사례로, 국가 및 비국가 행위자에 의한 사이버테러 현상을 분석하고, 이들이 사이버화폐를 어떻게 활용하여 재정적 이득을 도모하고 향후 적대 행위 및 폭력을 준비하는지를 비교·고찰한다. 본 연구는 사이버테러가 비국가 행위자에 국한된 개념이 아니라, 사이버 공간을 협박, 혼란, 테러의 수단으로 악용하는 적대적 국가 행위자까지 포괄하여 개념을 재정립할 필요가 있음을 제기한다. 하마스의 자금조달 방식과 북한 사이버 부대의 전술적 진화를 분석함으로써, 현대 사이버 작전에서 범죄적 동기와 정치적 목적이 결합되는 양상을 조명한다. 하마스와 달리 북한의 경우, 암호화폐 시장을 조직적으로 악용하고 있음을 중점적으로 분석하며, 이러한 활동이 단기적인 경제적 피해에 그치지 않고 장기적인 무력 충돌의 재원을 마련하는 기반이 되고 있다는 점을 강조한다. 결론적으로, 본 연구는 사이버 작전의 이중용도(dual-use)적 성격—즉, 전쟁과 테러 수단으로 기능할 수 있다는 점—에 주목하며, 이를 규율할 수 있는 국제적 제도와 정책적 대응의 시급한 정비 필요성을 강조한다.

주제어: 북한, 하마스, 사이버테러, 전자화폐

투 고 일: 2025.06.16.
심 사 일: 2025.06.23.
게재확정일: 2025.06.24.