Issue Brief

Vol.108, No.5, 2024

The Evolution of North Korea's Cyber Influence Operations and Its Implications

Sang-jung Byun
(Senior Research Fellow, INSS)
Junghyun Yoon
(Research Fellow, INSS)

INSS INSTITUTE FOR NATIONAL SECURITY STRATEGY
국가안보전략연구원

Abstract

North Korea has intensified its focus on cyber attacks within the realm of 'influence operations,' covertly shaping or distorting public opinion. The threat posed by North Korea's cyber influence operations lies in its ability to carry them out, alongside the increasing likelihood of deploying more sophisticated and effective operations, leveraging various attack techniques and information assets. Given the severity of North Korea's cyber influence operations, it is imperative to pay attention to institutional improvements in democratic countries aimed at blocking influence operations and proactively responding to the evolving strategies of North Korean cyber influence. Considering North Korea's vulnerable cyber environment compared to its offensive capabilities, it is critical to enhance our capabilities in line with the principles of an 'offensive cyber security strategy.' This includes improving institutional frameworks to support enhancing preemptive tracking and exploration capabilities, counter-operations against North Korean internal and external points, and nurturing white-hat hackers. Moreover, continuous efforts should be made to inform the public that such 'offensive principles' are the beginning of safeguarding democratic values and social interests and building social consensus.

Keywords

North Korea, Cyber Influence Operations, Cyber Security Strategy, Lazarus Group, Social Engineering

The Evolution of North Korea's Cyber Influence Operations and Its Implications

Sang-jung Byun
(Senior Research Fellow, INSS)
Junghyun Yoon
(Research Fellow, INSS)

At the 9th Plenary Meeting of the 8th Party held last year, Kim Jong-un abolished the concept of 'nation' and declared 'unification by force.' Additionally, North Korea completely changed its strategy towards South Korea, defining inter-Korean relations as "two hostile and warring countries," and has continued to engage in aggressive military demonstrations to this day. Notably, beyond traditional military displays such as missile provocations, it persists in covert and omnidirectional attacks targeting unspecified individuals in cyberspace. Of particular concern is the dissemination and proliferation of disinformation and fake news through social media, causing social conflict and eroding trust in government policies.

The recent hacking incident involving the Supreme Court of the Republic of Korea's computer network and the official X (formerly Twitter) account of the Ministry of Health and Welfare (MOHW) cannot be merely viewed as a "cyber breach incident." This is because the hacking group suspected to be from North Korea could potentially spread false information and fake news based on the large-scale personal information they have stolen, thereby sowing confusion in our society, particularly on economic, social, and health volatile issues.

An "influence operation" is "a sophisticated information warfare and psychological warfare aimed at changing the opinion and policies of other countries to be favorable to one's own country through various information dissemination and message delivery." Today, influence operations predominantly occur in cyberspace via online media, communities, and social platforms. North Korea's cyber influence operations executed in various ways have garnered significant attention not only domestically but also internationally in recent years. These operations primarily aim to achieve economic and political goals, serving as strategic attempts to maximize its interests amidst international sanctions and isolation. As high-intensity sanctions against North Korea persist, North Korean authorities actively seek new ways to generate revenue using the cyber domain, offering favorable conditions for low-cost execution and evasion of sanctions surveillance. North Korea has enhanced its cyber capabilities to achieve economic gain, gather information, and expand its political influence. Given Kim Jong-un's directive that "cyber warfare is an 'all-purpose sword' supporting the merciless attack capabilities of the People's Army along with nuclear weapons and missiles," further evolution in cyber hacking and influence operation methods is anticipated.

Goals of North Korea's Cyber Influence Operations

Firstly, North Korea's cyber influence operations aim to expand political influence. North Korea has made attempts to intervene in other countries' political processes to undermine their political stability or exert influence in the international community. Examples include cyberattacks to influence elections and manipulation of public opinion. North Korea possesses the technical and organizational capabilities to conduct such cyber influence operations professionally. Hackers affiliated with the North's Reconnaissance General Bureau and Pyongyang's Primary Intelligence Bureau continue to launch sophisticated cyberattacks,

posing a significant threat and challenge to government agencies, critical industrial facilities, and security professionals in major countries.

Secondly, North Korea conducts cyber espionage against government organizations and companies to gather critical intelligence in the military, political, and economic fields to shape its foreign policy and strategy.

Thirdly, North Korea's cyber influence campaigns also involve securing illicit funds. To alleviate economic pressure from international sanctions, North Korea raises funds through cyberattacks on financial institutions. The large-scale personal information obtained by North Korea by hacking into South Korea's financial and public computer networks can be used for election interference, public opinion manipulation, cryptocurrency exchange attacks, and cyber fraud. This allows North Korea to secure economic revenues, including illicit funds, and sow distrust in other governments that fail to protect personal information.

The Threat of Cyber Influence Operations with Social Engineering

The extensive data stolen by the North Korean hacking organization, Lazarus Group, from South Korea's Supreme Court's computer network between January 2021 and February 2023 included a wide range of personal information, such as basic resident registration, personal rehabilitation applications, local tax assessments, and hospital medical certificates. If exploited, this information could provide easy access to personal social media and emails, making spear-phishing against celebrities easier. To attack prominent figures in society, information on acquaintances, social relationships, and activities is obtained in advance, gradually narrowing down the scope of attack, and ultimately enabling targeted attacks. The hacking and utilization of personal

information extend beyond mere leakage and can pose a serious threat to national security by incorporating social engineering techniques into influence operations.

Evolution of North Korea's Cyber Influence Operations

Another reason North Korean influence operations are so threatening is the sophistication with which they are executed, including through human commentary. While not on the scale of Russian and Chinese disinformation operations using mechanized fake accounts or "bots," human commentary is notable for its nuanced errors and consistent spelling and grammar mistakes. In particular, it is difficult to distinguish between comments from South Koreans who speak the same language and those from North Korean influence agents (Kim Eun Yong, 2023).

In recent years, North Korea has maximized the effectiveness of its social media influence operations through the use of linguistic commentary weapons to elicit emotional empathy from communities and influencers. A small North Korean commenting force can easily distort public opinion online based on targeted groups such as pro-North Korean organizations and social influencers. Furthermore, by using generative AI that has been sophisticatedly trained to create phishing emails, identify targets, and learn vulnerabilities, North Korea can multiply the effectiveness of its influence operations through human-machine teaming.

Additionally, North Korea is also adapting the content and techniques of its traditional intimidating and dogmatic propaganda campaigns to suit the 'MZ generation.' It is using its cyber-influencers to upload content to global platforms such as YouTube, TikTok, and Weibo. Examples include YouTubers "Yumi" and "Songa," who share their daily lives. These videos, with

subtitles in English, Chinese, Russian, and other languages, depict young North Koreans enjoying their daily lives in peace, portraying Kim Jong-un as a “leader who loves the people” of a “normal state” rather than an oppressive dictator.

Recently, short-form videos of tourist destinations and friendly scenes in North Korea have also emerged, seemingly filmed and uploaded by foreign tourists with permission from North Korean authorities. These videos do not criticize the hidden realities of the people or the surveillance of the North Korean guides but only mention the enjoyable experiences. These propaganda videos, utilizing cyber-influencers both domestically and internationally, are part of a sophisticated influence campaign to improve North Korea's public image.

Implications

North Korea's influence operations are expected to focus on spreading insecurity in South Korean society, undermining military cooperation between the United States, South Korea, and Japan, and intensifying propaganda and incitement through online and offline mass rallies and protests against the South Korean government. North Korea's Reconnaissance General Bureau, Primary Intelligence Bureau, and the Security Department have been monitoring the South Korean political sphere and public response to its declaration of “hostile relations” with South Korea and the dissolution of the organization managing inter-Korean relations. In addition, North Korea has launched a series of cyberattacks on major institutions and politicians in tandem with its ICBM and short-range ballistic missile launches.

To date, there have been few examples of publicly disclosed North Korean cyber influence operations, limiting the ability to analyze the threat of North Korean cyber influence operations

and formulate policy responses. Recent crackdowns on disinformation and institutionalization to prevent influence operations in liberal democracies provide instructive examples. The U.S. Department of Homeland Security has characterized election meddling as a "threat to the 'critical infrastructure' supporting liberal democracies." Canada's Ministry of Public Safety amended the CSIS Act to allow intelligence agencies to collect and share sensitive information and expand the scope of warrants for suspected influence peddlers. The European Union has recently imposed mandatory measures on big tech platforms such as Meta to strictly regulate political advertising and content management to prevent the spread of Russian disinformation.

A shift in response to North Korea's evolving cyber influence operations is necessary. The current government has declared the principle of an "offensive cyber security strategy" for national security issues, moving away from the previous defensive strategy. Considering North Korea's weaker defense capabilities, it is necessary to utilize our capabilities more proactively with an offensive approach. Improving the system to support proactive tracking and detection capabilities, counter-attacks on North Korea's critical centers, and the development of white-hat hackers is urgent. Furthermore, promoting to the public that this offensive approach is the beginning of protecting liberal democratic values and social interests, and working to build social consensus is crucial.

The views and opinions expressed in this report are those of the author(s) and do not necessarily reflect the official position of INSS.