The Journal of Illiberalism Studies
Vol. 4 No. 3 (2024): 11-19.

Digital Architecture of Control: North Korea's Use of Technology to Consolidate Totalitarian Governance

JIEUN BAEK

Abstract

North Korea's increasing technological sophistication is reshaping its approach to totalitarian governance. This article examines how the regime employs digital tools to consolidate state power through enhanced surveillance, regulatory frameworks, and ideological programming. It argues that the strategic integration of technology is central to North Korea's efforts to reinforce its totalitarian system, deter foreign influence, and suppress internal dissent. By analyzing both deterrent measures (including advanced surveillance technologies and restrictive laws) and offensive measures (including the proliferation of state-approved media), this article demonstrates how these efforts are shaping citizen behavior to align more closely with state expectations. Additionally, the article explores instances of quiet resistance, where citizens subvert state control through the very technologies designed to monitor them. The findings contribute to broader discussions on authoritarianism and the role of digital governance in sustaining repressive regimes, offering insights for policymakers seeking to counter these developments.

Keywords: North Korea, digital authoritarianism, surveillance technology, political control

Jieun Baek
Atlantic Council, USA
jbaek@atlanticcouncil.org

DOI: 10.53483/XCQT3578

Contrary to popular perceptions, North Korea is quickly becoming a technologically sophisticated state. While it remains true that 0% of the population has free and unfettered access to the internet, internet *does* exist in North Korea, although it is extremely limited and reserved for very specific purposes and users. The country has its own intranet connection, called *gwangmyeong*, and a Wi-Fi network connected to it called Mirae. An estimated 20% of North Koreans use the country's Mirae intranet Wi-Fi service, with around 7 million citizens owning North Korean smartphones and others using older models like flip phones.[1] In September 2024, North Korean state media showcased a foldable smartphone that was displayed at the annual "National Exhibition of IT Successes" at Kim Il-Sung University in Pyongyang.[2] The increasing presence of North Korean-branded tablets and smart televisions, coupled with a secondhand market for Western electronics, reflects a growing technological landscape within the country.[3] Moreover, with state approval, some citizens have created YouTube channels and X (formerly Twitter) accounts, presenting curated, state-approved content aimed at foreign audiences. These efforts are part of North Korea's broader public diplomacy initiative, designed to create a false perception of normalcy and progress to external observers.[4]

Beneath these seemingly progressive developments lies a more complex and insidious use of technology. North Korea is not merely adopting digital tools for societal convenience but is strategically employing them to reinforce its totalitarian system. By integrating the latest high technology into its surveillance apparatus, the regime has digitized and expanded its methods of control. The observable trendlines indicate that the country's information and communications technology (ICT) landscape will only grow more repressive, increasingly consolidated under state control and more difficult for external actors to penetrate. North Korea's investment in dual-use technologies—those that serve both civilian and military purposes—further exemplifies its commitment to leveraging technological advancements to fortify its authoritarian governance.

Despite economic setbacks related to covid-19 border closures and international sanctions, North Korea continues to demonstrate its technological capabilities. In 2022, the regime conducted 68 missile tests, the highest number ever recorded in a single year and a tenfold increase over 2021.[5] Simultaneously, the military has tested spy drones near the Demilitarized Zone (DMZ), while domestic industries released at least five new smartphone models that same year. North Korea's investment in asymmetric capabilities, particularly its rapidly advancing cyber operations, is a critical part of the regime's broader strategic objectives. The government has

1 Mun Dong Hui, "One of Five North Koreans Are Users of the Country's Wi-Fi Service," Daily NK (news site), June 26, 2023, https://www.dailynk.com/english/one-of-five-north-koreans-are-users-country-wi-fi-service/; Mun Dong Hui, "North Korea Focuses Efforts on Preventing Illegal Use of Mirae, a Popular Wi-Fi Network," Daily NK (news site), October 4, 2022, https://www.dailynk.com/english/north-korea-focuses-efforts-preventing-illegal-use-mirae-popular-wi-fi-network/.

2 Martyn Williams, "North Korea Gets a Folding Smartphone," North Korea Tech (blog), October 1, 2024, https://www.northkoreatech.org/2024/10/02/north-korea-gets-a-folding-smartphone/.

3 Jeong Tae Joo, "Liquid Crystal TVs Appear in Markets in Pyongyang, Kaesong and Kangwon Province," Daily NK (news site), February 10, 2023, https://www.dailynk.com/english/liquid-crystal-tvs-appear-markets-pyongyang-kaesong-kangwon-province/.

4 Oliver Hotham and Colin Zwirko, "What's up Pyongyang? North Korea Experiments with Vlogging to Fight 'Fake News,' " NK News (news site), May 18, 2020, https://www.nknews.org/2020/05/whats-up-pyongyang-north-korea-experiments-with-vlogging-to-fight-fake-news/.

5 "The CNS North Korea Missile Test Database," Nuclear Threat Initiative (blog), April 28, 2023, https://www.nti.org/analysis/articles/cns-north-korea-missile-test-database/.

harnessed its most skilled computer scientists, engineers, and hackers to develop and execute cyber operations that serve both domestic and international purposes.[6]

For more than a decade, North Korean students have consistently excelled in international hacking competitions, such as the International Collegiate Programming Competition and Hacker Earth, outpacing participants from prestigious institutions such as Harvard, MIT, Oxford, and Seoul National University.[7] These cyber capabilities have become instrumental in expanding the regime's capacity for disruption and theft, with cybercrime now a key revenue stream funding the state's weapons programs and espionage efforts.[8] Persistent cyberattacks targeting financial institutions, government bodies, healthcare systems, and critical infrastructure have been documented since the mid-2000s.[9] Additionally, North Korean cyber actors have stolen vast amounts of cryptocurrency to bolster the regime's finances. Such cyber activities, both offensive and defensive, are essential to the regime's strategy of maintaining internal control and deterring external influence.[10]

6 Mun Dong Hui, "North Korea Released at Least Five New Smartphone Models Last Year," Daily NK (news site), April 17, 2023, https://www.dailynk.com/english/north-korea-released-at-least-five-new-smartphone-models-last-year/; Martyn Williams, "Smartphones of North Korea," Lumen (NGO website), September 2024, https://www.lumen.global/smartphones-of-north-korea.

7 Reddy Shreyas, "North Korean Students Win Hacking Contest Hosted by US-Based Firm: State Media," NK News (news site), July 3, 2023, https://www.nknews.org/2023/07/north-korean-students-win-hacking-contest-hosted-by-us-based-firm-state-media/; Kelly Kasulis, "North Koreans Sharpen Their Cyber Skills at Online Coding Competitions," NK News, NK PRO, April 2, 2021, https://www.nknews.org/pro/north-koreans-sharpen-their-cyberskills-at-online-coding-competitions/.

8 "US Treasury Targets DPRK Malicious Cyber and Illicit IT Worker Activities," US Department of the Treasury, June 27, 2023, https://home.treasury.gov/news/press-releases/jy1498. the Department of the Treasury's Office of Foreign Assets Control (OFAC

9 ChainalysisTeam, "North Korean Hackers Have Prolific Year as Their Unlaundered Cryptocurrency Holdings Reach All-Time High," Chainalysis (blog), January 13, 2022, https://blog.chainalysis.com/reports/north-korean-hackers-have-prolific-year-as-their-total-unlaundered-cryptocurrency-holdings-reach-all-time-high/; "North Korean Foreign Trade Bank Rep Charged for Role in Two Crypto Laundering Conspiracies," US Department of Justice, April 24, 2023, https://www.justice.gov/usao-dc/pr/north-korean-foreign-trade-bank-rep-charged-role-two-crypto-laundering-conspiracies; Sean Lyngaas, "Here's How North Korean Operatives Are Trying to Infiltrate US Crypto Firms," CNN, July 10, 2022, https://www.cnn.com/2022/07/10/politics/north-korean-hackers-crypto-currency-firms-infiltrate/index.html; Aaron Schaffer, "North Korean Hackers Linked to $620 Million Axie Infinity Crypto Heist," *Washington Post*, April 14, 2022, https://www.washingtonpost.com/technology/2022/04/14/us-links-axie-crypto-heist-north-korea/; "Three North Korean Military Hackers Indicted in Wide-Ranging Scheme to Commit Cyberattacks and Financial Crimes across the Globe," US Department of Justice, February 17, 2021, https://www.justice.gov/opa/pr/three-north-korean-military-hackers-indicted-wide-ranging-scheme-commit-cyberattacks-and.

10 "Guidance on the North Korean Cyber Threat," US Cybersecurity and Infrastructure Security Agency, June 23, 2020, https://www.cisa.gov/news-events/cybersecurity-advisories/aa20-106a; "North Korean State-Sponsored Cyber Actors Use Maui Ransomware to Target the Healthcare and Public Health Sector," US Cybersecurity and Infrastructure Security Agency, July 7, 2022, https://www.cisa.gov/news-events/cybersecurity-advisories/aa22-187a.

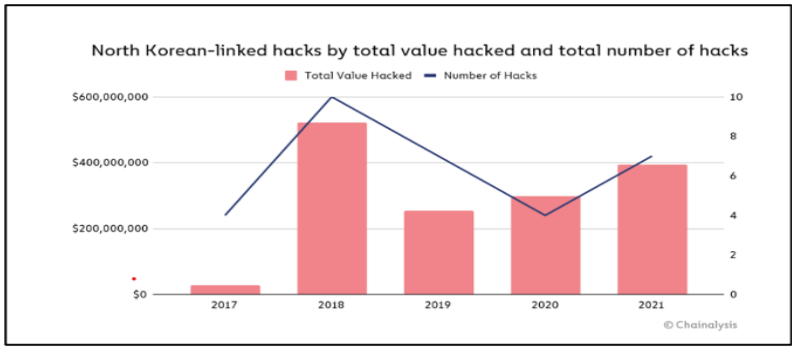

Figure 1. North Korean-linked hacks by total value hacked and total number of hacks. Used with permission from Chainalysis.

North Korean hackers pose a significant threat to global institutions and companies, including major technology firms and government agencies.[11] Notable cyberattacks, such as the 2014 Sony hack conducted in retaliation for the release of the film *The Interview*, and the 2017 WannaCry ransomware attack, which severely disrupted the UK's National Health Service, illustrate the far-reaching consequences of North Korean cyber operations. The infamous Lazarus Heist, an attempt to steal $1 billion from the Bangladesh Central Bank, resulted in the theft of $81 million before the fraudulent transfer was intercepted.[12] North Korean hackers have repeatedly targeted South Korea, attacking sectors ranging from nuclear energy to chip manufacturing, as well as government offices including the South Korean president's aide's email.[13]

In addition to cyber activities, North Korea deploys thousands of IT workers overseas to generate revenue for the regime. These workers, estimated at around 3,000, operate under false identities in countries across Africa, Southeast Asia as well as China and Russia, often subcontracting with major companies, including American firms. While these IT workers are not directly involved in domestic surveillance, their technological expertise underscores North Korea's growing capacity to evade international sanctions and reinforce its domestic control mechanisms. The regime's sustained investment in artificial intelligence (AI) research and biometric technologies, as exemplified by institutions like the Kim Il Sung High-Tech Development Institute, highlights the intersection of academia, government, and technological ambitions.[14]

11 "How We're Protecting Users from Government-Backed Attacks from North Korea," Google's Threat Analysis Group, April 5, 2023, https://blog.google/threat-analysis-group/how-were-protecting-users-from-government-backed-attacks-from-north-korea/; "Active North Korean Campaign Targeting Security Researchers." A. J. Vicens, "North Korean Hackers Used Polished LinkedIn Profiles to Target Security Researchers," CyberScoop (blog), March 10, 2023, https://cyberscoop.com/north-korea-hackers-linkedin-phishing/.

12 Geoff White, *The Lazarus Heist: From Hollywood to High Finance—Inside North Korea's Global Cyber War*, (London: Penguin, 2023)

13 For a more detailed list and descriptions of the types of threats that the North Korean hackers pose, see the US Cybersecurity and Infrastructure Security Agency, "North Korea Cyber Threat Overview and Advisories," US Cybersecurity and Infrastructure Security Agency website, accessed May 4, 2023, https://www.cisa.gov/northkorea.

14 US Office of Foreign Assets Control, "Publication of North Korea Information Technology Workers Advisory," US Office of Foreign Assets Control website, accessed May 4, 2023, https://ofac.treasury.gov/recent-actions/20220516; US Department of the Treasury, "US Treasury Targets DPRK Malicious Cyber and Illicit IT Worker Activities,"the Department of the Treasury's Office of Foreign Assets Control (OFAC https://home.treasury.gov/news/press-releases/jy1498.

Given the regime's disproportionately favorable outcomes from its cyber activities relative to the resources it invests, it is likely that North Korea will continue expanding its cyber operations abroad while enhancing its domestic surveillance capabilities. This trajectory is reinforced by North Korea's investments in artificial intelligence, biometric recognition, and other advanced technologies.[15] North Korean universities and research institutions are actively engaged in these fields, contributing to both civilian and military applications. The regime's strategic focus on technology reflects its long-term goal of consolidating power through digital means.

This article aims to contribute to the understanding of North Korea's strategic use of technology in reinforcing its totalitarian governance. By analyzing both deterrent and offensive measures, the article elucidates how the regime effectively employs technology to create a controlled information environment, ensuring that citizen behavior increasingly aligns with state expectations. It begins by examining two principal deterrent measures: (1) the deployment of advanced surveillance technologies and (2) the implementation of restrictive legal frameworks. These tools have been instrumental in consolidating state power, enhancing the regime's ability to monitor, control, and suppress dissent.

In addition to these deterrent strategies, the article explores three offensive measures designed to fortify the regime's ideological control: (1) the enhancement of ideological programming aimed at countering foreign influence, (2) the establishment of social norms and role models that align with state-sanctioned behavior, and (3) the provision of alternative media and entertainment to shape domestic cultural consumption. These strategies have collectively contributed to observable shifts in citizen behavior, which now more closely reflect the government's ideological objectives.

The article also addresses the ways in which some North Korean individuals subtly resist state control by leveraging the same technologies designed to monitor them. By engaging in quiet forms of defiance and exploiting technological loopholes, these individuals demonstrate that, despite the regime's extensive control mechanisms, opportunities for quiet subversion exist. The analysis of this dynamic underscores the complex interplay between state power and individual agency in highly controlled environments.

This article strives to advance the scholarly discourse on digital authoritarianism by demonstrating how North Korea's growing technological investments have fortified its authoritarian methods, making the regime more efficient and resilient. The article concludes with recommendations for policymakers and researchers seeking to counter the effects of North Korea's digital totalitarianism, offering insights into potential strategies for weakening the regime's control over information and promoting more open access to external ideas and content.

Methodology and Data

The insights presented in this article are drawn from qualitative data collected through interviews with North Korean defectors, a hard-to-reach population due to the highly secretive nature of the regime and the significant risks associated with

15 Hyuk Kim, "North Korea's Artificial Intelligence Research: Trends and Potential Civilian and Military Applications," 38 North (blog), Stimson Center, January 23, 2024, https://www.38north.org/2024/01/north-koreas-artificial-intelligence-research-trends-and-potential-civilian-and-military-applications/; Tai Wei Lim, "North Korea's Artificial Intelligence (A.I.) Program," *North Korean Review* 15, no. 2 (Fall 2019): 97–103, https://www.jstor.org/stable/26915828. particularly its sub-field machine learning (ML

defection. Although these interviews were not conducted explicitly for the purposes of this article, they are the result of longitudinal fieldwork that I have undertaken in recent years as part of my broader academic and professional engagement with North Korean political dynamics and human rights issues.

Ethical considerations have been at the forefront of this research process, given the sensitive and precarious circumstances of many interviewees. Rigorous measures were implemented to ensure the protection of participants' identities and well-being. Informed consent was obtained from all participants, with detailed explanations provided about the research aims and potential risks. All identifying details were anonymized to safeguard the safety of the participants, and great care was taken to ensure that their experiences were represented with accuracy and sensitivity, particularly within the broader context of North Korea's evolving ICT and surveillance strategies.

As a Korean-American female academic and practitioner with extensive experience in the North Korean research and human rights field, my positionality plays a significant role in collecting qualitative data. Over two decades of active engagement in this space have afforded me both cultural insight and a high degree of trust within hard-to-reach networks of North Korean defectors, particularly those from elite backgrounds with direct experience in sectors critical to this article's focus. This privileged access has allowed me to gather firsthand accounts and nuanced perspectives. These unique opportunities are especially crucial in the context of studying North Korea's deployment of digital technologies to reinforce its authoritarian governance.

As both a practitioner and an academic involved in information operations targeting North Korea, my dual role provides distinct advantages but also requires critical reflection on the implications of my embedded position. This dual positionality grants me privileged access to sensitive networks and valuable insights into the inner workings of North Korea's digital surveillance apparatus. However, it also necessitates careful attention to the potential influence my professional background may exert on the responses of interviewees as well as my own assumptions. Throughout the research process, I have remained vigilant in maintaining an open and reflective stance, ensuring that the participants' voices as data are not overshadowed by preconceived assumptions.

Through leveraging my extensive network and relationships within networks of North Korean defectors, this article strives to offer a novel perspective on the intersection of governance, technology, and control in North Korea. At the same time, it is firmly grounded in ethical research practices, ensuring that the narratives and experiences of North Korean defectors are treated with the dignity and care they deserve. This methodological approach not only enriches the article's contribution to the scholarly discourse on authoritarian regimes, but also highlights the importance of ethical engagement with vulnerable populations in politically sensitive research.

The Digitalization of North Korea's Mass Surveillance System

Since its inception, North Korea has been structurally and organizationally building out its mass surveillance system throughout the country. Government agencies, including the Ministry of State Security and the Ministry of Public Security, have very wide reach as part of maintaining the country's mass surveillance system. The Korean Workers' Party's hierarchical and thorough organizational structure ensures that there are party entities embedded in every administrative entity, all the way

down to the *inminban* level.[16] Organizational life is designed so that every citizen is accounted for, including mandatory associations that are responsible for political and ideological training.[17] Self-criticism sessions are critical to organizational life, where all citizens are required to publicly confess a political offense and then accuse a fellow citizen of a political offence he or she committed the previous week. People have long been incentivized to inform the authorities of a fellow citizen's political offenses, because withholding such information is also a criminal offense.

North Korean defectors I interviewed shared memories from the late 2000s of Bureau 109 officers shutting off the electricity in apartment complexes during hours when most residents would be home and watching media on their TVs.[18] With the electricity suddenly shut off, residents would not be able to press the "eject" button to expel any illegal DVDs they may have been watching on their TVs. Then the Bureau 109 officers would go door to door, checking the households' electronic devices and analyzing what content was on DVDs and CDs that were stuck in media players. To evade nosy neighbors or informants, some consumers of unauthorized media would close the curtains, turn the volume low on their TVs, NoteTels, or laptops, and secretly and quietly watch their illicit entertainment of choice (often South Korean dramas) in their homes.[19] As citizens adopted increasingly clever ways to outwit the authorities, the government quickly caught up with the population by no longer depending on such simple and brute-force tactics of control, turning instead to much more sophisticated technologies that have been enabling the government to reinforce its human-based surveillance networks with technology, and maximally expose all people to even more touch points with the state ideology.

Deterrents

Technology and Surveillance

In February 2023, the US charged a Russian national with supplying Russia and North Korea with US technologies for counterintelligence purposes. "As alleged, the defendant violated U.S. law by procuring, smuggling, and repairing counterintelligence operation devices for the benefit of Russia's secret police and the North Korean government," stated United States Attorney Breon Peace in a US Justice Department press release about this case.[20] This recent indictment reveals how wide North Korea's global reach is in procuring tools to further digitize its domestic surveillance capabilities.

16 The North Korean *inminban* (people's unit) is a neighborhood surveillance system composed of small, government-organized groups that monitor residents' daily activities to enforce loyalty, control information, and maintain social order.

17 Andrei Nikolaevich Lankov, In-ok Kwak, and Choong-Bin Cho, "The Organizational Life: Daily Surveillance and Daily Resistance in North Korea," *Journal of East Asian Studies* 12, no. 2 (May 2012): 193–214, https://doi.org/10.1017/S1598240800007839; Robert Collins, *North Korea's Organization and Guidance Department: The Control Tower of Human Rights Denial* (Washington, DC: Committee for Human Rights in North Korea, 2019), https://www.hrnk.org/documentations/north-koreas-organization-and-guidance-department-the-control-tower-of-human-rights-denial/.

18 Bureau 109, also known as Group 109 or Department 109, is a North Korean government task force responsible for monitoring and cracking down on illegal foreign media consumption, including unauthorized films, music, and literature, to enforce ideological control and prevent the spread of outside information.

19 NoteTel, a portmanteau of "notebook" and "television," is a popular Chinese multimedia player in North Korea. This device features multiple ports for various media types, including USB, CD-ROM, and sometimes radio, making it versatile and accessible.

20 US Attorney's Office, Eastern District of New York, "Russian National Charged with Supplying U.S. Technology to the Russian and North Korean Governments," US Justice Department, February 24, 2023, https://www.justice.gov/usao-edny/pr/russian-national-charged-supplying-us-technology-russian-and-north-korean-governments.

North Korea has a history of working with other countries and foreign companies to create restrictive domestic networks. The government's collaboration with Chinese technology companies KPTC and Orascom to create one of the most restrictive cellular environments in the world underscores this point.[21] In addition to importing technology from other countries, the North Korean government has been developing its own surveillance tools, such as spectrum analyzers to detect and track wireless signals.[22]

Since the outbreak of covid, North Korea has effectively sealed its border with China, and dramatically ceased most activities regarding trade, diplomacy, and any other arena that required cross-border person-to-person contact. North Korea continues to replace and upgrade its radio wave detectors along its borders to clamp down on international phone calls and foreign radio consumption, install more closed-circuit television systems (CCTVs) to deter or catch unauthorized human activity at the borders (mainly defections), and fortify its physical infrastructure with more fences and more guard posts. International calls made at the border using Chinese cellular network data will become increasingly more challenging, due to the government's investment in more and newer detection devices. The North Korean government has reinforced the Sino-North Korean border with its special elite Special Operations Forces (also referred to as Storm Corp) and additional fences, has installed more CCTVs at the border, and implemented new policies that expanded the border area exclusion zone, which North Koreans are prohibited from entering.[23] One point of reference is the number of guard posts at the border to prevent defections and other illicit cross-border activity, such as trade. According to Human Rights Watch's latest research report on this border, North Korea had 38 guard posts before the start of covid. Presently, Human Rights Watch has identified at least 6,056 guard posts along the border.[24] The covid-related border shutdown is presumed to be at least one of the reasons for why there has been a dramatic decrease in the number of defectors arriving in South Korea.[25]

21 Ellen Nakashima, Gerry Shih, and John Hudson, "Leaked Documents Reveal Huawei's Secret Operations to Build North Korea's Wireless Network," *Washington Post*, July 22, 2019.

22 Mun Dong Hui, "N. Korea's New 'Spectrum Analyzer' May Be a Surveillance Tool," Daily NK (news site), December 2, 2019, https://www.dailynk.com/english/north-korea-new-spectrum-analyzer-may-be-surveillance-tool/; Kim Chae Hwan, "North Korea Replaces Radio Wave Detectors on Border with the Latest Models," Daily NK (news site), November 3, 2022, https://www.dailynk.com/english/north-korea-replaces-radio-wave-detectors-border-latest-models/.

23 Kim Jeong Yoon, "Shedding Light on the Cruelty of North Korea's Border Protection Squad, the Storm Corps," Daily NK (news site), March 28, 2023, https://www.dailynk.com/english/shedding-light-cruelty-north-korea-border-protection-squad-storm-corps/; Lee Chae Un, "North Korea Announces Severe Punishments for International Callers in China-North Korea Border Region," Daily NK (news site), January 28, 2022, https://www.dailynk.com/english/north-korea-announces-severe-punishments-for-international-callers-in-china-north-korea-border-region/; Lee Chae Un, "N. Korea Forces Border Residents to Sign Oaths to 'Never Use Foreign-Made Cell Phones,' " Daily NK (news site), September 2, 2022, https://www.dailynk.com/english/n-korea-forces-border-residents-to-sign-oaths-to-never-use-foreign-made-cell-phones/.

24 Human Rights Watch, " 'A Sense of Terror Stronger than a Bullet': The Closing of North Korea, 2018–2023," Human Rights Watch, March 7, 2024, https://www.hrw.org/report/2024/03/07/a-sense-of-terror/stronger-than-a-bullet-the-closing-of-north-korea-2018%E2%80%932023.

25 Republic of Korea's Ministry of Unification, "Policy on North Korean Defectors" Ministry of Unification website, accessed July 27, 2021, https://www.unikorea.go.kr/eng_unikorea/relations/statistics/defectors/.

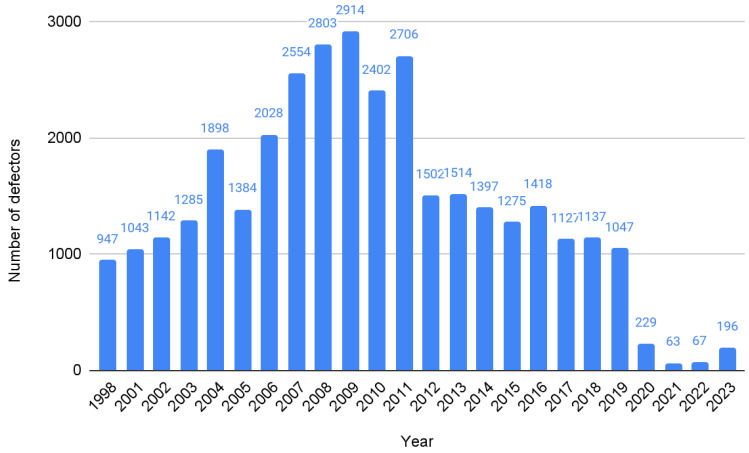

Figure 2. North Korean defectors arriving in the Republic of Korea by year. *Source:* Republic of Korea Ministry of Unification.

For decades, the North Korean government has developed communication networks designed for surveillance. For example, according to the Stimson Center's 38 North website, which obtained and analyzed meeting notes between the Egyptian company Orascom Telecom and the state-owned North Korea Post and Telecommunications Corporation (KPTC), "Eavesdropping and network security were the top concerns of the North Korean government in the months before Koryolink, the country's current mobile network service, was launched in December 2008."[26]

North Korea is only increasing its investment in surveillance devices, cameras, and other technologies to monitor people at the social, group, individual, and device level.[27] CCTVs have been dramatically on the rise in schools, offices, buildings, and on streets. The state has been importing more wiretapping software to crack down on international phone calls made at the border.[28] People have been required to update their devices with invasive software. Examples of items purchased include spectrum analyzers and signal analyzers from the German company Rohde & Schwarz, which

26 Martyn Williams, "North Korea's Koryolink: Built for Surveillance and Control," 38 North (blog), July 22, 2019, https://www.38north.org/2019/07/mwilliams072219/.

27 Chad O' Carroll, "Video Surveillance Equipment on Rise inside North Korea," NK News (news site), October 9, 2018, https://www.nknews.org/2018/10/video-surveillance-equipment-on-rise-inside-north-korea/. a recent trip by NK News journalists to Pyongyang and photos taken from around the country suggests. Closed-circuit television equipment was spotted installed in dozens of locations throughout Pyongyang, the September NK News visit showed, including factories, tourist attractions and hotel [...]","container-title":"NK News","language":"en-US","title":"Video surveillance equipment on rise inside North Korea","URL":"https://www.nknews.org/2018/10/video-surveillance-equipment-on-rise-inside-north-korea/","author":[{"family":"O' Carroll","given":"Chad"}],"accessed":{"date-parts":[["2023",5,5]]},"issued":{"date-parts":[["2018",10,9]]}},"label":"page"}],"schema":"https://github.com/citation-style-language/schema/raw/master/csl-citation.json"}

28 Seulkee Jang, "North Korea May Be Using 5G Mobile Communications Technology to Monitor Border," Daily NK (news site), July 13, 2021, https://www.dailynk.com/english/north-korea-may-using-5g-mobile-communications-technology-monitor-border/.

allow authorities to quickly identify live phone calls being made from their domestic cellular network.[29]

About 7 million North Korean citizens use North Korean smartphones, which are Android mobile phones with a touchscreen and an operating system capable of running downloaded applications.[30] But they do not have internet access, and most are not even connected to the country's intranet *Gwangmyeong*. These phones allow users to make domestic calls, send text messages, and use North Korean-produced applications that are generally not connected to the intranet. They have software that will neither open nor play foreign files that do not have the North Korean digital signature attached to the file names, and which sometimes will auto-delete such files. The Trace Viewer application can take screenshots of people's phones at any time and can turn on their mics without the user knowing, basically turning people's smartphones into personal surveillance devices.[31]

The Broader Cybersurveillance Industry

The quickly expanding cybersurveillance industry is as lucrative as it is unregulated.[32] In addition to the elite companies in commercial spyware like Israel's NSO Group, North Macedonia's Cytrox, Germany's Finfisher, and the Italian company Hacking Team, there "is a burgeoning secondary tier of suppliers composed of boutique spyware firms, hacker-by-night operations, exploit brokers, and similar groups."[33] North Korean defectors who worked in the IT sector told me that their teams that were dispatched abroad purchased cheap surveillance tools as well as developed their own software to monitor each other and the general population back home. According to Bill Marczak, a senior fellow at the Citizen Lab at the University of Toronto's Munk School of Global Affairs who has been tracking the spread of spyware around the globe, "There's no substantial regulation … Any government who wants spyware can buy it outright or hire someone to develop it for you. And when we see the poorest countries deploying spyware, it's clear [that] money is no longer a barrier."[34]

China's digital surveillance system industry, which was at first focused on its domestic market, now exports diverse surveillance technologies and AI surveillance products to a global customer base of at least 63 countries. "Increased collaboration between the party-state and private Chinese actors in the sale of surveillance products inspires trepidations about the proliferation of China's surveillance tools, ergo the

29 Williams, "North Korea's Koryolink." It is unclear how North Korea procured these devices, though it is unlikely that North Korea purchased them directly from the German company, as that would constitute a clear violation of UN sanctions.

30 Williams, "Smartphones of North Korea."

31 For more, see Martyn Williams and Niklaus Schiess, "Project REVEAL: New Research into North Korea's Digital Control System," Lumen (NGO website), accessed October 24, 2022, https://www.lumen.global/reveal-report; Nat Kretchun, Catherine Lee, and Seamus Tuohy, "Compromising Connectivity: Information Dynamics Between the State and Society in a Digitizing North Korea," US-Korea Institute at Johns Hopkins SAIS, accessed July 1, 2024, https://usakoreainstitute.org/wp-content/uploads/2017/03/Compromising-Connectivity-Final-Report.pdf; Martyn Williams, "Digital Trenches: North Korea's Information Counter-Offensive," Committee for Human Rights in North Korea, December 2019, https://www.hrnk.org/uploads/pdfs/Williams_Digital_Trenches_Web_FINAL.pdf.

32 Steven Feldstein, "The Global Expansion of AI Surveillance," Carnegie Endowment for International Peace, May 5, 2023, https://carnegieendowment.org/2019/09/17/global-expansion-of-ai-surveillance-pub-79847.

33 Steven Feldstein "Why Does the Global Spyware Industry Continue to Thrive? Trends, Explanations, and Responses," Carnegie Endowment for International Peace, March 13, 2023, https://carnegieendowment.org/research/2023/03/why-does-the-global-spyware-industry-continue-to-thrive-trends-explanations-and-responses?lang=en

34 Nicole Perlroth, "Governments Turn to Commercial Spyware to Intimidate Dissidents," *New York Times*, May 29, 2016.

rise of unwarranted surveillance."[35] There is a growing and lucrative ecosystem of Chinese startups that are used by security services globally to conduct defensive and offensive cyber operations.[36] Over half of the world's 1 billion CCTVs are in China (approximately 540 million as of 2021), which gives Chinese companies massive data sets to test, iterate, and refine their digital surveillance products for export.[37]

While China may choose to selectively enforce UN sanctions again, as it did in 2017, consequently straining Sino-North Korean relations, it is in China's clear interest for North Korea to remain stable. In July 2021, the two countries commemorated the 60th anniversary of the DPRK-China Treaty of Friendship, Cooperation, and Mutual Assistance, and renewed this treaty for another 20 years. This is the only formal defense treaty that either country has with any other country. Given China's treaty-based relationship with North Korea, the former's strict view of cyber sovereignty, and its longstanding views on non-intervention policies toward states, China will most likely continue countering any efforts to destabilize the North Korean regime by permitting its companies to sell surveillance technology to North Korea for the latter's domestic surveillance.

Given the low costs of second-tier cybersurveillance tools that could be easily purchased or developed by its own IT workers, paired with their high returns on investment, North Korea will most likely continue to develop its own surveillance technologies as well import them from state and nonstate actors.

Laws, Regulations, and Decrees

For decades, North Korea has had a variety of laws and criminal codes that prohibit citizens from consuming foreign content, but the enforcement of such laws varied in severity under Kim Il-Sung and Kim Jong-Il's reigns. Months after Kim Jong-Un came to power, there began a steady increase in efforts to "purify" the ideological environment of North Korea by stamping out unauthorized content and foreign influence that the government did not approve of.[38]

Passing new laws or legal amendments has been one major mechanism through which the North Korean government has been demonstrating to the population its seriousness in terms of eliminating the consumption of unauthorized information. Changes in legislation in North Korea are important to follow because they publicly signal what Kim and the Korean Workers' Party are prioritizing.

In late 2019, North Korean authorities escalated their efforts to suppress foreign information by introducing the Reactionary Ideology and Culture Rejection Law. This legislative initiative was further reinforced in 2022 when the Presidium of the Supreme People's Assembly amended the Reactionary Ideology and Culture Rejection

35 Bulelani Jili, "China's Surveillance Ecosystem and the Global Spread of Its Tools," Atlantic Council, October 17, 2022, https://www.atlanticcouncil.org/in-depth-research-reports/issue-brief/chinese-surveillance-ecosystem-and-the-global-spread-of-its-tools/.

36 Muyi Xiao, Paul Mozur, Isabelle Qian, and Alexander Cardia, "China's Surveillance State Is Growing: These Documents Reveal How," *New York Times*, June 21, 2022.

37 Jili, "China's Surveillance Ecosystem and the Global Spread of Its Tools."

38 Martyn Williams, "Digital Surveillance in North Korea: Moving Toward a Digital Panopticon State," 38 North (blog), October 18, 2024, 13–15, https://www.38north.org/reports/2024/04/digital-surveillance-in-north-korea-moving-toward-a-digital-panopticon-state/.

Act of the Democratic People's Republic of Korea.[39] In January 2023, the regime passed an additional measure, the Pyongyang Cultural Language Protection Act.[40] Both laws meticulously delineate the types of content and speech deemed illegal, as well as the range of punishments for those found in violation. These legislative frameworks not only broaden the categories of prohibited behavior, but also increase the range of penalties for engaging in what is considered "deviant" activity. The laws explicitly forbid the consumption, distribution, or possession of unauthorized content, and extend to any actions that could facilitate such consumption, including the manipulation of phones, radios, televisions, and other media devices. The specificity of these regulations indicates that the state had observed a widespread occurrence of such behaviors, prompting a categorical prohibition nationwide. While media consumption has long been tightly controlled, these laws formalize and codify the increasingly stringent measures that Kim Jong-Un and the Korean Workers' Party have implemented since 2011.

These laws are being rigorously enforced. It remains unclear whether the increase in convictions is due to a rise in the consumption of illegal content, or to more effective detection and enforcement following the implementation of the new legal frameworks. Nonetheless, the significant number of individuals being prosecuted and penalized underscores the regime's heightened commitment to curbing unauthorized media consumption. This suggests a systematic effort by the government to address what it perceives as a serious threat to its ideological control.

In addition to these two laws, both Kim Jong-Un and his younger sister Kim Yo-Jong have delivered numerous speeches condemning individuals who are influenced by information or media that has not been sanctioned by the state.[41] Kim Jong-Un has repeatedly called the war on foreign culture an "invisible war" and "silent battle," which demonstrates the extent to which he views foreign influence as a danger to his political legitimacy.

Offensive Measures

Since Kim Jong-Un assumed power, the regime has implemented multifaceted enhancements to its ideological programming aimed at countering foreign cultural influences. In addition to deterrent measures, the government has adopted an offensive strategy to intensify ideological indoctrination and resist foreign information, culture, and influence. One key approach has been to expand the scope and intensity of the ideological training imposed on citizens. In March 2023, as reported by Radio Free Asia, the state mandated that citizens read 10,000 pages of propaganda throughout the year to foster loyalty and suppress the influence of "reactionary" South Korean popular culture.[42]

39 For the Korean text of this law, see Seulkee Jang, "Daily North Korea Acquires Full Text of the Anti-Reactionary Thought Law" Daily NK (news site), March 21, 2023, https://www.dailynk.com/english/daily-nk-acquires-full-text-of-the-anti-reactionary-thought-law/.

40 Mun Dong Hui, "Daily NK Obtains the Full Text of the Pyongyang Cultural Language Protection Act," Daily NK (news site), March 23, 2023, https://www.dailynk.com/english/daily-nk-obtains-full-text-pyongyang-cultural-language-protection-act/.

41 Sang-Hun Choe, "Kim Jong-Un Calls K-Pop a 'Vicious Cancer,'" *New York Times*, June 11, 2021; Mun Dong Hui, "New N. Korean Video Harshly Condemns People Caught Enjoying Foreign Content," Daily NK (news site), December 30, 2022, https://www.dailynk.com/english/new-north-korean-video-harshly-condemns-people-caught-enjoying-foreign-content/; Martyn Williams, "North Korea Intensifies War against Foreign Influence," 38 North (blog), Stimson Center, November 10, 2021, https://www.38north.org/2021/11/north-korea-intensifies-war-against-foreign-influence/.

42 "North Korea Orders Citizens to Read 10,000 Pages of Propaganda This Year," Radio Free Asia, May 4, 2023, https://www.rfa.org/english/news/korea/10000_pages-04282023093517.html.

Kim Jong-Un and the Korean Workers' Party have clearly prioritized this offensive strategy by extending the duration of ideological training, producing increasingly ideologically rigorous content and, crucially, granting access to state-approved foreign media and entertainment. These efforts are intended to shape and control the preferences of the populace, ensuring alignment with state-sanctioned narratives.

In addition to intensifying political education, the government has broadcast documentaries that publicly condemn individuals for exhibiting behaviors influenced by foreign culture. These broadcasts feature still images of the offenders, accompanied by their names, *inminban* numbers, and the specific infractions committed—such as wearing jeans, sporting unapproved hairstyles, or engaging in public displays of affection. This tactic of personalized naming and shaming is reinforced by social role modeling, whereby citizens who conform to state-sanctioned dress, speech, and behavior are publicly praised. For instance, in one documentary, images of women deemed counterrevolutionary for their appearance are shown alongside their personal details, including their hometown, neighborhood, *inminban* unit, and full name. The primary aim of these broadcasts is to publicly humiliate individuals as a form of ideological enforcement, reinforcing socialist narratives.

Provision of State-Approved Alternative Media and Entertainment

LCD and smart televisions continue to play North Korean channels: five in Pyongyang, and one in areas outside of Pyongyang.[43] In 2016, the government released a North Korean IP streaming TV service called Manbang that non-Pyongyang citizens could purchase to watch the additional channels that they did not have access to as non-Pyongyang residents.[44] Through the IPTV streaming service, the state propaganda could theoretically reach all homes in a much more updated, frequent, and diverse manner.

Based on dozens of interviews I conducted with defectors who had been overseas workers before defecting, I learned that foreign workers are sent abroad with the North Korean setup boxes to stream North Korean content so that they can watch Pyongyang content even while abroad.

Beyond the IPTV streaming services for non-Pyongyang residents, the North Korean government has been allowing vendors to sell approved foreign movies to citizens. Such state-approved foreign films and programming like international soccer matches are shown on television or sold on DVDs or USBs. Interviews I have conducted with defectors over the years reveal that state-approved foreign films and documentaries are very old ones with ideologically aligned or neutral content from Vietnam, China, India, or Soviet-era Russian productions. Citizens today have more options to purchase mobile applications, mobile games, and films from state-approved storefronts to keep them entertained.[45]

43 Jeong Tae Joo, "Liquid Crystal TVs Appear in Markets in Pyongyang, Kaesong and Kangwon Province," Daily NK (news site), February 10, 2023, https://www.dailynk.com/english/liquid-crystal-tvs-appear-markets-pyongyang-kaesong-kangwon-province/.

44 Martyn Williams, "Manbang IPTV Service in Depth," 38 North (blog), Stimson Center, February 22, 2019, https://www.38north.org/2019/02/mwilliams022219/.

45 Mun Dong Hui, "New North Korean Report Cites around 400 Cybercrime-Related Incidents inside the Country," Daily NK (news site), April 6, 2023, https://www.dailynk.com/english/new-north-korean-report-cites-around-400-cybercrime-cases-inside-country/; Mun Dong Hui, "North Korean Research Paper Calls for New Law to Combat Cybercrime," Daily NK (news site), January 9, 2023, https://www.dailynk.com/english/north-korean-research-paper-calls-new-law-combat-cybercrime/; Mun Dong Hui, "Think North Koreans Don't Fall Victim to Cybercrime? Think Again," Daily NK (news site), October 11, 2022, https://www.dailynk.com/english/think-north-koreans-fall-victim-cybercrime-think-again/.

Subtle Acts of Defiance in a Digitally-Controlled Society

The North Korean regime's extensive deterrent and offensive measures aimed at curbing foreign influence have led to significant, observable shifts in the behavior of its citizens with respect to the procurement and consumption of unauthorized information. Through the imposition of new technologies and stricter legal frameworks, the state has systematically constrained access to uncensored content, compelling the general population to align its behavior and attitudes more closely with government-imposed expectations. Insights from interviews conducted between 2023 and 2024 reveal a growing reluctance among North Koreans to engage in risky behavior for the sake of accessing foreign media. As one interviewee noted, "If I can watch a less interesting but nonetheless foreign film, such as a Chinese or Indian film that the North Korean government has approved of, why would I go out and risk my life and the safety and security of my household to watch a foreign film that may be more interesting, but is highly illegal?"[46]

The interviews suggest that individuals' risk calculations are becoming increasingly conservative. Rather than purchasing illicit content as was common a decade ago, many now prefer to share and circulate materials quietly among trusted acquaintances. Despite the tightening grip of state control, there remain segments of the population—particularly those with access to knowledge or power—who continue to engage in more dangerous behaviors, leveraging their technical skills to access prohibited content. These individuals have found ways to bypass state restrictions by jailbreaking phones, manipulating devices to view foreign media, and even hacking fellow citizens. These actions highlight the persistence of subtle acts of resistance, even in a highly surveilled society.

Moreover, the longstanding practice of bribing local authorities when caught with foreign media is becoming less viable, as the regime has implemented a robust array of legal, social, and technological measures aimed at preventing such behaviors. The Kim Jong-Un regime has intensified the consequences for consuming unauthorized material, thus discouraging traditional methods of circumventing state control. This shift has led to a notable reduction in the number of actors involved in smuggling information into the country. Although civil society organizations continue to send information via leaflets or USBs across the DMZ, these methods are increasingly rare and less effective.

However, despite the regime's efforts to create a self-regulating and self-censoring populace, new forms of resistance are emerging, particularly among technically-skilled individuals, such as high school and university students. These individuals have demonstrated the ability to exploit technology to access the global internet without state permission, manipulate devices to access foreign content, and even engage in unauthorized hacking activities.[47] The use of specific software programs designed to circumvent state surveillance further exemplifies the resourcefulness of this group in navigating the constraints imposed by the regime.[48]

46 Interviewee #1, interview conducted in Seoul on March 13, 2023.

47 Jeong Tae Joo, "Several State Security Agency Agents Busted for Accessing Internet without Permission," Daily NK (news site), March 10, 2023, https://www.dailynk.com/english/several-state-security-agency-agents-busted-for-accessing-internet-without-permission/.

48 Mun Dong Hui, "North Koreans Are Using around 10 Programs to Circumvent Big Brother's Watchful Eye," Daily NK (news site), July 29, 2022, https://www.dailynk.com/english/north-koreans-use-around-10-programs-circumvent-big-brother-watchful-eye/.

Notably, there has been a marked increase in domestic cybercrime within North Korea. Recent reports have documented over 400 cases of cyber-related offenses, including instances in which North Korean hackers infiltrated the personal accounts of government officials. In late 2021, for example, a second-year student at the Pyongyang University of Science and Technology was arrested for hacking into individual accounts within the country. The growing prevalence of such activities has prompted calls for new legislative measures to combat cybercrime, as reflected in an article published by the *Journal of Kim Il Sung University* in early 2023.[49] This rising trend underscores the complexities of managing technological advancement within an authoritarian state that seeks to maintain strict control over both information and individual behavior.

North Korea in 2024–2030: Predictions and Prescriptions

Assessments

North Korea possesses several key elements that contribute to its continued stability in the foreseeable future: (1) The regime benefits from a highly stable domestic political system, underpinned by an effective totalitarian state structure and the necessary infrastructure to reinforce and maintain control; (2) the country is largely insulated from the threat of foreign military intervention due to its nuclear deterrent capabilities; (3) North Korea enjoys a degree of an economic safety net, bolstered by its strategic alliance with China, which is likely to prevent any potential collapse arising from economic or political challenges; and (4) the regime's expansion of illicit revenue generation methods further strengthens its domestic political and economic stability. These factors are significantly reinforced by the state's ongoing research, investment, and development in both civilian and military technologies.

Predictions

As the regime continues to invest in surveillance technologies and the broader digitization of various aspects of society, it is reasonable to predict that certain segments of the population will develop more sophisticated means of accessing unauthorized information. A small group of North Korea's elite hackers and IT specialists will likely continue to exploit their skills for self-serving purposes, such as engaging in unofficial activities, including wiping government employees' devices for a fee or assisting others in circumventing state surveillance mechanisms.

As previously noted, many traditional actors involved in disseminating information into North Korea have withdrawn from these activities as a result of significant suppression from the North Korean regime, leading to a significant decline in both the frequency and efficacy of land-based information distribution. However, this reduction in conventional information campaigns also presents new avenues for academic inquiry and policy development, as well as opportunities for the creation of innovative policies and technologies better suited to addressing North Korea's increasingly stringent information environment.

Prescriptions

Kim Jong-Un refers to his citizens' consumption of unauthorized content as the "invisible battle, a silent war" and has been investing significant resources to prevent

49 Hui, "North Korean Research Paper Calls for New Law to Combat Cybercrime."

North Koreans from accessing foreign information.[50] Codification of increasingly severe punishments for consuming foreign information, investments in monitoring and censorship software for individual devices, and maintaining powerful jamming systems to block unauthorized radio signals are just a few of the many ways in which the regime actively fights information from the outside world. Efforts to provide North Koreans access to information in a safe and secure way could certainly benefit from today's technologies to help citizens circumvent their government's censorship and monitoring methods.

What strategies can the global community employ to counter North Korea's digital totalitarianism? There are significant opportunities for various international actors to collaborate in providing access to information and media for North Korean citizens. The United States government has been actively engaged in efforts to transmit radio broadcast programs, such as Voice of America and Radio Free Asia, into North Korea. In addition, it has supported civil society organizations (CSOs) in their creative initiatives to disseminate information within the country. With increased resources, these CSOs could further expose the gap between North Korean state propaganda and real living standards in the country. Moreover, the United States, along with its allies and other interested governments, could enhance public diplomacy efforts aimed at better understanding, informing, and influencing the North Korean population through innovative, targeted information campaigns. Additionally, the US government could streamline the process for technology companies seeking Office of Foreign Assets Control (OFAC) waivers, enabling them to provide North Korean citizens with access to information, the internet, and communications technologies.

Scholars can leverage historical precedents to extract lessons from contexts where information campaigns have successfully breached information blockades. Information warfare has persisted for centuries, and the lessons from these historical experiences can and should be adapted to the North Korean context. Furthermore, principles from psychology and behavioral science offer critical insights into how to effectively communicate with audiences that are both curious and potentially resistant to external information. Examples include researching cult deprogramming, how minds change, and unintended psychological backfire effects when an individual is confronted with new information that challenges their core beliefs.[51] Understanding how cognitive shifts occur—especially in individuals deeply embedded in a closed ideological system—is essential to designing successful information dissemination strategies. Researching how North Korean citizens' minds are shaped and changed by information campaigns is fundamental to any effort aimed at penetrating the state's hermetic information environment. Additionally, academics should explore how exposure to external information may influence preference falsification,[52] foster horizontal linkages within an atomized society, or creates the potential building blocks for collective action.

50 The original source comes from North Korea's official news source: Korean Central News Agency, "Boiji anhneun daegyeol, sorieopsneun jeonjaeng," KCNA, October 19, 2019, https://rodong.rep.kp/ko/index.php?strPageID=SF01_02_01&newsID=2019-10-19-0038. For a more secure version of this source, see the Seoul-based NK News organization's KCNA Watch (news site), October 19, 2019, https://kcnawatch.org/newstream/1572205449-137058496/보이지-않는-대결-소리없는-전쟁/?t=1588256865519.

51 Author? "Boiji anhneun daegyeol, sorieopsneun jeonjaeng (Invisible Conflict, Silent War)." [As above, whichever rule applies here]

52 Preference falsification is the act of misrepresenting one's true preferences due to perceived public pressures or sanctions, involving the expression of a public preference that contradicts one's privately held views. For more, see Timur Kuran, Private Truths, Public Lies: The Social Consequences of Preference Falsification (Cambridge, Mass.: Harvard University Press, 2022), https://www.hup.harvard.edu/catalog.php?isbn=9780674707580.

The entertainment, marketing, and advertising industries are valuable sources for understanding how to tailor content for specific audiences and sustain their engagement. Their best practices—such as professional audience testing, incorporating feedback from proxy groups (with defectors serving as the closest proxies for North Korean citizens), and involving members of these proxy groups in the actual content creation process—can be highly instructive. These industries can also provide guidance to governments and CSOs on influencing attitudes, shifting behavior, and inspiring individuals to learn about historical figures who have driven transformative change.

The technology sector is also uniquely positioned to contribute to information dissemination efforts, offering tools, expertise, and resources that can significantly enhance these operations. Satellite-enabled technologies, including communication networks, television, and the internet, can be adapted to the North Korean context, allowing citizens to safely access unauthorized content and communicate both domestically and externally. Crucially, these tech companies should collaborate closely with defectors to maintain an up-to-date understanding of North Korea's ICT landscape, ensuring that well-meaning efforts do not inadvertently cause harm by overlooking critical security considerations in the country.

It is important to recognize that not all information efforts targeting North Korea are helpful. Well-intentioned but poorly informed initiatives can backfire, reinforcing the regime's propaganda narrative and entrenching existing beliefs. Worse still, such efforts may expose North Korean information consumers to danger. The moral hazard is significant: the risk falls entirely on North Koreans themselves rather than the external information distributors.

Any efforts to weaken Kim Jong-Un's totalitarian system of governance must not underestimate the state's capacity for repression. The Kim family's hereditary totalitarian system has survived for three generations, largely due to its ability to adapt and maintain control through various forms of surveillance and coercion. Kim Jong-Un is now integrating new technologies to further consolidate his power and ensure that the Korean Workers' Party remains stable, making external interventions particularly fraught. Thus, those seeking to provide information to North Koreans must stay abreast of the country's ICT landscape and approach any such efforts with extreme caution.

A central best practice for any effort aimed at expanding information access in North Korea is to engage consistently with defectors, whose lived experiences provide invaluable insights into the intricacies of a system that outsiders can never fully comprehend. However, North Korea's highly stratified and atomized society ensures that each defector's narrative captures only a fragment of the broader reality. Thus, a comprehensive understanding of North Korean society necessitates the inclusion of diverse perspectives from those who have lived under the regime's authoritarian control. To contribute meaningfully to the future of North Korea, it is essential to approach these efforts with humility and a steadfast commitment to understanding the experiences of individuals who have endured profound repression yet continue to aspire to meaningful change.