North Korea's Strategic Situational Awareness Capabilities

A Country Primer

BY JASON ARTERBURN

Executive Summary

North Korea's developing strategic situational awareness (SA) capabilities incorporate technologies that could introduce new risks in a conflict or crisis on the Korean Peninsula. North Korea possesses multifaceted command, control, communications, computers, intelligence, surveillance, and reconnaissance (C4ISR) systems that support a range of provocative asymmetric operations, including but not limited to GPS jamming, communications spoofing, cyberespionage, and cyberattacks.[1] While North Korea has rapidly developed its domestic telecommunications infrastructure and advanced computing capability in recent years, its systems continue to face technical and operational limitations that may constrain North Korea's SA in engagements across the spectrum of conflict.

This report synthesizes publicly available information on North Korea's C4ISR systems and capabilities in order to consider how technology could affect escalatory dynamics or crisis stability during conflict in East Asia. The author prioritized primary sources from North Korean institutions or companies, official reports from governments, technical reports from specialist research firms, and articles from English-, Korean-, and Chinese-language media.[2] Wherever possible, the author also attempted to corroborate information across multiple sources in different languages. Because the public domain contains little information on North Korea's C4ISR equipment, readers are advised that the findings in this report likely provide an incomplete view of North Korea's strategic SA capabilities, which therefore limits the scope of conclusions that readers should draw about the effect that these technologies may have in conflict.[3] Nonetheless, this report represents a broad review of literature on North Korea's approach to emerging technologies and should be of interest to policymakers and informed observers who wish to consider the relationship between technology and strategic stability on the Korean Peninsula.

[1] CSIS Project on Nuclear Issues defines "strategic situational awareness" as "the ability to observe the operating environment, detect attacks, and discern actual attacks from false alarms across the spectrum of conflict."

[2] The author would like to thank Jennifer Jun, Lauren Sung, and Jason Bartlett for their invaluable Korean-language research support.

[3] In their report "North Korea's Cyber Operations: Strategy and Responses" (2015), the authors Jenny Jun, Scott LaFoy, and Ethan Sohn detailed four key challenges in researching North Korea's capabilities from sparse materials in the open source: the prevalence of disinformation, an echo chamber of unverified statements cited repeatedly across sources, incentives for different stakeholders to either overestimate and underestimate North Korean capabilities, and limited synthesis of information on this subject across technical disciplines and languages. See Jenny Jun, Scott LaFoy and Ethan Sohn, *North Korea's Cyber Operations: Strategy and Responses.* (Lanham: Rowman & Littlefield, 2015), https://csis-prod.s3.amazonaws.com/s3fs-public/legacy_files/files/publication/151216_Cha_NorthKoreasCyberOperations_Web.pdf.

Intelligence & Operations

Since the Korean War, North Korea has developed a warfighting strategy that emphasizes asymmetric engagement through hybrid use of conventional and unconventional forces either to deter aggression or, if having failed to do so, to defeat adversaries quickly after an attack.[4] This section describes the organizations that produce intelligence in North Korea, situates them within North Korea's command and control architecture, and examines their operational approaches to asymmetric engagements across the spectrum of conflict.

Intelligence Apparatus

The Reconnaissance General Bureau (RGB; 정찰총국) is North Korea's primary service for foreign intelligence, clandestine operations, and asymmetric operations.[5] The RGB formed in May 2009 when two separate intelligence bureaus in the Korean Workers' Party (KWP; 조선로동당) and the Ministry of People's Armed Forces (MPAF; 인민무력부) merged during a broader reorganization of North Korea's intelligence apparatus.[6] The RGB is believed to report directly to the State Affairs Commission, North Korea's highest state military organ that is chaired by Kim Jong Un.[7] [8]

English- and Korean-language reports often contain conflicting information about the RGB's precise structure and the specific mandates of its subordinate bureaus. Generally, however, the RGB is believed to consist of at least six bureaus, several of which engage in intelligence collection, information warfare, and cyber operations.[9] In particular, the Sixth Bureau (제 6 국) is believed to work with the Electronic Warfare Division of the General Staff Department (GSD; 총참모부) to develop and conduct signals intelligence (SIGINT), electronic warfare (EW), and information warfare operations.[10] The Sixth Bureau also allegedly contains Lab 110 (110 연구소), a cyber unit believed to collect foreign intelligence and generate foreign currency through malicious cyber activity conducted

---

[4] For work describing North Korea's operational and strategic thinking, see James M. Minnich, North Korean Tactics. (2011), http://www.faoa.org/resources/Documents/NorthKoreanMilitaryTactics.pdf; Joseph S. Bermudez, Shield of the Great Leader: The Armed Forces of North Korea. (Sydney: Allen & Unwin, 2001 and London: I.B. Taurus, 2001); and Joseph S. Bermudez, Jr, North Korea's Strategic Culture. (Defense Threat Reduction Agency Advanced Systems and Concepts Office, 2006), https://fas.org/irp/agency/dod/dtra/dprk.pdf.

[5] Jenny Jun, Scott LaFoy and Ethan Sohn, *North Korea's Cyber Operations: Strategy and Responses.* (Lanham: Rowman & Littlefield, 2015), https://csis-prod.s3.amazonaws.com/s3fs-public/legacy_files/files/publication/151216_Cha_NorthKoreasCyberOperations_Web.pdf.

[6] Joseph S. Bermudez Jr., "A New Emphasis on Operations Against South Korea?," 38 North, U.S. – Korea Institute at SAIS at Johns Hopkins University, June 11, 2010, www.38north.org/?p=920.

[7] Public reporting contains some discrepancies on whether the RGB reports directly to the SAC. For example, in its March 2020 report, the UN Panel of Experts established pursuant resolution 1874, which is responsible for monitoring sanctions compliance on North Korea, cited a Member State to state that "the RGB is organized under the General Staff Department, which exercises operational command and control over the Korea People's Army" and is "directly subordinate to the State Affairs Commission," thereby illustrating "not only its high degree of strategic importance but also … close bureaucratic oversight by the highest levels of leadership." See page 155 of United Nations, Security Council, *Report of the Panel of Experts established pursuant to resolution 1874 (2009),* S/2020/151, March 2, 2020, accessed Spring 2020. https://undocs.org/S/2020/151.

[8] *The conventional military balance on the Korean Peninsula*, The International Institute for Strategic Studies. (2018). https://www.iiss.org/-/media/images/comment/military-balance-blog/2018/june/the-conventional-military-balance-on-the-korean-peninsula.ashx?la=en&hash=C51D23B426579E41B43CF30A0D8969328FE57803. See also 유동열 [Yoo Dong Yeol], "북한 정보기구의 변천과 현황 [Changes to and status of North Korea's Intelligence Organizations]," 국가정보연구 [Journal of National Intelligence Studies] 11-1 (2018), http://www.kanis.or.kr/sample/down.php?bbs_id=magazine_search&kbbs_doc_num=123&file=1.

[9] Joseph S. Bermudez Jr., "A New Emphasis on Operations Against South Korea?," 38 North, U.S. – Korea Institute at SAIS at Johns Hopkins University, June 11, 2010, www.38north.org/?p=920.

[10] The General Staff Department reports directly to the State Affairs Commission. See ibid.

from both North Korea and overseas.[11] Some researchers also speculate that the Sixth Bureau may combine offensive cyber operations with other foreign intelligence collection methods like HUMINT, which are formally the mandates of other RGB Bureaus.[12]

In addition to the RGB, the Korean People's Army (KPA; 조선인민군) also has an intelligence mandate. The KPA General Staff Classified Information Department[13] (총참정보부) reportedly produces, disseminates, stores, and maintains hardware and software related to intelligence products and works jointly with the Communications Bureau (통신국) and other departments of the Military Security Command (보위사령부).[14] Some experts have indicated that the KPA and RGB may coordinate in several military and intelligence functions. For example, reports from 2010 based on expert interviews state that the KPA General Staff Communications Bureau maintains the military's telecommunications and signals infrastructure for both foreign and domestic SIGINT collection, and that the General Staff Department's Electronic Warfare Bureau coordinates between the Communications Bureau and the Reconnaissance General Bureau to manage EW and "electronic intelligence warfare" (EIW; 전자정보전) operations.[15] Coordination between North Korea's military and intelligence apparatus for SIGINT, EW, and EIW operations would suggest that, as other researchers have also speculated, the RGB also coordinates with the KPA's General Staff for broader operational planning, through which its cyber units could support military engagement.[16] Because the RGB also reportedly manages a small number of ships and submarines, it may also coordinate with the Korean People's Navy (KPN; 조선인민군 해군), but the public domain contains little information on the subject.[17]

Technical & Operational Approaches

North Korean leadership has expressed interest in SIGINT, EW, and EIW operations since at least the armistice of the Korean War, in which Kim Il Sung constituted SIGINT and communications intelligence (COMINT) abilities

---

[11] For example, in a criminal complaint against North Korean hacker Park Jin Hyok, the U.S. Department of Justice alleged that Park Jin Hyok was involved in "a conspiracy to conduct multiple destructive cyberattacks around the world resulting in damage to massive amounts of computer hardware, and the extensive loss of data, money, and other resources" while working for a North Korean front company in China affiliated with Lab 110. See Office of Public Affairs, "North Korean Regime-Backed Programmer Charged With Conspiracy to Conduct Multiple Cyber Attacks and Intrusions," Department of Justice, September 6, 2018, https://www.justice.gov/opa/pr/north-korean-regime-backed-programmer-charged-conspiracy-conduct-multiple-cyber-attacks-and.

[12] Researchers at CSIS specifically suggested that the hacking operations could be incorporated with HUMINT operations of the First and Second Bureaus. For more information, see Jenny Jun, Scott LaFoy and Ethan Sohn, North Korea's Cyber Operations: Strategy and Responses. (Lanham: Rowman & Littlefield, 2015), https://csis-prod.s3.amazonaws.com/s3fs-public/legacy_files/files/publication/151216_Cha_NorthKoreasCyberOperations_Web.pdf.

[13] English and Korean sources contain variance in use of the name "bureau" and "division." For an example of Korean-language sources using the word "division," see 정태주 [Jung Tae Joo], "北 총참모부, 한미공중연합훈련에 GPS 교란공격 준비 지시 [North Korean Chieg of the General Staff of the KPA order preparations for GPS attacks on South Korea - U.S. joint air exercise]," Daily NK, November 13, 2019, https://www.dailynk.com/%E5%8C%97-%EC%B4%9D%EC%B0%B8%EB%AA%A8%EB%B6%80-%ED%95%9C%EB%AF%B8%EA%B3%B5%EC%A4%91%EC%97%B0%ED%95%A9%ED%9B%88%EB%A0%A8%EC%97%90-gps-%EA%B5%90%EB%9E%80%EA%B3%B5%EA%B2%A9-%EC%A4%80%EB%B9%84/.

[14] "KPA General Staff." North Korea Leadership Watch. Accessed Fall 2019. http://www.nkleadershipwatch.org/dprk-security-apparatus/general-staff-department/.

[15] "KPA General Staff." North Korea Leadership Watch. Accessed Fall 2019. http://www.nkleadershipwatch.org/dprk-security-apparatus/general-staff-department/.

[16] For example, see Emma Chanlett-Avery et al. "North Korean Cyber Capabilities," *Congressional Research Service,* August 3, 2017, https://fas.org/sgp/crs/row/R44912.pdf.

[17] *The conventional military balance on the Korean Peninsula*, The International Institute for Strategic Studies. (2018). https://www.iiss.org/-/media/images/comment/military-balance-blog/2018/june/the-conventional-military-balance-on-the-korean-peninsula.ashx?la=en&hash=C51D23B426579E41B43CF30A0D8969328FE57803

within the Ministry of Internal Affairs and the Reconnaissance Bureau (정찰국).[18] When Kim Il Sung began to emphasize the development of North Korea's defense industry, the government established related curricula at both civilian and military educational institutions.[19] Both the Reconnaissance Bureau and the Korean People's Army (KPA) dispatched personnel to the Soviet Union and the People's Republic of China for training in computer science, EW, and SIGINT.[20] Around the same time, North Korea's Ministry of Public Security (인민보안성) and Academy of Defense Sciences (국방과학원) acquired first-generation computers from the Soviet Union, which provided a key technical capability that would serve as the basis for subsequent developments in SIGINT and EW capabilities.[21]

In the decades that followed, both the KPA and the Ministry of People's Armed Forces (MPAF) studied the use of SIGINT and EW in conflicts around the world. In the mid-1980s, the North Korean government made a broad attempt to again accelerate the development of SIGINT and EW capabilities.[22] In 1984, the government established the Mirim Academy in Pyongyang, which hired professors from the Soviet Union's Frunze Military Academy and educated physics, automation, and mathematics postgraduates from elite North Korean universities on jamming, radar detection, missile control and guidance, computers, and infrared detection and tracking.[23] At the same time, the government created a computer science department at Kim Il Sung University; related research institutes at Kim Chaek University of Technology and the Academy of Sciences; and a number of other computer colleges around Pyongyang and Hamhung.[24] By the 1990s, the Korean People's Army had established an Electronic Warfare Division (전자전구분대), and the North Korean government continued to open additional computer institutes and research and development facilities like the Integrated Circuit Test Facility (평양집적회로시험공장) and the Korea Computing Center (조선콤퓨터쎈터), among others.[25]

Following U.S. Operation Desert Storm, which the MPAF is reported to have studied extensively, Kim Jong Il directed all branches of the KPA to research EW and ordered expansions by organizations operating in the computer industry, including computer science departments at universities.[26] [27] The government established more research institutes for software development that focused on technical cooperation with Third World countries and

---

[18] Joseph S. Bermudez Jr., "SIGINT, EW and EIW in the Korean People's Army: An Overview of Development and Organization," *Bytes and Bullets in Korea,* ed. Alexandre Y. Mansourov (Honolulu: Asia-Pacific Center for Security Studies, 2005), http://www.apcss.org/Publications/Edited%20Volumes/BytesAndBullets/TOC.pdf.

[19] Ibid page 237-8.

[20] Ibid page 237-8.

[21] Ibid page 238.

[22] Ibid page 239.

[23] Ibid page 239.

[24] Ibid page 239-40.

[25] Ibid page 241-2, which uses the name "Electronic Warfare Bureau" rather than "Electronic Warfare Division." English and Korean reporting use different names for the department. For an example of a Korean source that use "Electronic Warfare Division," see 정태주 [Jung Tae Joo], "北, 대남 GPS 공격 강행?… 다음주부터 新 무기 배치 시작" [North Korea undertaking GPS attacks against South Korea?… Starting deployment of new weapons next week]," Daily NK, April 23, 2020, https://www.dailynk.com/%E5%8C%97-%EB%8C%80%EB%82%A8-gps-%EA%B3%B5%EA%B2%A9-%EA%B0%95%ED%96%89-%EB%8B%A4%EC%9D%8C%EC%A3%BC%EB%B6%80%ED%84%B0-%E6%96%B0-%EB%AC%B4%EA%B8%B0-%EB%B0%B0%EC%B9%98-%EC%8B%9C%EC%9E%91/.

[26] Ibid page 242.

[27] For a discussion of the role of GPS jamming in the Gulf War, see Tegg Westbrook, "The Global Positioning System and Military Jamming: geographies of electronic warfare," *Journal of Strategic Security* 12, no. 2 (2019): 1-16. www.jstor.org/stable/26696257.

the procurement of relevant technology from Japan and the West.[28] Over time, North Korea continued to develop its IT capabilities as a means for revenue generation by providing services in image and video processing, data entry, computer animation, and software development for clients overseas.[29] These trends continued and accelerated as Kim Jong Un assumed power in 2013, during which North Korea's cyber capabilities have reached new levels of sophistication as both an asymmetric offensive capability and a tool for illicit revenue generation.[30] [31]

In 2005, Joseph S. Bermudez Jr. published a list of operational principles that the MPAF reportedly believed important for successful SIGINT, EW, and EIW, which drew from author interviews, declassified documents, and a U.S. Army publication from 1992[32]:

> Limiting electronic emissions by strict adherence to COMSEC regulations which emphasize the use of landlines, total or partial radio silence, etc.; When electronic emissions are required, to limit the enemy's ability to exploit them by limiting their duration, use of directional antennas, using reduced power outputs, etc.; Extensive use of electronic deception operations which will include the creation, operation, and maintenance of false communication networks, the random use of decoy transmitters, etc.; Strict adherence to tactical COMSEC and OPSEC techniques such as the frequent relocation of C4ISR assets when possible, fortification of such units when relocation is not feasible or desirable, the frequent and random changing of call signs and frequencies, etc.; Extensive route training of communications operators to follow COMSEC regulations and to operate their networks/assets under conditions of extensive enemy jamming and countermeasures (electronic and physical attack); Education of a cadre of officers and enlisted personnel dedicated to the SIGINT, EW, and EIW missions; Thorough prewar physical and electronic reconnaissance to locate and identify major enemy C4ISR networks and assess their vulnerabilities; Rapid wartime neutralization or destruction of enemy C4ISR capabilities. Secure its computer networks from EIW operations while conducting such operations against the enemy's military and civilian networks.

---

[28] Joseph S. Bermudez Jr., "SIGINT, EW and EIW in the Korean People's Army: An Overview of Development and Organization," *Bytes and Bullets in Korea,* ed. Alexandre Y. Mansourov (Honolulu: Asia-Pacific Center for Security Studies, 2005), http://www.apcss.org/Publications/Edited%20Volumes/BytesAndBullets/TOC.pdf.

[29] "Archive for the 'Animation Category," North Korean Economy Watch, accessed Fall 2019, http://www.nkeconwatch.com/category/civil-society/art/animation/page/4/.

[30] "Guidance on North Korean Cyber Threat," Department of State, Department of the Treasury, Department of Defense, and the Federal Bureau of Investigation, April 15, 2020, https://www.us-cert.gov/sites/default/files/2020-04/DPRK_Cyber_Threat_Advisory_04152020_S508C.pdf.

[31] For work describing North Korea's operational and strategic thinking, see James M. Minnich, *North Korean Tactics.* (2011), http://www.faoa.org/resources/Documents/NorthKoreanMilitaryTactics.pdf; Donghui Park, "North Korea Cyber Attacks: A New Asymmetrical Military Strategy," The Henry M. Jackson School of International Studies at the University of Washington, June 28, 2016, https://jsis.washington.edu/news/north-korea-cyber-attacks-new-asymmetrical-military-strategy/; Joseph S. Bermudez, *Shield of the Great Leader: The Armed Forces of North Korea*. (Sydney: Allen & Unwin, 2001 and London: I.B. Taurus, 2001); Joseph S. Bermudez, Jr, *North Korea's Strategic Culture.* (Defense Threat Reduction Agency Advanced Systems and Concepts Office, 2006), https://fas.org/irp/agency/dod/dtra/dprk.pdf; and Joseph S. Bermudez Jr., "North Korea and the Political Uses of Strategic Culture," *Strategic Culture and Weapons of Mass Destruction: Culturally Based Insights into Comparative National Security Policymaking,* ed. Jeannie Johnson, Kerry Kartchner, and Jeffrey Larsen (New York: Palgrave Macmillan), https://www.palgrave.com/gp/book/9780230618305.

[32] This information was first published Joseph S. Bermudez Jr., "SIGINT, EW and EIW in the Korean People's Army: An Overview of Development and Organization," *Bytes and Bullets in Korea,* ed. Alexandre Y. Mansourov (Honolulu: Asia-Pacific Center for Security Studies, 2005), http://www.apcss.org/Publications/Edited%20Volumes/BytesAndBullets/TOC.pdf, and was compiled using interview transcripts, declassified documents and the U.S. Army's North Korean People's Army Handbook (1992).

North Korea's documented use of extensive peacetime cyberespionage operations[33], GPS jamming devices against civilian targets[34], and false signal broadcasts on merchant vessels to evade sanctions[35] suggests that North Korea may continue to adapt similar operational principles for the modern technological environment. The following sections of this report examine the technology systems that would provide North Korea's intelligence apparatus and military with such a capability.

Infrastructure & Assets

Over the last decade, North Korea has significantly expanded its domestic telecommunications and internet infrastructure to advance both military and economic objectives.[36] Infrastructural improvements may improve connectivity between North Korea's military and intelligence organizations and facilitate expanded asymmetric operations in cyberspace and across the electromagnetic spectrum. However, because limited information exists in the public domain on the technical specifications of North Korea's domestic systems, additional research is required in order to determine the net effect of recent infrastructural improvements on North Korea's strategic SA capabilities.

Telecommunications

North Korea maintains a national fiber optic cable system that provides landline communications services across the country, which serves as the backbone of its command, control, and communications (C3) system for conventional forces.[37] In the early 1990s, the United Nations Development Program laid fiber optic cables in North Korea and launched the Pyongyang Optical Fiber Cable Factory (평양빛섬유통신케블[광케이블]공장), which has domestic production capability for fiber optic cables.[38] Thailand's Loxley Pacific Company and North Korea's state-owned Korea Post and Telecommunications Corporation (조선체신회사) later established a joint venture called Northeast Asia Telephone and Telegraph (동북아시아전화통신회사) to expand the fiber optic cable lines to the

---

[33] United Nations, Security Council, *Report of the Panel of Experts established pursuant to resolution 1874 (2009),* S/2020/151, March 2, 2020, accessed Spring 2020. https://undocs.org/S/2020/151.

[34] North Korea has engaged in GPS jamming and spoofing activities since the Korean War. For a summary of more recent jamming incidents, see "Space Threat 2018: North Korea Assessment," Aerospace, CSIS, 2018, https://aerospace.csis.org/space-threat-2018-north-korea/.

[35] In March 2019, the UN Panel of Experts observed that North Korea has deployed GPS spoofing systems on its merchant fleet to obfuscate vessel identity and location by allowing vessels to adopt the identities of other ships or appear in multiple locations at the same time. See United Nations, Security Council, *Report of the Panel of Experts established pursuant to resolution 1874 (2009),* S/2019/171, March 12, 2019, accessed Spring 2020. https://undocs.org/S/2019/171

[36] For detailed analysis of the historical development of North Korea's telecommunications and Internet infrastructure, see Alexandre Y. Masourov, "North Korea on the Cusp of Digital Transformation," The Nautilus Institute, 2011, accessed Fall 2019, http://www.nautilus.org/wp-content/uploads/2011/12/DPRK_Digital_Transformation.pdf. See also: Marcus Noland, "Telecommunications in North Korea: Has Orascom Made the Connection?," *North Korean Review* 5, no. 1 (2009): 62-74, accessed Fall 2019. www.jstor.org/stable/43910262.

[37] The public domain contains little information about the technical specificiations of North Korea's nuclear C3 system and whether or not it has developed an independent system for its nuclear forces. For more information, see Myeongguk Cheon, "DPRK'S NC3 SYSTEM", NAPSNet Special Reports, June 06, 2019, https://nautilus.org/napsnet/napsnet-special-reports/dprks-nc3-system/.

[38] Office of the Secretary of Defense, "Military and Security Developments Involving the Democratic People's Republic of Korea 2017," Department of Defense, 2017, https://fas.org/irp/world/dprk/dod-2017.pdf.

Rajin-Sunbong Economic and Trade Zone in the northeast of the country.[39] Today, fiber optic connections reportedly extend to the county-level.[40] The World Bank estimates that in 2017, the latest year on record, North Korea had 1.18 million landline subscriptions, which constitutes approximately 5% of the population.[41]

North Korea also maintains wireless communications infrastructure through three telecommunications companies.[42] In 2008, North Korea established the joint venture CHEO Holdings with the Egyptian telecommunications company Orascom Telecommunication to launch Koryolink (고려링크), which provides 3G mobile data services including but not limited to voice, video, SMS, MMS, voicemail, and domestic intranet access but no international phone services.[43] In July 2019, the *Washington Post* reported that the Chinese telecommunications giant Huawei Technologies Co. has provided CHEO Holdings with equipment, software, and network integration services needed to launch Koryolink since at least 2008.[44] North Korea's state-owned Korea Post and Telecommunications Corporation reportedly worked with both Huawei and Orascom Telecommunication to incorporate encryption, call surveillance, and communications jamming systems that both support the state's domestic surveillance program and prevent foreign espionage.[45] Two other telecommunications companies, Kangsong Net (강성네트망) and Byol (별), reportedly also provide mobile services to North Korean users, but unlike Koryolink, they do not provide services to foreigners.[46] [47]

North Korea's consumer market for smartphones is reportedly expanding for phone models that are imported from abroad and produced domestically, which reportedly use software to track users, limit data transfers, and censor content.[48] The World Bank estimates that in 2017, the latest year on record, North Korea had 3.81 million mobile

---

[39] Loxley Pacific Company later helped develop North Korea's Internet infrastructure through a second joint venture. See Marcus Noland, "Telecommunications in North Korea: Has Orascom Made the Connection?," *North Korean Review* 5, no. 1 (2009): 62-74, accessed Fall 2019. www.jstor.org/stable/43910262.

[40] "East Asia/Southeast Asia :: Korea, North," *CIA,* accessed Fall 2019, https://www.cia.gov/library/publications/the-world-factbook/geos/print_kn.html.

[41] "Fixed telephone subscriptions – Korea, Dem. People's Rep.," The World Bank, accessed Fall 2019, https://data.worldbank.org/indicator/IT.MLT.MAIN?end=2018&locations=KP&name_desc=false&start=2014.

[42] In 2003, before North Korea established a domestic wireless system, Chinese companies reportedly constructed relay towers along the China-North Korea border, which led to a dramatic increase in the prepaid phone use in North Korea's border region met by crackdown from North Korea officials. Additional research is required to determine the extent to which China's telecommunications infrastructure along the China-North Korea border may support military or civilian communications networks in North Korea. For more information on early developments in China's wireless industry, see Marcus Noland, "Telecommunications in North Korea: Has Orascom Made the Connection?," *North Korean Review* 5, no. 1 (2009): 62-74, accessed Fall 2019. www.jstor.org/stable/43910262.

[43] North Korea's state-owned Korea Post and Telecommunications Corporation and Egypt's Orascom Telecommunication established the joint venture. For more information, see Alexandre Y. Masourov, "North Korea on the Cusp of Digital Transformation," The Nautilus Institute, 2011, accessed Fall 2019, http://www.nautilus.org/wp-content/uploads/2011/12/DPRK_Digital_Transformation.pdf.

[44] Ellen Nakashima, Gerry Shin, and John Hudson, "Leaked documents reveal Huawei's secret operations to build North Korea's wireless network," *The Washington Post,* July 22, 2019, https://www.washingtonpost.com/world/national-security/leaked-documents-reveal-huaweis-secret-operations-to-build-north-koreas-wireless-network/2019/07/22/583430fe-8d12-11e9-adf3-f70f78c156e8_story.html.

[45] Martyn Williams, "North Korea's Koryolink: Built for Surveillance and Control," 38 North, July 22, 2019, https://www.38north.org/2019/07/mwilliams072219/.

[46] In interviews conducted by the author in April 2020, at least one expert speculated that Kangsong Net and Byol may be the same entity. Additional research is required in order to determine the relationship of Kangsong Net and Byol.

[47] Tia Han, "Call me, comrade: the surprise rise of North Korean smartphones," *NK News,* July 30, 2018, https://www.nknews.org/2018/07/call-me-comrade-the-surprise-rise-of-north-korean-smartphones/.

[48] Ju-min Park, "How a sanctions-busting smartphone business thrives in North Korea," *Reuters,* September 25, 2019, https://www.reuters.com/article/us-northkorea-smartphones-insight/how-a-sanctions-busting-smartphone-business-thrives-in-north-korea-idUSKBN1WB01Z.

phone subscriptions, which constitutes approximately 15% of the population.[49] As its domestic telecommunications infrastructure evolves to support significantly more phone subscriptions, North Korea may develop more resilient communications systems that could support military and intelligence operations across the spectrum of conflict. However, increasing service demands from an expanding civilian and military user base may also negatively affect system performance.

Intranet

North Korea maintains an expansive intranet called the Kwangmyong (광명망), which is disconnected from the global internet. The Kwangmyong connects government institutions, companies, banks, educational institutions, and other domestic users to websites containing e-mail services, educational materials, advertisements, basic websites, and propaganda.[50] The Kwangmyong uses fiber optic cables to transmit data with reportedly different connection configurations for enterprises and private households.[51] In preliminary research, the author found no public reporting that examines how Kwangmyong development does or does not affect North Korea's military command and control systems, which also use North Korea's fiber optic cable infrastructure.

While reporting contains varied estimates for the number of people and companies with an active Kwangmyong connection, evidence suggests that access is expanding as Kim Jong Un seeks to transition towards a "knowledge-based economy" (지식경제사회), for which key elements include e-commerce systems and a remote digital education infrastructure.[52] In November 2018, Korean Central Television unveiled Mirae, a new Wi-Fi service that enables mobile devices to access the intranet, which was the first publicized instance of an outdoor Wi-Fi service in North Korea.[53] According to a November 2019 article by the North Korean outlet *Pyongyang Times*, users can access the Mirae network at Kim Il Sung University and Kim Chaek University of Technology; on Mirae Scientists, Ryomyong, Yonggwang, and Haebangsan Streets; at the Sci-Tech Complex; and in other parts of Pyongyang, with plans to expand across the city.[54] North Korea's expanding intranet continues to improve connectivity between government institutions, enterprises, universities, and other organizations, which may facilitate communication and information sharing despite strict surveillance mechanisms and user controls on most operating systems.[55] Additional research is required to understand how increasing service demands from an expanding user base may affect performance during crisis or conflict.

---

[49] See "Mobile cellular subscriptions (per 100 people) – Korea, Dem. People's Rep.," The World Bank, accessed Fall 2019, https://data.worldbank.org/indicator/IT.CEL.SETS.P2?end=2018&locations=KP&name_desc=false&start=2014; and "이동전화가입자 수 [Number of mobile phone subscribers]," Korean Statistical Information Service, accessed Fall 2019, http://kosis.kr/statHtml/statHtml.do?orgId=101&tblId=DT_IZGI03_502&vw_cd=MT_BUKHAN&conn_path=MT_BUKHAN&path=%252Fbukhan%252Fsearch%252Fsearch.do, which draw estimates from 2016 and 2017 respectively.

[50] Alexandre Y. Masourov, "North Korea on the Cusp of Digital Transformation," The Nautilus Institute, 2011, accessed Fall 2019, http://www.nautilus.org/wp-content/uploads/2011/12/DPRK_Digital_Transformation.pdf.

[51] Ibid.

[52] 나승혁 [Na Seung Hyuk], *북한과학기술의 수준 분석 및 전략적 활용방안 도출 연구* [*A study on the analysis of level of North Korea's Science & Technology and the derivation of its strategic utilization*], 한국과학기술기획평가원 [Korea Institute of S&T Evaluation and Planning] 2016-007 (2016).

[53] Pratik Jakhar, "North Korea's high-tech pursuits: Propaganda or progress?," *BBC,* December 25, 2018, https://www.bbc.com/news/world-asia-46563454.

[54] Jong Kwa Sun, "Company sniffs opportunity out of wireless networking," Pyongyang Times, accessed Spring 2020, http://www.pyongyangtimes.com.kp/?bbs=32189.

[55] North Korea's domestically produced operating systems support the regime's domestic surveillance capability. North Korean computers run a Linux-based operating system called Red Star, which uses encryption and firewalls to restrict certain user functions. The source code for Red Star 3.0 has appeared in the public domain, and various technical blogs have analyzed the code to understand certain surveillance

Internet

North Korea's internet users[56] can access the internet in three ways, each of which relies on infrastructure owned and controlled by major Chinese and Russian telecommunications companies.[57] First, North Korean computers can access the internet allocated .kp range of IP addresses 175.45.176.0/22, which constitutes the block of IP addresses allocated to North Korea by the Internet Assigned Numbers Authority.[58] The Chinese state-owned telecommunications company China Unicom and the Russian state-owned company TransTelekom route internet traffic for IP addresses in this range, which hosts the nation's only internet-accessible websites of North Korean state-run media, travel, and education-related sites.[59] Internet users in North Korea can reportedly also access two assigned IP ranges: 210.52.109.0/24, controlled by China Netcom, and 77.94.35.0/24, controlled by a Russian satellite company that resolves to SatGate in Lebanon.[60] Subnet analysis by cybersecurity firm Recorded Future indicates that the proportion of North Korean internet activity transiting Russia's TransTelekom infrastructure is increasing relative to other providers, reaching 45% in February 2020.[61]

North Korea maintains limited but rapidly expanding access to the internet from domestic computers and networks. Historically, North Korea's limited infrastructure has lacked redundant systems and relied on shared servers, proxies, and load balancers to host websites and route outbound internet traffic, with performance further degraded by significant bandwidth used for video streaming and online gaming services.[62] However, since

---

functions. For some examples, see Jamie Lendino, "North Korea's Linus-based Red Star OS is as oppressive as you'd expect," Extreme Tech, December 28, 2015, https://www.extremetech.com/computing/219963-north-koreas-linux-based-red-star-os-is-as-oppressive-as-youd-expect; also see Robert Hansen, "North Korea's Naenara Web Brower: It's Weirder Than We Thought," White Hat Security, January 08, 2015, https://www.whitehatsec.com/blog/north-koreas-naenara-web-browser-its-weirder-than-we-thought/. North Korean state-run media has reported that some North Korean companies and institutions have started to run Red Star 4.0. For more information, see Martyn Williams, "Red Star 4 appears in a workplace learning system," North Korea Tech, February 11, 2020, https://www.northkoreatech.org/2020/02/11/red-star-4-appears-in-a-workplace-learning-system/.

[56] Most North Koreans cannot access the internet, which is restricted to certain government departments, universities, and trading companies. Visiting foreigners may also have limited access. North Korea's domestic internet users reportedly access a variety of social media accounts; use VoIP services to communicate internationally; access AOL accounts; investigate industrial hardware and technology optimization services; research the work of top global cybersecurity firms; receive training for using satellite communications equipment; and research international academic publications. Several reports on North Korean internet activity indicate that between 2017 and 2018, North Korean internet users had predominantly used Western social media websites and search engines like Facebook, Instagram, and Google before migrating to their Chinese equivalents like Baidu, Alibaba, and Tencent. Their analysis did find, however, that North Korean Internet users continued to use LinkedIn, albeit at a low volume. For more analysis of the activities of internet users in North Korea, see "North Korea's Ruling Elite Are Not Isolated," Insikt Group, Recorded Future, July 25, 2017, https://www.recordedfuture.com/north-korea-Internet-activity/. See also "Shifting Patterns in Internet Use Reveal Adaptable and Innovating North Korean Ruling Elite," Insikt Group, Recorded Future, October 25, 2018, https://www.recordedfuture.com/north-korea-Internet-usage/.

[57] "Shifting Patters in Internet Use Reveal Adaptable and Innovative North Korean Ruling Elite," Insikt Group, Recorded Future, October 25, 2018, https://www.recordedfuture.com/north-korea-Internet-usage/.

[58] For more information on IP address allocation, see "Number Resources," Internet Assigned Numbers Authority, accessed Fall 2019, https://www.iana.org/numbers.

[59] "Shifting Patters in Internet Use Reveal Adaptable and Innovative North Korean Ruling Elite," Insikt Group, Recorded Future, October 25, 2018, https://www.recordedfuture.com/north-korea-Internet-usage/.

[60] It is possible that the Internet users in North Korea observed during the research period were foreigners. For more information, see "Shifting Patters in Internet Use Reveal Adaptable and Innovative North Korean Ruling Elite," Insikt Group, Recorded Future, October 25, 2018, https://www.recordedfuture.com/north-korea-Internet-usage/.

[61] "How North Korea Revolutionized the Internet as a Tool for Rogue Regimes," Insikt Group, Recorded Future, February 9, 2020, https://www.recordedfuture.com/north-korea-internet-tool/.

[62] According to Recorded Future, "[l]oad balancers manage ingoing and outgoing internet traffic and distribute it to a specific range of servers to increase capacity and network reliability for concurrent users." See Priscilla Moriuchi, "North Korea's Ruling Elite Adapt Internet Behavior to Foreign Scrutiny," Insikt Group, Recorded Future, April 25, 2018, https://www.recordedfuture.com/north-korea-Internet-behavior/. To see a breakdown of DPRK Internet activity, see "North Korea's Ruling Elite Are Not Isolated," Insikt Group, Recorded Future, July 25, 2017, https://www.recordedfuture.com/north-korea-Internet-activity/.

TransTelekom laid a new fiber optic cable in 2017, North Korean internet traffic has reportedly increased 300%.[63] North Korea's expanded internet infrastructure since 2017 may have enabled its military and intelligence to change operational approaches in cyberspace. In the past, North Korea's cyber operatives conducted operations from overseas locations, which provided better internet infrastructure and helped obfuscate their identities.[64] However, in February 2020, Recorded Future reported that nearly all such activity now emanates from territorial North Korea, a change that the UN Panel of Experts also observed in its annual report one month later.[65] [66] While previous studies have assessed that North Korea's limited domestic internet activity was insufficient to telegraph early warning of missile tests or strategic military action, it is possible that North Korean internet activity could begin to provide greater early warning value to the United States and its allies as domestic use continues to expand.[67]

Research also suggests that North Korea's internet users are developing stronger operations security (OPSEC) practices, which may reduce the effectiveness of U.S. and allied surveillance and improve North Korea's reconnaissance capabilities. For example, between 2017 and 2018, Recorded Future observed a 1,200% increase in the use of obfuscation services like virtual private networks (VPNs), virtual private servers, transport layer security, and onion routing, which conceal online identities and browsing activities.[68] Following the European Union's passage of the General Data Protection Regulation (GDPR), North Korea's internet users also reportedly began routing internet traffic through Europe, where the new policy provided greater legal protections for user privacy.[69] More recently, North Korea has reportedly created its own VPN to use DNS tunneling, which could support more sophisticated technical reconnaissance missions.[70] While the United States and its allies are believed to have extensively penetrated North Korea's domestic cyber infrastructure for surveillance and early warning purposes, North Korea's continued OPSEC improvements may reduce its effectiveness.[71]

Pronouncements by North Korean officials suggest that the development of North Korea's internet will remain a priority in at least the near-term. In August 2018, North Korea Tech reported that North Korea completed construction of a new Pyongyang headquarters for the Internet Communication Bureau (평양인터네트통신국건설), for which the Minister of Posts and Telecommunications and Vice Minister of External

---

[63] "How North Korea Revolutionized the Internet as a Tool for Rogue Regimes," Insikt Group, February 9, 2020, https://www.recordedfuture.com/north-korea-internet-tool/.

[64] David E. Sanger, David D. Kirkpatrick and Nicole Perlroth, "The World Once Laughed at North Korean Cyberpower. No More," The New York Times, October 15, 2017, https://www.nytimes.com/2017/10/15/world/asia/north-korea-hacking-cyber-sony.html.

[65] "How North Korea Revolutionized the Internet as a Tool for Rogue Regimes," Insikt Group, Recorded Future, February 9, 2020, https://www.recordedfuture.com/north-korea-internet-tool/.

[66] United Nations, Security Council, *Report of the Panel of Experts established pursuant to resolution 1874 (2009),* S/2020/151, March 2, 2020, accessed Spring 2020. https://undocs.org/S/2020/151.

[67] The report arrives at these conclusions in part because so few North Koreans access the internet domestically, and when they do, they do not do so for malicious purposes. For more information, see "North Korea's Ruling Elite Are Not Isolated," Insikt Group, Recorded Future, July 25, 2017, https://www.recordedfuture.com/north-korea-Internet-activity/.

[68] Priscilla Moriuchi, "North Korea's Ruling Elite Adapt Internet Behavior to Foreign Scrutiny," Insikt Group, Recorded Future, April 25, 2018, https://www.recordedfuture.com/north-korea-Internet-behavior/.

[69] Ibid.

[70] "How North Korea Revolutionized the Internet as a Tool for Rogue Regimes," Insikt Group, Recorded Future, February 9, 2020, https://www.recordedfuture.com/north-korea-internet-tool/.

[71] David E. Sanger and Martin Fackler, "N.S.A. Breached North Korean Networks Before Sony Attack, Officials Say," *The New York Times,* January 18, 2015, https://www.nytimes.com/2015/01/19/world/asia/nsa-tapped-into-north-korean-networks-before-sony-attack-officials-say.html.

Economic Relations had attended a groundbreaking ceremony in 2015.[72] One observer suggested that the purpose of the bureau is "focused on the global internet…[implying] that internet usage and access is growing in [North Korea], although still at a low level."[73] While the Bureau's ultimate purpose is uncertain, its expansion coincides with infrastructural investments that have significantly expanded internet capacity within the country since 2017, which may signal North Korean leadership's commitment to developing its military and intelligence capabilities in cyberspace.

Satellites

North Korea does not have operational satellites despite clear space ambitions demonstrated over the last two decades. Since 1998, North Korea has attempted to launch five satellites, the last of which occurred in 2016, and while two have successfully entered orbit, neither has remained functional once in space.[74] Evidence suggests that North Korea continues to invest in key infrastructure that supports its space program. For example, analysts at the James Martin Center for Nonproliferation Studies used commercially available satellite imagery to show that, as recently as March 2020, North Korea expanded Sohae Satellite Launching Station (서해위성발사장), which supports testing for both satellite launch vehicles and missile systems.[75] North Korean state media also continues to express commitment to developing the country's space program, which has value not only for its military and intelligence apparatus but also as a tool for regime propaganda.[76] For example, in April 2020, Naenara, a North Korean state-run propaganda website, affirmed its commitment "to develop space thoroughly for peaceful purposes" through projects in satellite image processing, geographic information systems software development, and broadband communications.[77]

Some analysts have argued that North Korea does not appear to be making sufficient investments to build or sustain a domestic space industrial base, relying instead on technology from abroad to advance its satellite capability.[78] Evidence also suggests that North Korea may also seek to benefit from China's BeiDou Navigation Satellite System, which is slated to be globally operational by May 2020.[79] For example, news reports indicate that, in 2014, North Korean engineers traveled to China for training on BeiDou systems, which could support both its missile navigation systems and its rapidly expanding telecommunications network.[80] However, additional

---

[72] Martyn Williams, "North Korea and the Internet: Building for the Future," North Korea Tech, August 1, 2018, https://www.northkoreatech.org/2018/08/01/pyongyang-Internet-communication-bureau/.

[73] Ibid.

[74] "Space Threat 2018: North Korea Assessment," Aerospace, CSIS, 2018, https://aerospace.csis.org/space-threat-2018-north-korea/.

[75] Geoff Brumfiel, "North Korea Seen Expanding Rocket Launch Facility It Once Promised To Dismantle," NPR, March 27, 2020, https://www.npr.org/2020/03/27/822661018/north-korea-seen-expanding-rocket-launch-facility-it-once-promised-to-dismantle.

[76] For an example of analysis considering the role of space program development in North Korean propaganda, see Jeffrey Lewis, "Is North Korea Gearing Up for Another Space Launch," 38 North, June 2, 2015, https://www.38north.org/2015/06/jlewis060215/

[77] Yi Wonju, "N.K. pushing for five-year space development program purely for peaceful purposes: state media," Yonhap News Agency, April 02, 2020, https://en.yna.co.kr/view/AEN20200402005600325.

[78] "Space Threat 2018: North Korea Assessment," Aerospace, CSIS, 2018, https://aerospace.csis.org/space-threat-2018-north-korea/.

[79] Liu Zhen, "China's BeiDou system one satellite closer to full operation," South China Morning Post, March 10, 2020, https://www.scmp.com/news/china/science/article/3074499/chinas-beidou-system-one-satellite-closer-full-operation.

[80] Martyn Williams, "North Koreans learn about China's Beidou satellite navigation system," North Korea Tech, July 31, 2014, https://www.northkoreatech.org/2014/07/31/north-koreans-learn-about-chinas-beidou-satellite-navigation-system/.

research is required in order to determine if or how North Korea uses BeiDou systems to support civilian or military infrastructure.[81] [82]

Air- and Sea-Based Systems

The Korean People's Air Force (KPAF; 조선인민군 항공 및 반항공군) and Navy (KPN; 조선인민군 해군) rely on aging equipment and have limited systems for reconnaissance and surveillance purposes. According to a 2018 Defense White Paper by the South Korean Ministry of National Defense, the Korean People's Army Air and Anti-Air Force consists of 810 combat aircraft, 30 surveillance aircraft, and 340 non-combat aircraft including An-2s, 170 trainer aircraft, and 290 helicopters.[83] South Korean experts believe that the KPAF suffers from a lack of flight training and increasingly outdated technological knowledge.[84]

Some have assessed that the KPAF's old systems could neither withstand modern EW attacks or survive against U.S. and South Korean forces, which has led to a significant reliance on air-defense systems.[85] North Korea maintains what the U.S. Department of Defense describes as "a dense, overlapping air defense system of SA-2/3/5 [surface-to-air missile] sites, mobile and fixed [anti-aircraft artillery], and numerous man-portable air-defense systems, like the SA-7," consisting of both foreign-origin and domestically produced equipment.[86] Some analysts estimate that North Korea has more than 50 early warning radar systems, including more advanced systems like phased array radar systems procured from Iran. [87] [88] Some reports also indicate that North Korea uses automated systems to improve the speed and accuracy of air defense systems.[89]

---

[81] Some observers have speculated whether China would provide North Korea with access to BeiDou's military signal capabilities. For example, see Peter J. Brown, "Is North Korea Using China's Satellites to Guide Its Missiles?," The National Interest, May 23, 2017, https://nationalinterest.org/blog/the-buzz/north-korea-using-chinas-satellites-guide-its-missiles-20810

[82] Systems that support both conventional and nuclear systems create escalatory risks through entanglement. For more information, see James M. Acton, "Escalation through Entanglement: How the Vulnerability of Command- and-Control Systems Raises the Risks of an Inadvertent Nuclear War," International Security 43:1 (2018): 56-99. https://www.mitpressjournals.org/doi/pdf/10.1162/isec_a_00320.

[83] "2018 국방백서 [2018 Defense White Paper]," 대한민국 국방부 [Republic of Korea Ministry of National Defense] (2018), http://www.mnd.go.kr/user/mnd/upload/pblictn/PBLICTNEBOOK_201901160236460390.pdf

[84] 나승혁 [Na Seung Hyuk], *북한과학기술의 수준 분석 및 전략적 활용방안 도출 연구* [*A study on the analysis of level of North Korea's Science & Technology and the derivation of its strategic utilization*], 한국과학기술기획평가원 [Korea Institute of S&T Evaluation and Planning] 2016-007 (2016).

[85] *The conventional military balance on the Korean Peninsula*, The International Institute for Strategic Studies. (2018). https://www.iiss.org/-/media/images/comment/military-balance-blog/2018/june/the-conventional-military-balance-on-the-korean-peninsula.ashx?la=en&hash=C51D23B426579E41B43CF30A0D8969328FE57803

[86] Anthony H. Cordesman and Aaron Lin, *The Changing Military Balance in the Koreas and Northeast Asia* (Lanham: Rowman & Littlefield, 2015), https://csis-prod.s3.amazonaws.com/s3fs-public/legacy_files/files/publication/150615_Cordesman_NortheastAsiaMilBalance_Web.pdf.

[87] *The conventional military balance on the Korean Peninsula*, The International Institute for Strategic Studies. (2018). https://www.iiss.org/-/media/images/comment/military-balance-blog/2018/june/the-conventional-military-balance-on-the-korean-peninsula.ashx?la=en&hash=C51D23B426579E41B43CF30A0D8969328FE57803

[88] Dave Majumdar, "If Donald Trump Attacks North Korea: Beware of Kim's Air Defense Systems," The National Interest, April 14, 2017, https://nationalinterest.org/blog/the-buzz/if-donald-trump-attacks-north-korea-beware-kims-air-defense-20207.

[89] Terence Roehrig, "The abilities – and limits – of North Korean early warning," Bulletin of the Atomic Scientists, November 27, 2017, https://thebulletin.org/2017/11/the-abilities-and-limits-of-north-korean-early-warning/.

The KPN is considered one of the world's largest submarine forces, with around 70 attack, coastal, and midget-type submarines.[90] North Korea's small coastal submarines comprise the largest proportion of its submarine fleet and have been used historically for espionage missions, infiltration, and coastal defense.[91] The KPN is the primary operator of North Korea's submarine assets, but a small number are also operated by the RGB.[92] In 2017, the U.S. Department of Defense observed that KPN "has displayed some modernization efforts," as evidenced by upgrades of vessels as well as programs to produce modern "missile-armed patrol boats and corvettes."[93] Additional research is required to determine what technical systems North Korea may use to communicate with units while at sea, including ballistic submarines.[94]

Unmanned Aerial Vehicles

North Korea has developed unmanned aerial vehicles (UAVs) for military and reconnaissance purposes that are generally regarded as "rudimentary" and without precision or stealth capabilities.[95] North Korea has developed UAVs after receiving equipment or technical consultation from countries like China, Russia, Syria, and Egypt over several decades.[96] In 2014, the Sejong Institute, a South Korean think tank, estimated that North Korea had approximately 1,000 UAVs in strategic locations around the country, which appear modeled after UAVs from the United States, China, and Russia.[97] Others have placed the figure lower, estimating that North Korea owns 300 to 400 unmanned reconnaissance planes with a flight range of approximately 600 kilometers.[98]

Since 2013, South Korean media has repeatedly reported stories about crashed UAV systems believed to have originated from North Korea to collect military intelligence. Between 2013 to 2014, North Korean UAVs reportedly

---

[90] Office of the Secretary of Defense, "Military and Security Developments Involving the Democratic People's Republic of Korea 2017," Department of Defense, 2017, https://fas.org/irp/world/dprk/dod-2017.pdf

[91] "North Korea Submarine Capabilities," Nuclear Threat Initiative, October 4, 2018, https://www.nti.org/analysis/articles/north-korea-submarine-capabilities/

[92] Ibid.

[93] Office of the Secretary of Defense, "Military and Security Developments Involving the Democratic People's Republic of Korea 2017," Department of Defense, 2017, https://fas.org/irp/world/dprk/dod-2017.pdf

[94] For an analysis that considers the relationship of North Korea's submarine communications systems and nuclear stability, see Vipin Narang and Ankit Panda, "Command and Control in North Korea: What a Nuclear Launch Might Look Like," War on the Rocks, September 15, 2017, https://warontherocks.com/2017/09/command-and-control-in-north-korea-what-a-nuclear-launch-might-look-like/

[95] *The conventional military balance on the Korean Peninsula*, The International Institute for Strategic Studies. (2018). https://www.iiss.org/-/media/images/comment/military-balance-blog/2018/june/the-conventional-military-balance-on-the-korean-peninsula.ashx?la=en&hash=C51D23B426579E41B43CF30A0D8969328FE57803

[96] North Korea's initial interest in UAVs is believed to have started in the 1970s, when United States's UAVs (AQM-34Q) based on Osan Air Base in South Korea flew hundreds of missions along the coast for communication monitoring. Investment into the country's UAV development is believed to have increased shortly after United States' use of UAVs during Operation Iraqi Freedom. North Korea reportedly acquired its first UAVs from China between 1988 and 1990, shortly after an announcement by South Korean Ministry of National Defense in 1988 that it was preparing to finance development of reconnaissance UAVs. For more information on the history of North Korea's drone program, see, for example: Joseph S. Bermudez Jr., "North Korea Drones On: Redeux," 38 North, January 19, 2016, https://www.38north.org/2016/01/jbermudez011916/ and 나승혁 [Na Seung Hyuk], *북한과학기술의 수준 분석 및 전략적 활용방안 도출 연구* [*A study on the analysis of level of North Korea's Science & Technology and the derivation of its strategic utilization*], 한국과학기술기획평가원 [Korea Institute of S&T Evaluation and Planning] 2016-007 (2016).

[97] 이대우 [Lee Dae Woo], 북한 무인기: 새로운 비대칭 무기 [North Korean UAV: A New Asymmetric Weapon], 정세와 정책 [State of Affairs and Policy] 2014-05, Sejong Institute (2014), http://napci.sejong.org/boad/bd_news/1/egofiledn.php?conf_seq=2&bd_seq=465&file_seq=1067.

[98] See Tae-jun Kang, "North Korea's Quest for Autonomous Technology," The Diplomat, July 13, 2018, https://thediplomat.com/2018/07/north-koreas-quest-for-autonomous-technology/ and 민병조 [Min Byoung Jo], 비행거리 2 배 늘어난 북한 무인기…북한 정찰총국 소행 추정 [North Korea's UAVs double in flight distance…North Korean RGB Believed to be Behind Flight], MBN News, June 22, 2017, http://mbn.mk.co.kr/pages/news/newsView.php?category=mbn00006&news_seq_no=3260422.

crashed in Paju, Baengnyeon-do, and Samcheok, South Korea.[99] [100] The vehicles found in Paju and Samcheok were SKY09P models, which are produced by a Chinese company.[101] A crashed UV10CAM vehicle found in Baengnyeon-do was also reportedly based on a Chinese model and used a mounted Nikon D800 DSLR camera.[102] [103] Some observers have speculated that North Korea's low-cost drones have supported high-value reconnaissance missions. For example, after a North Korea-origin drone crashed in Inje, South Korea in June 2017, some reports speculated that the same model drone had been the source of aerial photos of Terminal High Altitude Area Defense (THAAD) system components that North Korea had released publicly the month prior.[104] [105]

Public reporting suggests that North Korea may have also developed more advanced UAV systems. In September 2018, Kim Jong Un reportedly hosted a UAV airshow during a visit by South Korean President Moon Jae-in.[106] Moon Sung Tae, a senior researcher at the Korea Aerospace Research Institute (한국항공우주연구원), commented that the show's coordination, operation, and real-time kinematic capabilities rivaled that of the South Korean drone show at the PyeongChang Olympics.[107] If true, these cases indicate that North Korea may continue to develop more advanced UAV technology that could support a range of intelligence and military operations.

Capabilities

While North Korea's infrastructure investments may improve connectivity between the organizations involved in North Korea's military and intelligence enterprise, it may also enable North Korea to engage in an expanding range of provocative attacks against adversary computer networks and communications systems, which has long been a key component of its asymmetric approach to military engagements. The following section explores how

---

[99] "무인비행장치 안전관리 정책방향 [Policy Direction for Safety Management of Uninhabited Air Vehicles]," 국토교통부 [South Korea Ministry of Land, Infrastructure and Transport], September 2015, http://www.aerospace.or.kr/m/_inc/downFileData.php?id=721.

[100] Joseph S. Bermudez Jr., "North Korea Drones On: Redeux," 38 North, January 19, 2016, https://www.38north.org/2016/01/jbermudez011916/.

[101] 안석, 하종훈 [Ahn Suk and Ha Jong Hoon], 비행거리 280-400 여 km… 생화학무기·신경가스 살포 가능 [Flight Range of 280-400 km … Able to Spray Biochemical Weapons and Nerve Gas], Seoul Shinmun, May 08, 2014, https://www.seoul.co.kr/news/newsView.php?id=20140509002001.

[102] 윤상호, 조숭호 [Yoon Sang Ho and Jo Soong Ho], "메모리칩에 입력된 비행경로와 사진찍은 곳 완벽 일치 [Flight path entered in memory chip perfectly matches the photographed location]," May 09, 2014, http://www.donga.com/news/article/all/20140509/63343715/1

[103] 안석, 하종훈 [Ahn Suk and Ha Jong Hoon], 비행거리 280-400 여 km… 생화학무기·신경가스 살포 가능 [Flight Range of 280-400 km … Able to Spray Biochemical Weapons and Nerve Gas], Seoul Shinmun, May 08, 2014, https://www.seoul.co.kr/news/newsView.php?id=20140509002001.

[104] "N. Korea unveils 'satellite photos' of THAAD in S. Korea," Yonhap News Agency, May 10, 2017, https://m-en.yna.co.kr/view/AEN20170510009000315.

[105] "북한 무인기 조사결과가 나왔다. 3년 전보다 훨씬 성능이 좋아졌다 [Study of North Korean UAVs released. Their performance is much better than three years ago]," Huffington Post Korea, June 21, 2017, https://www.huffingtonpost.kr/2017/06/21/story_n_17235866.html.

[106] "北집단체조에 '드론 공연' 등장…최신기술로 남북정상회담 강조 [Drone Performance Appears in North Korean Mass Games… Emphasize Inter-Korean Summit with the Latest Technology]," September 10, 2018, https://www.yna.co.kr/view/AKR20180910041200009

[107] 류준영 [Ryu Joon Young], "드론 전문가가 본 北드론쇼…선진국과 견줄 수준 [North Korean drone show comparable to that of developed countries according to drone experts]," 머니투데이 [Money Today], September 20, 2018, https://news.mt.co.kr/mtview.php?no=2018092014573537444.

North Korea's developing technological infrastructure supports emerging capabilities across the spectrum of conflict.

Cyber

In recent years, North Korea's sophisticated cyberspace capabilities have gained international attention after a series of high-profile cyberattacks, including but not limited to a massive hack of Sony Pictures, an $81 million heist from Bangladesh Bank, and the globally disruptive WannaCry 2.0 ransomware campaign.[108] In January 2019, the Office of the Director of National Intelligence described North Korea as a "significant cyber threat," specifically in hacks against financial institutions, cyberespionage, and generally disruptive attacks, and in April 2020, the U.S. Departments of State, Treasury, Homeland Security, and Justice issued a joint advisory on North Korea's threats in cyber space against financial institutions and critical infrastructure.[109] While North Korea's military and intelligence apparatus engages in malicious cyber activities for revenue generation, reconnassaince, and disruption, the UN Panel of Experts indicates that North Korea's IT workers and cyber units are operationally separated in order to avoid drawing attention to overseas IT workers, who constitute an important revenue stream for the Kim regime amidst broad multilateral sanctions.[110]

The RGB reportedly controls nearly all of North Korea's malicious cyber actors, including but not necessarily limited to the Kimsuky Group, the Lazarus Group (aka Guardians of Peace, Hidden Cobra, Whois Team, and Zinc), and its subgroups Bluenoroff (aka APT38 and Stardus Chollima) and Andariel (aka Velvet Chollima) with both cyberespionage and revenue-generation missions.[111] Historically, North Korea has dispatched its cyber units overseas to countries with better internet infrastructure, and since 2017, reports have allegedly identified malicious North Korea-linked cyber activity emanating from India, Malaysia, New Zealand, Nepal, Kenya, Mozambique, Indonesia, Thailand, and Bangladesh.[112] [113] [114] However, evidence suggests that as North Korea continues to develop its domestic internet infrastructure, its cyber units will begin to conduct more operations from territorial locations. Between 2017 and 2020, the volume of North Korean internet activity reportedly increased by 300%

---

[108] "Guidance on North Korean Cyber Threat," Department of State, Department of the Treasury, Department of Defense, and the Federal Bureau of Investigation, April 15, 2020, https://www.us-cert.gov/sites/default/files/2020-04/DPRK_Cyber_Threat_Advisory_04152020_S508C.pdf.

[109] "Guidance on North Korean Cyber Threat," Department of State, Department of the Treasury, Department of Defense, and the Federal Bureau of Investigation, April 15, 2020, https://www.us-cert.gov/sites/default/files/2020-04/DPRK_Cyber_Threat_Advisory_04152020_S508C.pdf.

[110] See page 157 of United Nations, Security Council, *Report of the Panel of Experts established pursuant to resolution 1874 (2009),* S/2020/151, March 2, 2020, accessed Spring 2020. https://undocs.org/S/2020/151.

[111] See page 50 footnote 148 of United Nations, Security Council, *Report of the Panel of Experts established pursuant to resolution 1874 (2009),* S/2020/151, March 2, 2020, accessed Spring 2020. https://undocs.org/S/2020/151.

[112] Will Ripley, "North Korean defector: 'Bureau 121' hackers operating in China," CNN, January 7, 2015, https://www.cnn.com/2015/01/06/asia/north-korea-hackers-shenyang/index.html.

[113] Park Jin-Hyok, the first individual North Korean hacker charged by the Federal Bureau of Investigation in 2018, "conducted legitimate IT work under the front company 'Chosun Expo' or the Korean Expo Joint Venture in addition to activities conducted on behalf of North Korea's Reconnaissance General Bureau." For more information, see "Park Jin Hyok," FBI, accessed Fall 2019, https://www.fbi.gov/wanted/cyber/park-jin-hyok.

[114] The study in question observed Internet activity between April and July 2017. "North Korea's Ruling Elite Are Not Isolated," Insikt Group, Recorded Future, July 25, 2017, https://www.recordedfuture.com/north-korea-Internet-activity/. The same researcher applied the same activity heuristic to similar data from December 2017 to March 2018 and found that all the same countries exhibited the same features except for Malaysia and New Zealand, which no longer fit the model. Thailand and Bangladesh were identified only in the second study. See Priscilla Moriuchi, "North Korea's Ruling Elite Adapt Internet Behavior to Foreign Scrutiny," Insikt Group, Recorded Future, April 25, 2018, https://www.recordedfuture.com/north-korea-Internet-behavior/.

due primarily to expanded bandwidth from TransTelekom's new fiber optic cable, and in March 2020, the UN Panel of Experts reported that almost all malicious cyberattacks now emanate from territorial North Korea.[115]

While estimates vary on the number of cyber operatives in North Korea, several reports in the United States and South Korea have presumed the number to be around 6,000.[116] [117] [118] [119] Some reports have indicated that gifted students are trained in intensive computer science training at Pyongyang's elite Keumsung 1 and 2 Middle Schools before undertaking further study at Mirim College or Moranbong University.[120] [121] [122] Other top universities such as Kim Il Sung University, Kim Chaek Industrial University, and Pyongyang Computer Technology University are also known to have rigorous curricula in computer science and related fields.[123] [124] Top graduates reportedly undergo special training in the 414 Liaison Office (414 연락소) and 258 Research Center (258 연구소).[125] Those who complete such special training are believed to be placed in RGB-operated units, where they are presumed to receive further practical training on South Korean targets.[126]

---

[115] See page 157 of United Nations, Security Council, *Report of the Panel of Experts established pursuant to resolution 1874 (2009),* S/2020/151, March 2, 2020, accessed Spring 2020. https://undocs.org/S/2020/151.

[116] "North Korean Cyber Capabilities: In Brief," Congressional Research Service, R44912 Version 3, August 3, 2017, https://crsreports.congress.gov/product/pdf/R/R44912.

[117] "보도자료: 국방비, 대한민국의 평화와 국민 행복을 지치는 소중한 투자 [Press Release: Defense spending, a valuable investment for the peace and happiness of the Republic of Korea]," 국방부 [Ministry of National Defense], June 13, 2016, http://www.korea.kr/common/download.do?fileId=184273134&tblKey=GMN.

[118] 한상미 [Han Sang Mi], "북한, 과학 영재 50-60 명씩 유학 보내 사이버 요원 양성 [North Korea sends 50-60 science gifted students to study abroad to train as cyber agents]," VOA, June 14, 2016, https://www.voakorea.com/a/3375411.html.

[119] A 2015 report from the Center for Naval Analyses estimated that North Korea has between 3,000 and 6,000 hackers between the RGB and the KPA's General Staff. See Ken Gause, "North Korea's Provocation and Escalation Calculus: Dealing with the Kim Jong-un Regime," Center for Naval Analyses, August 2015.

[120] 한상미 [Han Sang Mi], "북한, 과학 영재 50-60 명씩 유학 보내 사이버 요원 양성 [North Korea sends 50-60 science gifted students to study abroad to train as cyber agents]," VOA, June 14, 2016, https://www.voakorea.com/a/3375411.html.

[121] Joseph S. Bermudez Jr. traced the direct recruitment of high school graduates to 1986, which the MPAF reorganized the Mirim Academy in Pyongyang into the Mirim College and expanded the curriculum to include two-, four-, and five-year courses of study. For more information, see page 240 of Joseph S. Bermudez Jr., "SIGINT, EW and EIW in the Korean People's Army: An Overview of Development and Organization," *Bytes and Bullets in Korea,* ed. Alexandre Y. Mansourov (Honolulu: Asia-Pacific Center for Security Studies, 2005), 260-261. https://apps.dtic.mil/dtic/tr/fulltext/u2/1032407.pdf.

[122] Jong-Kap Baek. Implementation of cyberwarfare response systems through analysis of the cybersecurity situation of various countries in the world (각국의 사이버테러 대응실태 분석을 통한 대응체계 구축방안). Yongin University. February 2017.

[123] 유진평, 민석기, 최광, 장재혁 [Yoo Jin Pyong, Min Seok Gi, Choi Gwang, Jang Jae Hyuk], "국정원, 北정찰국 110 호 연구소 배후 지목 [NIS points to RGB as being behind 110 Research Center," https://www.mk.co.kr/news/special-edition/view/2009/07/378227/.

[124] 강진규 [Kang Jin Gyu], "평양콤퓨터기술대, 프로그램공학부를 지능정보공학부로 전환 [Pyongyang Computer Technology University converts Program Engineering Department to Intelligence Information Engineering Department]," June 23, 2019, https://www.nkeconomy.com/news/articleView.html?idxno=1570

[125] 백종갑 [Baek Jong Kap], "각국의 사이버테러 대응실태 분석을 통한 대응체계 구축방안 [Implementation of cyberwarfare response systems through analysis of the cybersecurity situation of various countries in the world], (2017). Yongin University.

[126] Ibid.

Cyberattacks publicly attributed to North Korea have used ransomware, malware, spear phishing campaigns, and distributed denial-of-service attacks, among other methods.[127] [128] North Korean hackers have targeted government institutions, nuclear power plants, defense contractors, research organizations, cryptocurrency exchanges, banks, ATMs, and media companies in attacks noted for their scale and sophistication.[129] [130] [131] American cybersecurity firm CrowdStrike assesses the speed of the North Korean hackers to be second only to Russian intrusion groups and superior to China's cyber units.[132]

Artificial Intelligence

North Korea produces automated video processing and data integration tools that support its domestic surveillance program and military. In November 2019, Arirang-Meari, a North Korean news outlet, published at least three articles about facial recognition technologies engineered at Kim Il Sung University, including applications that "use artificial intelligence technology to comprehensively detect and confirm surveillance objects on a national scale."[133] In January 2020, the same website described a biometric technology product that allegedly uses deep neural network technology for facial recognition products.[134] NK Economy, a specialist news outlet based in Seoul, South Korea, reported that North Korea had developed a video surveillance system capable of automated object detection and real-time movement that could be integrated with other databases to "determine abnormalities on moving objects, generate corresponding alarms, and store abnormal events and moving images in a database."[135]

---

[127] For a sample of code used in DPRK-affiliated cyber-attacks, see "North Korean Malicious Cyber Activity," Cybersecurity and Infrastructure Security Agency, Department of Homeland Security, accessed Fall 2019 and Spring 2020, https://www.us-cert.gov/HIDDEN-COBRA-North-Korean-Malicious-Cyber-Activity.

[128] 임종인 [Jong-In Lim]. 북한의 사이버전력 현황과 한국의 국가적 대응전략 [North Korea's Cyber War Capability and South Korea's National Counterstrategy]," *국방정책연구* [*The Quarterly Journal of Defense Policy Studies*] 29-4, 143, 한국국방연구원 [Korea Institute of Defense Analyses] (2013).

[129] Emma Chanlett-Avery et al. "North Korean Cyber Capabilities," *Congressional Research Service,* August 3, 2017, https://fas.org/sgp/crs/row/R44912.pdf.

[130] For example, in September 2018, the Department of Justice filed a criminal complaint indicating North Korea-linked hackers had launched unsuccessful spear phishing campaigns against Lockheed Martin in emails that referenced the THAAD. See Office of Public Affairs, "North Korean Regime-Backed Programmer Charged With Conspiracy to Conduct Multiple Cyber Attacks and Intrusions," Department of Justice, September 6, 2018, https://www.justice.gov/opa/pr/north-korean-regime-backed-programmer-charged-conspiracy-conduct-multiple-cyber-attacks-and.

[131] For example, some believe that North Korean hackers may have breached the administrative network at Kudankulam Nuclear Power Plant in Tamil Nadu, India as recently as September 2019. See Debak Das, "An Indian nuclear power plant suffered a cyberattack. Here's what you need to know." *The Washington Post,* November 4, 2019, https://www.washingtonpost.com/politics/2019/11/04/an-indian-nuclear-power-plant-suffered-cyberattack-heres-what-you-need-know/.

[132] Crystal Tai, "North Korean cyberwarfare: as big a threat as its nuclear weapons?" *South China Morning Post,* February 25, 2019, https://www.scmp.com/week-asia/geopolitics/article/2187363/north-korean-cyberwarfare-big-threat-its-nuclear-weapons.

[133] 배다연 [Bae Da Yeon], "대자료기술이 도입된 <내 나라> 홈페지 통합검색체계와 동영상감시체계 사용자들속에서 인기 [Nae Nara [My Country] homepage popular for its integrated search system and video surveillance system with big data technology]," 아리랑통신[Arirang News], 메아리[Meari], November 7, 2019, http://www.arirangmeari.com/index.php?t=news&no=10928.

[134] 김다현 [Kim Da Hyun], "심층신경망기술을 도입한 얼굴인식출입관리기 개발 [Development of face recognition access control system using deep neural network technology]," 아리랑통신[Arirang News], 메아리[Meari], January 05, 2020, http://www.arirangmeari.com/index.php?t=news&cg=1&no=11654.

[135] 강진규 [Kang Jin Gyu], "북한 모란봉기술협력교류사, 지능감시시스템 개발 [North Korea Moranbong Technology Cooperative Exchange develops intelligence monitoring system]," January 16, 2020, http://www.nkeconomy.com/news/articleView.html?idxno=2525.

While few technical experts have evaluated North Korea's image and video processing tools, evidence suggests that North Korea's software may be considered advanced by international standards.[136] In a 2018 report, the Center for Advanced Defense Studies (C4ADS), a nonprofit based in Washington DC, showed that North Korea-origin facial recognition technology placed second in the 2015 Intel® RealSense™ App Challenge in the Law Enforcement Computer Vision category via inadvertent submission by an Australian organization.[137] The Australian company unwittingly purchased the technology from RGB-affiliated front companies in Vietnam and reportedly deployed it in "an integrated facial recognition and Automatic Number Plate Recognition (ANPR) system [supplied] to law enforcement."[138] The success of North Korea-origin technology in international software competitions underscores that North Korea possesses the engineering expertise to produce operational artificial intelligence applications that can support its C4ISR mission.

Some evidence also suggests that North Korea has deployed artificial intelligence applications to improve the speed and accuracy of its air defense systems.[139] While the full extent to which North Korea has incorporated artificial intelligence into its military systems is difficult to assess, the technical limitations of North Korea's aging military equipment may create incentives to improve capabilities through advanced computing applications.

Electronic Warfare

North Korea has developed various EW equipment including GPS jamming for anti-aircraft defense purposes, which it has deployed against civilian targets in South Korea.[140] Since 2010, media reports have detailed incidents of alleged North Korean GPS jamming and spoofing targeted primarily at civilian South Korean assets.[141] According to the South Korean National Assembly's Science, Technology, Broadcasting and Communications Committee, four GPS jamming and spoofing attacks tied to North Korea occurred between 2010 to 2016 that affected a total of 2,229 base stations, 2,143 aircraft, and 980 vessels.[142] In 2016, South Korea reported to the United Nations Security Council that North Korea was jamming GPS signals across the border, and that these

---

[136] For analysis on how North Korea's commercial information technology sector has operated overseas for decades, see Andrea Berger, Cameron Trainer, Shea Cotton, and Catherine Dill, "OP#36: The Shadow Sector: North Korea's Information Technology Networks," James Martin Center for Nonproliferation Studies, Middlebury Institute of International Studies at Monterey, May 7, 2018, https://www.nonproliferation.org/op36-the-shadow-sector-north-koreas-information-technology-networks/.

[137] Jason Arterburn, "Dispatched: Mapping Overseas Forced Labor in North Korea's Proliferation Finance System," C4ADS, 2018, https://static1.squarespace.com/static/566ef8b4d8af107232d5358a/t/5bfc1b8ab8a045b4c0408779/1543248819621/Dispatched.pdf.

[138] For the archived Intel RealSense App challenge page, see Travis Reddy, "Law Enforcement Computer Version (Facial/ANPR/Vehicle Tracking)," Intel Software, Accessed Fall 2018, https://perma.cc/C3LB-7Q57. To understand the means by which RGB-affiliated companies sold the technology to the Australian company, see ibid p. 43-48.

[139] See Terence Roehrig, "The abilities – and limits – of North Korean early warning," Bulletin of the Atomic Scientists, November 27, 2017, https://thebulletin.org/2017/11/the-abilities-and-limits-of-north-korean-early-warning/ and *The conventional military balance on the Korean Peninsula*, The International Institute for Strategic Studies. (2018). https://www.iiss.org/-/media/images/comment/military-balance-blog/2018/june/the-conventional-military-balance-on-the-korean-peninsula.ashx?la=en&hash=C51D23B426579E41B43CF30A0D8969328FE57803

[140] "2018 국방백서 [2018 Defense White Paper]," 대한민국 국방부 [Republic of Korea Ministry of National Defense] (2018), http://www.mnd.go.kr/user/mnd/upload/pblictn/PBLICTNEBOOK_201901160236460390.pdf.

[141] North Korea has engaged in GPS jamming and spoofing activities since the Korean War. For a summary of more recent jamming incidents, see "Space Threat 2018: North Korea Assessment," Aerospace, CSIS, 2018, https://aerospace.csis.org/space-threat-2018-north-korea/.

[142] 최민지 [Choi Min Ji], "17 배나 증가한 교란영향, 북한 GPS 전파교란 대응체계 시급 [Disruption effects increase 17-fold, response system to North Korean GPS jamming system urgently needed]," www.ddaily.co.kr/news/article/?no=160576

jamming events originated in Pyongyang, Kaesong, Haeju, Yonan, and Mount Kumgang.[143] North Korea received a formal warning from the International Civil Aviation Organization but faced no other legal repercussions.[144]

The South Korean Defense Ministry has stated that "a regiment-sized electronic warfare unit near the North Korean capital Pyongyang, and battalion-sized units closer to the inter-Korean border" are responsible for North Korea's GPS jamming attacks, which use "downlink jamming systems" with an "effective radius of 50 to 100 kilometers" that are "mounted on mobile platforms," "operated intermittently," and therefore "difficult to locate and neutralize in a conflict."[145] North Korea reportedly obtained hardware for GPS jamming from Russia, which has developed extensive capability and applied operational experience during peacetime and conflict.[146] [147] Most recently, in March 2019, the UN Panel of Experts observed that North Korea has deployed GPS spoofing systems on its merchant fleet to obfuscate vessel identity and location by allowing vessels to adopt the identities of other ships or appear in multiple locations at the same time.[148]

Anti-Satellite

The Defense Intelligence Agency notes that North Korea possess both kinetic and non-kinetic counterspace capabilities including GPS and satellite communication jamming.[149] While North Korea possesses ballistic missiles and space launch vehicles that could, in theory, destroy adversary satellites during conflict, North Korea is not known to possess the onboard sensors or guidance systems that would be required to maintain a kinetic anti-satellite capability.[150]

Quantum Communications

Through public statements and published academic research with foreign universities, North Korea's leading universities have signaled an interest in quantum communications systems that, if developed, would degrade adversary reconnaissance and surveillance capabilities. As recently as April 2020, Kim Nam Chol, the Head of the Department of Physics at Kim Il Sung University, described the development of quantum information technology as "an important strategic task" for the country in Uriminzokkiri, a state-controlled website that provides

---

[143] Michelle Nichols, "South Korea tells U.N. that North Korea GPS jamming threatens boats, planes," Reuters, April 11, 2016, https://www.reuters.com/article/us-northkorea-southkorea-gps/south-korea-tells-u-n-that-north-korea-gps-jamming-threatens-boats-planes-idUSKCN0X81SN.

[144] John G. Grisafi, "Aviation agency to warn North Korea on GPS jamming," NK News, June 24, 2016, https://www.nknews.org/2016/06/aviation-agency-to-warn-north-korea-on-gps-jamming/.

[145] Todd Harrison, Kaitlyn Johnson, and Thomas G. Roberts, "Space Threat Assessment 2018," The CSIS Aerospace Security Project, April 2018, https://aerospace.csis.org/wp-content/uploads/2018/04/Harrison_SpaceThreatAssessment_FULL_WEB.pdf#page=25.

[146] Ibid.

[147] For more on Russia's use of GPS jamming and spoofing technology, see "Above Us Only Stars: Exposing GPS Spoofing in Russia and Syria," C4ADS, 2019, https://static1.squarespace.com/static/566ef8b4d8af107232d5358a/t/5c99488beb39314c45e782da/1553549492554/Above+Us+Only+Stars.pdf.

[148] United Nations, Security Council, *Report of the Panel of Experts established pursuant to resolution 1974 (2009),* S/2019/171, March 5, 2019, accessed Fall 2019. https://undocs.org/S/2019/171.

[149] "Challenges to Security in Space," Defense Intelligence Agency, (2019), https://www.dia.mil/Portals/27/Documents/News/Military%20Power%20Publications/Space_Threat_V14_020119_sm.pdf.

[150] "Space Threat 2018: North Korea Assessment," Aerospace, CSIS, 2018, https://aerospace.csis.org/space-threat-2018-north-korea/.

news from North Korea's Central News Agency.[151] North Korean propaganda sites like Sogwang have similarly described quantum technologies as a means to secure North Korea's communications system and praised Kim Il Sung University's research in developing the capability.[152] If successfully developed, quantum communications technology could prevent the United States and its allies from intercepting or decrypting North Korea communications.[153] While North Korean state-media claims that Kim Il Sung University researchers have successfully developed the technology, the author found no additional evidence to support the claim.

Battlefield C4ISR Systems: The Glocom Case Study

Public reporting contains limited information on the C4ISR systems that North Korea would deploy in battle across its conventional and nuclear forces, which has constrained analysis on technological risk factors for crisis stability on the Korean Peninsula. This section describes a non-exhaustive sample of battlefield systems from the technical brochures on the arms dealer Glocom, which the UN Panel of Experts identified as an RGB operation after Egyptian authorities interdicted one of its shipments bound from North Korea to Eritrea in August 2017.[154] [155] [156] On its website, Glocom openly advertises battlefield equipment for sale on international markets, which may provide partial insights into how North Korea's intelligence apparatus conceptualizes the role of emerging technologies in developing a conflict C4ISR capability.[157]

---

[151] "주목을 끄는 량자정보기술 [Eye-catching quantum information technology]," 우리민족끼리 [uriminzokkiri], April 19, 2020, http://www.uriminzokkiri.com/index.php?ptype=csense&mtype=view&no=1190815.

[152] "해킹방지를 위한 첨단통신기술개발 [Development of advanced communication technology to prevent hacking]," 서광 [Sogwang], http://www.sogwang.com/kp/post/583aa3916a1ef805ec12bbbf.

[153] In December 2018, the Government Accountability Office conducted a study to identify long-range emerging threats to the United States as determined by the Departments of Defense, State, and Homeland Security and the Office of the Director of National Intelligence. The report indicates that "Quantum communications could enable adversaries to develop secure communications that U.S. personnel would not be able to intercept or decrypt. Quantum computing may allow adversaries to decrypt information, which could enable them to target U.S. personnel and military operations." For more information, see "National Security: Long-Range Emerging Threats Facing the United States As Identified by Federal Agencies," U.S. Government Accountability Office, December 2018, https://www.gao.gov/assets/700/695981.pdf.

[154] James Pearson and Rozanna Latiff, "North Korea spy agency runs arms operation out of Malaysia, U.N. says," Reuters, February 26, 2017, https://uk.reuters.com/article/uk-northkorea-malaysia-arms-insight-idUKKBN1650YG.

[155] United Nations, Security Council, *Report of the Panel of Experts established pursuant to resolution 1874 (2009),* S/2017/150, February 27, 2018, accessed Fall 2019, https://www.securitycouncilreport.org/atf/cf/%7B65BFCF9B-6D27-4E9C-8CD3-CF6E4FF96FF9%7D/s_2017_150.pdf.

[156] Glocom, 2018, accessed Spring 2019, http://glocom-corp.com/2018/index.php and Glocom, 2017, accessed Spring 2019, http://glocom-corp.com/2017/.

[157] Readers should be advised that preliminary research did not find additional evidence to corroborate that the equipment exists or that it would be operational in conflict.

Command & Control Systems

The Glocom GS-3100 Elephant Box is a computerized command, control, communications, and intelligence equipment package of Glocom's various hardware and software products. The Elephant Box is intended to provide a scalable, collaborative operational planning capability for land forces that is interoperable between military and civilian systems through a web-based architecture with security and access controls. The platform allegedly integrates ground pictures, geospatial data, battle order information, and all source intelligence to support rapid decision-making. The Elephant Box also allegedly supports users on computers and mobile devices.

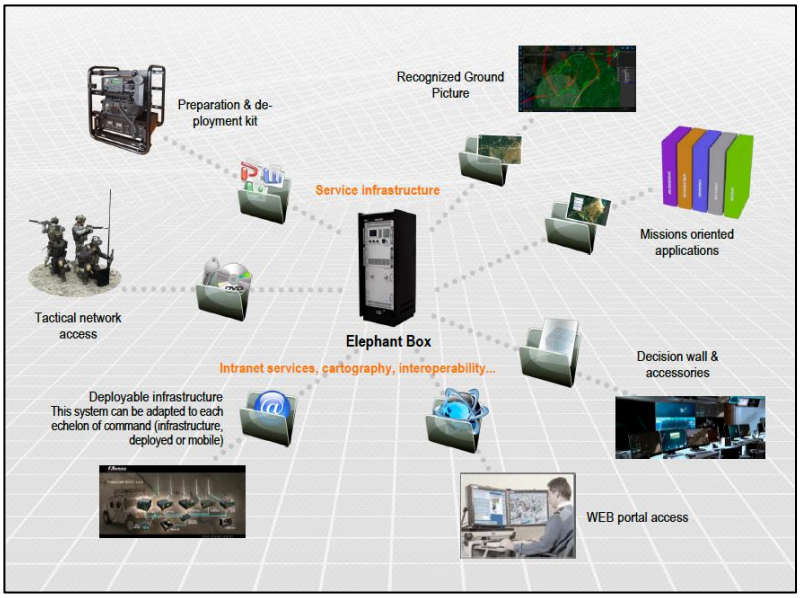

Figure 1: Product Brochure Screenshot for GS-3100

If deployed, the Elephant Box may support North Korea's military in monitoring battlefield operations from locations across the country where internet or intranet services were sufficient to maintain network connection, which rely primarily on North Korea's underground network of fiber optic cables. Product information does not provide sufficient technical detail to assess the system's data storage or integration capabilities, which would need to be substantial in order to manage, store, and integrate real-time video footage from troops or UAVs. Because the system purportedly uses a web-based architecture, the Elephant Box may face operational challenges if deployed on North Korea's limited internet infrastructure.

Battlefield Communications

The GS-2500 Universal Soldier Information System (USIS) is advertised as a system to improve a soldier's battlefield observation capability by facilitating communication with other units, mapping "blue force" units, displaying digital renderings of the battlefield, providing encrypted communications with other soldiers on the network, transmitting emergency warnings, monitoring heart rate, and tracking location. The system is designed to integrate with other Glocom C4ISR systems designed for aircraft, ground vehicles, and command centers. Other related systems allegedly provide operational planning tools based in geographic information systems software packages.

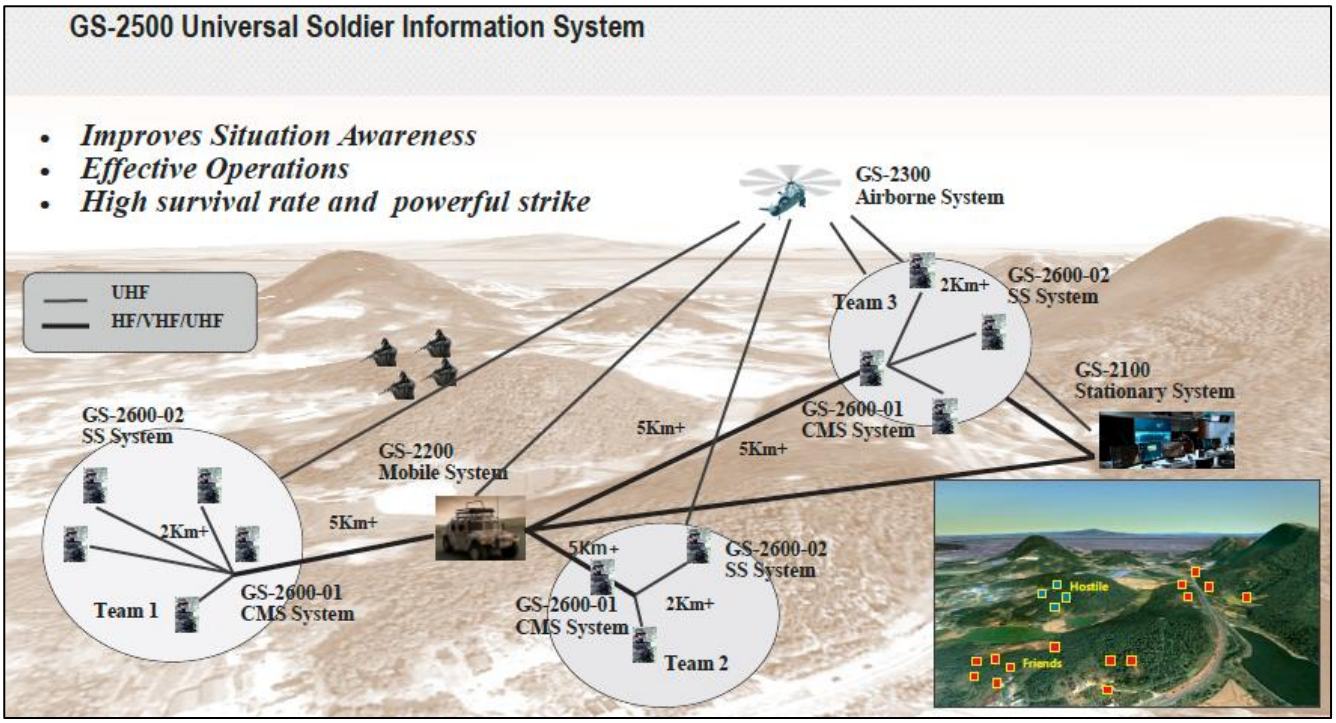

Figure 2: Product Brochure for the GS-2500

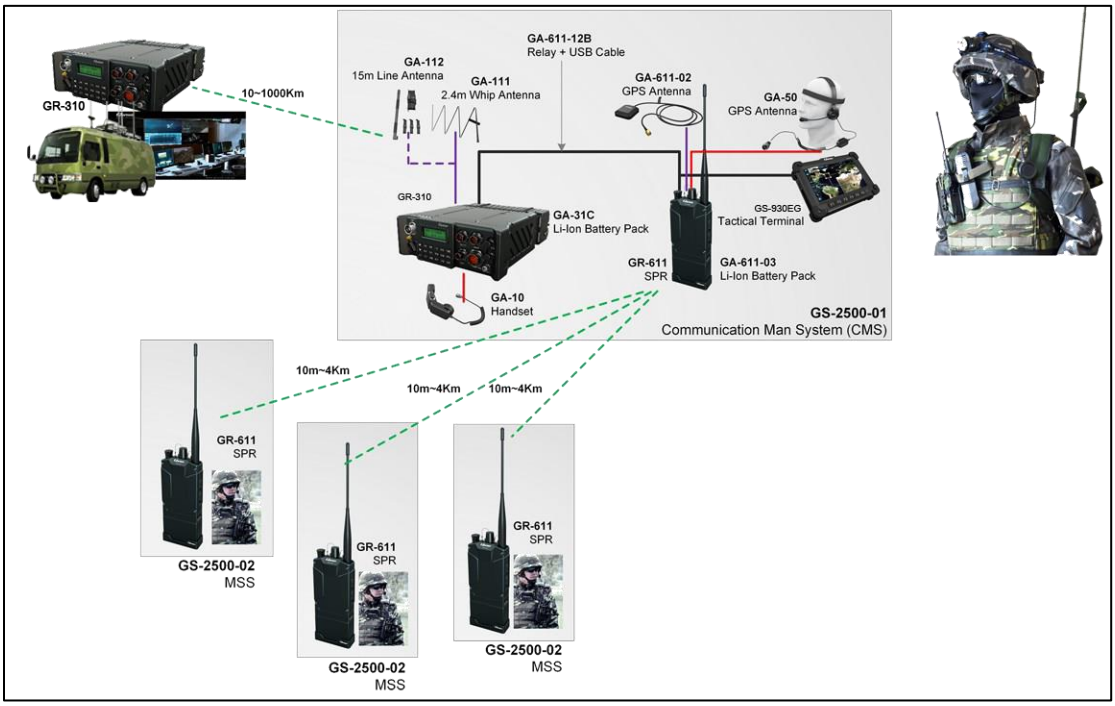

Figure 3: Product Brochure for the GS-2500

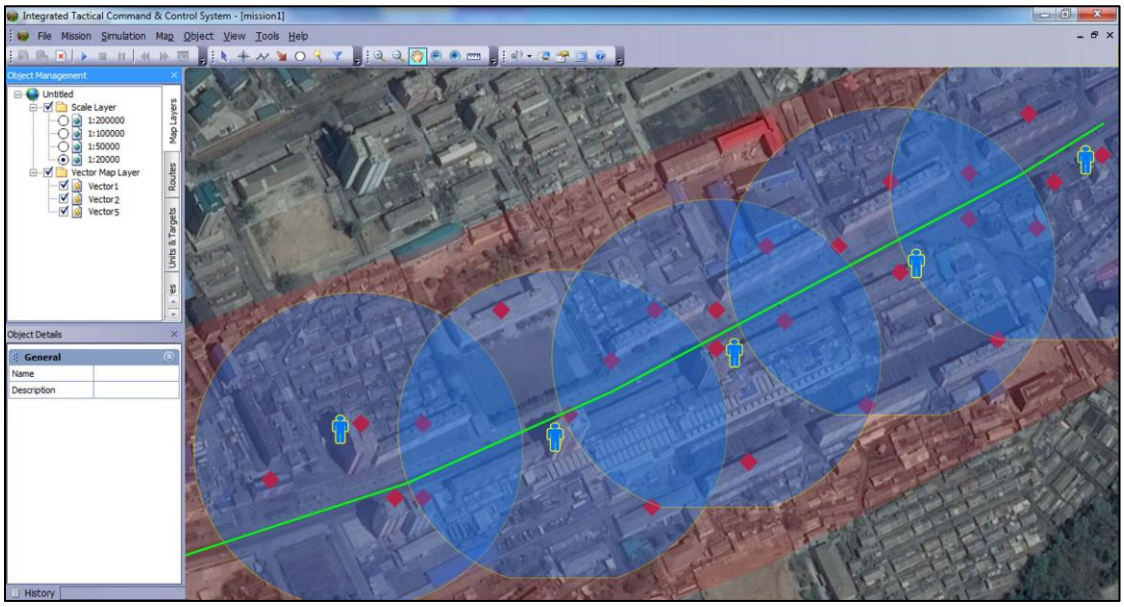

Figure 4: Product Brochure for GS-2700

Air Defense, Telemetry, & Datalink Systems

GS-2600-03 is an air defense command, control, and communication system built to provide real-time data exchange between radars, command post centers, launching stations, and missiles. The GS-2600-02 is advertised as a telemetry, tracking, and command & communication system designed to transmit data and information between aircraft, command centers, and launch centers, and is purportedly built with electronic counter-countermeasures (ECCM) capability. The system purportedly includes datalink transceivers, network controllers, and high capacity data radios. Product brochures do not explicitly mention artificial intelligence or other forms of automation, which North Korea has reportedly incorporated into some of its surveillance and air defense systems.

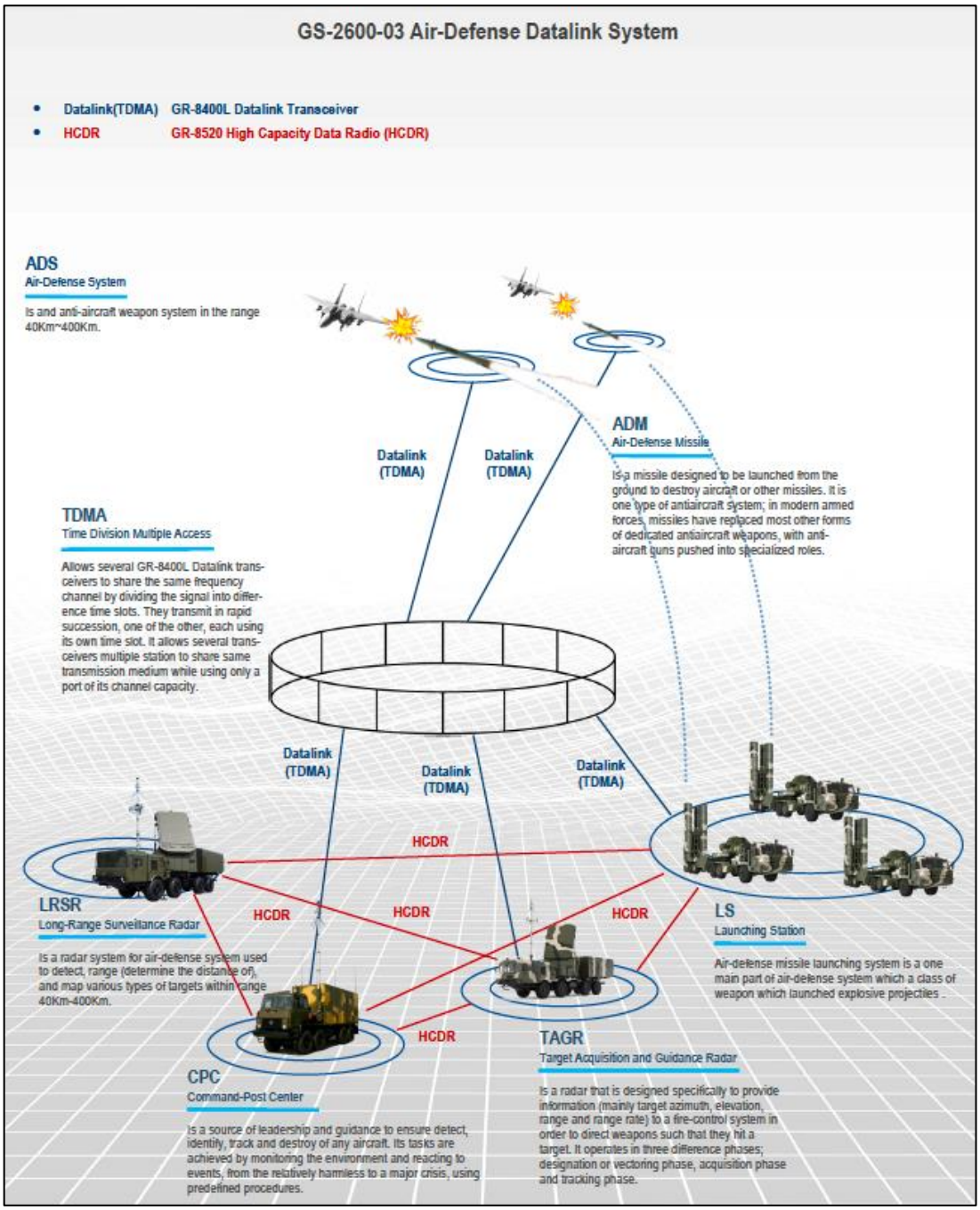

Figure 5: Product Brochure for GS-2600-03

Glocom also advertises telemetry systems for unmanned aerial and surface vehicles. The GS-2600-01 UAV/USV Video, Telemetry/Control System is advertised for coastal surveillance and special military operations. Glocom markets the GS-2600-01 system as one of the company's "main products" with "long history and experience." The system alleges to provide high quality real-time video communication for UAVs, USVs, missiles, remote sensors, and telemetry/remote control equipment. Like subsequent models, it also allegedly incorporates ECCM functionality for compatibility with electronic warfare.

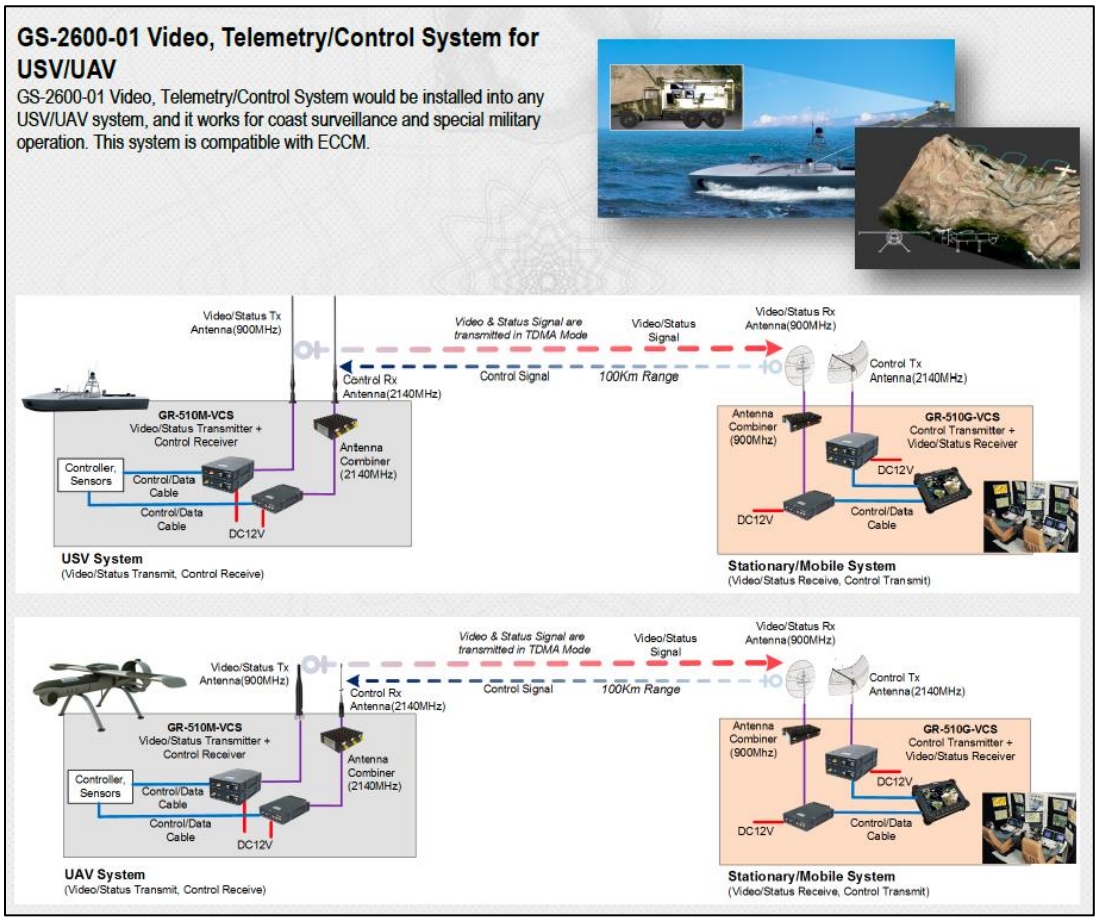

Figure 6: Product Brochure for GS-2600-01

If deployed, the GS-2600-01 could support an expanded reconnaissance and combat mission for North Korea's UAVs. Evidence suggest that North Korea uses rudimentary UAVs for basic reconnaissance missions in South Korea, which used basic digital cameras intended for personal use. If North Korea possesses UAV systems capable of more video transmission, it would represent an improved intelligence, surveillance, and reconnaissance capability that could be deployed both in peacetime and during conflict.

Ground-Based Surveillance

The GBSS-2017 Border Security System is a border surveillance and security system that can allegedly be loaded onto mobile vehicles for deployment either at fixed locations or in special areas of operation. The system allegedly integrates video, imagery, and signals data from unattached ground sensors, ground radars, video cameras, and infrared cameras; and supports communication via tactical radio nets, video radio/high capacity data radios, microwave radios, SATCOM systems, and mobile phones. The GBSS-2017 also appears to be able to link into fiber optic cables as a backbone for higher-volume data transmission to command center or other units.

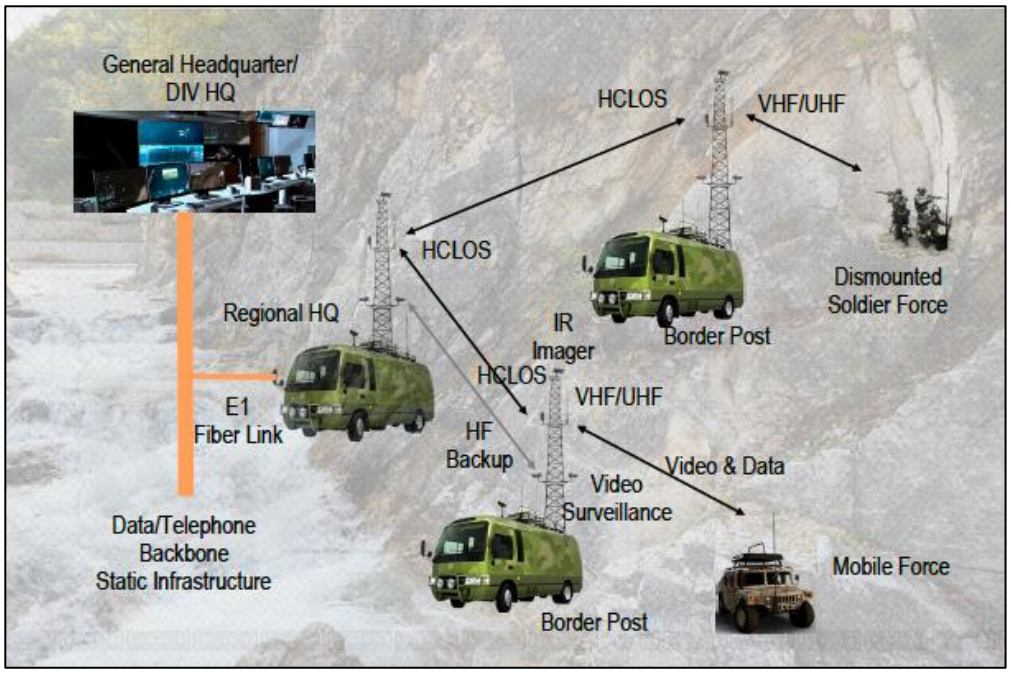

Figure 7: Product Brochure for GBSS-2017

If deployed, the GBSS-2017 may provide an alternative, more resilient system for command, control, and communications during conflict. The GBSS-2017 purports to use a range of communication systems that may provide redundancy during conflict, but because it allegedly uses fiber optic links to connect with command centers, it may be vulnerable to an attack on North Korea's core telecommunications infrastructure. While the system does not explicitly mention artificial intelligence applications, it describes capabilities for video processing and data integration in which North Korea has demonstrated expertise in other surveillance products like facial recognition, optical character recognition, object tracking, and automated alerting.[158]

Sea-Based Communication Systems

GS-2400 Shipborne Communication System is designed to support command and control between systems at sea, including submarines, and their counterparts on land and in air. Product advertisements state that the GS-2400 system supports position reporting, information sharing between radar and command & control systems, remote control access via local area networks, military operations planning, and mission control data management. The radio systems allegedly use a transmission frequency from 1.6MHz to 2.4GHz and have secure communications capabilities with electronic protective measures and integrated encryption. Glocom advertises the system with a flexible range of applications that support both local and remote operations for military vessels and USVs. If the GS-2400 could in fact support communication between terrestrial command centers, vessels, and submarines, it may support North Korea's ability to communicate with ballistic submarines during conflict.[159]

[158] For evidence of North Korea's domestically produced artificial intelligence systems, see the above section entitiled "Capabilities: Artificial Intelligence."
[159] For a discussion of command and control vulnerabilitiues related to North Korea's nuclear forces and sea-based systems, see Vipin Narang and Ankit Panda, "Command and Control in North Korea: What a Nuclear Launch Might Look Like," War on the Rocks, September 15, 2017, https://warontherocks.com/2017/09/command-and-control-in-north-korea-what-a-nuclear-launch-might-look-like/

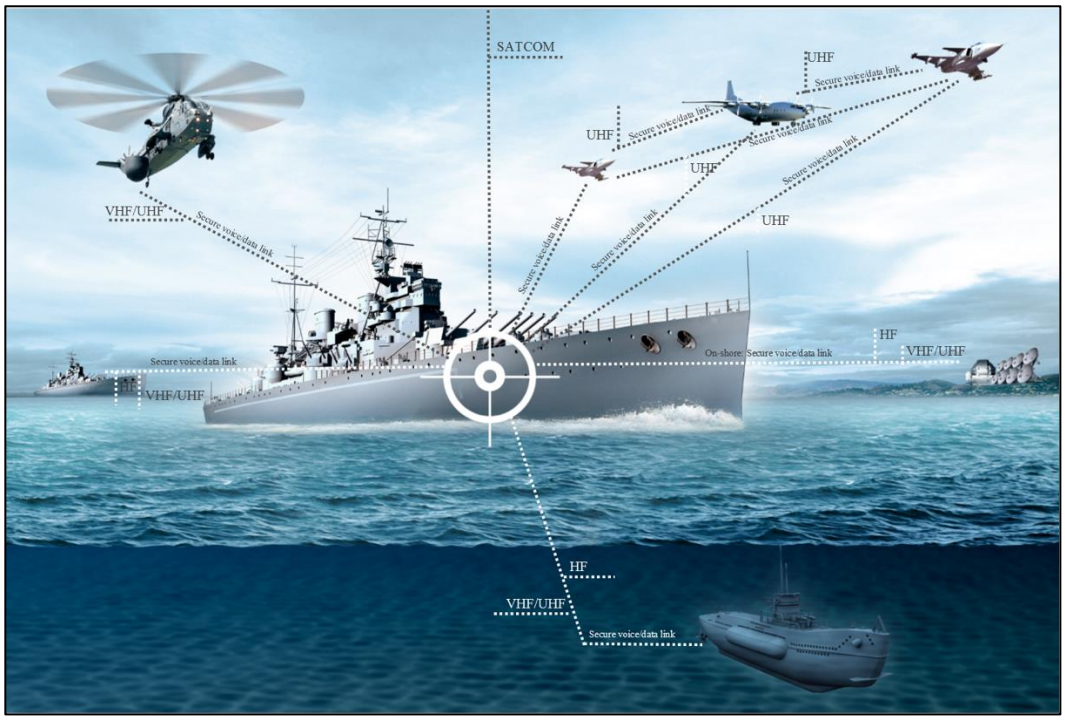

Figure 8: Product Brochure of GS-2400

Air-Based Communication Systems

GS-2300 Airborne C4ISR System is advertised as an integrated tactical command & control system that is compatible with various kinds of civilian and military aircraft. Marketing brochures indicate that GS-2300 radios use multiband, multimode, and multirole capabilities to allow one device to support a range of missions. The GS-2300 purportedly includes three subsystems: the GS-2300-01 Stationary System, the GS-2300-02 Mobile System, and the GS-2300-03 Airborne System. The GS-2300-01 is advertised as a stationary command & control center for air operations. The GS-2300-02 is advertised as a system for mobile vehicles to support air traffic control for military and civilian aircraft. The GS-2300-03 is advertised for aircraft and includes equipment for the cockpit, avionic bay, and aircraft body for high survival voice and data communication to command & control centers.

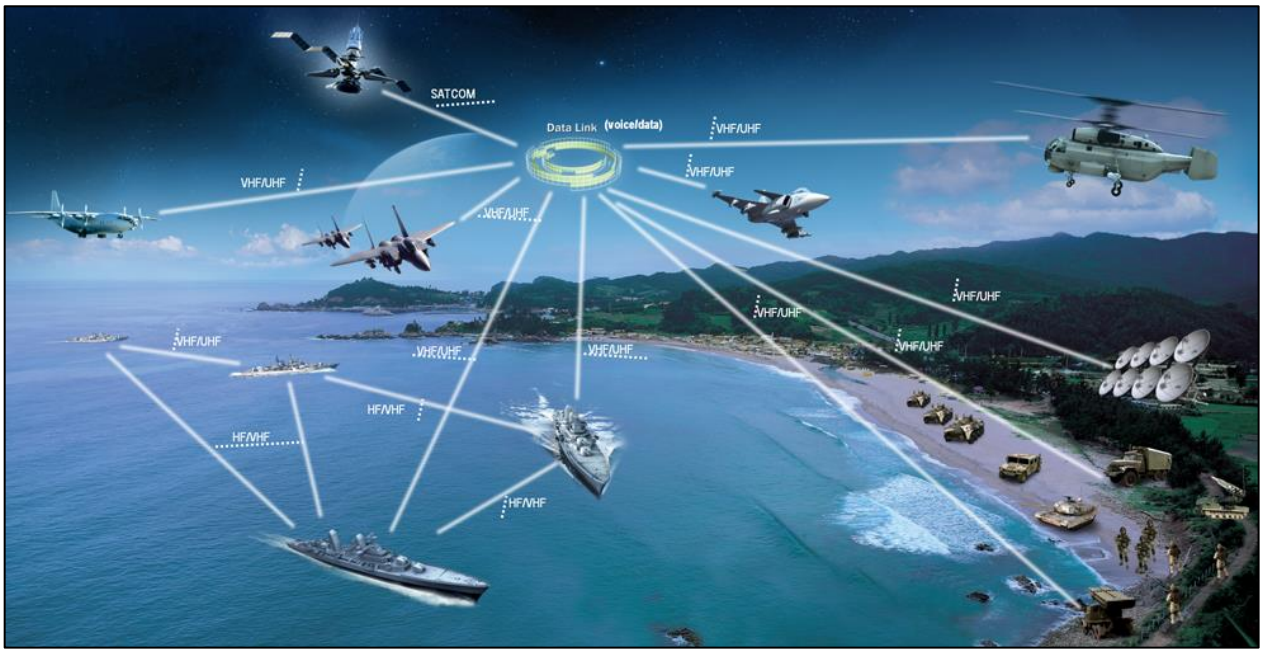

Figure 9: Product Brochure for GS-2300

While no public evidence can confirm that these systems exist or are operational, Glocom's product brochures provide evidence of how North Korea's intelligence and military apparatus conceptualizes battlefield systems integration for asymmetric engagements that use both conventional and unconventional forces. Future research may use satellite imagery, academic publications, news reporting, state media broadcasts, and other forms of publicly available information to determine if and how North Korea adopts similar technology systems into its military and intelligence apparatus.

Concluding Assessments

North Korea's developing strategic situational awareness capabilities incorporate technologies that could introduce new risks in a conflict or crisis on the Korean Peninsula. North Korea is rapidly developing its domestic telecommunications and internet infrastructure, where a lack of redundant systems and bandwidth constraints have historically degraded performance. While North Korea's infrastructure investments may improve connectivity between the organizations involved in North Korea's military and intelligence enterprise, evidence suggests that it may also create new pathways to escalation by enabling North Korea to engage in an expanding range of provocative attacks against adversary computer networks and communications systems, which has long formed a key component of its approach to asymmetric engagements.

North Korea's military relies heavily on old, foreign-origin equipment with serious technical and operational limitations, which may create incentives for North Korea to introduce artificial intelligence into weapons systems to improve capability. Over decades, North Korea has developed significant expertise in advanced computing through its information technology industry and military, and in recent years, its artificial intelligence programs have won international competitions for surveillance applications in law enforcement. While the full extent of North Korea's use of artificial intelligence in weapons systems is difficult to assess, some public reporting indicates that North Korea has already begun to incorporate automation into its air defense systems to improve speed and accuracy. As broad-based multilateral sanctions continue to limit North Korea's access to international commercial

systems, North Korea's military and intelligence services may face incentives to continue developing capabilities through advanced computing applications, for which North Korea has significant domestic technical expertise. For other key C4ISR systems like satellites, North Korea may continue to expand its capabilities through academic, technical, or military cooperation with states like China or Russia that have provided key equipment and training over decades and continue to do so today.

Since the Korean War, North Korea has developed a warfighting strategy that emphasizes asymmetric engagement through hybrid use of conventional and unconventional forces either to deter aggression or, if having failed to do so, to defeat adversaries quickly after an attack. While the public domain does contain some technical brochures that offer partial, unverified insights into North Korea's domestically produced battlefield C4ISR systems, it remains unclear whether North Korea possesses the systems required to manage the increased information complexity that those systems would introduce, or whether those systems are sufficient to provide reliable, resilient communication channels to its conventional and nuclear forces. North Korea has expanded its situational awareness capabilities through technologies that both facilitate provocation and increase the possibility of misperception, which could therefore introduce destabilizing risks in a conflict or crisis on the Korean Peninsula.

ABOUT CSIS

Established in Washington, D.C., over 50 years ago, the Center for Strategic and International Studies (CSIS) is a bipartisan, nonprofit policy research organization dedicated to providing strategic insights and policy solutions to help decision-makers chart a course toward a better world.

In late 2015, Thomas J. Pritzker was named chairman of the CSIS Board of Trustees. Mr. Pritzker succeeded former U.S. senator Sam Nunn (D-GA), who chaired the CSIS Board of Trustees from 1999 to 2015. CSIS is led by John J. Hamre, who has served as president and chief executive officer since 2000.

Founded in 1962 by David M. Abshire and Admiral Arleigh Burke, CSIS is one of the world's preeminent international policy in-stitutions focused on defense and security; regional study; and transnational challenges ranging from energy and trade to global development and economic integration. For eight consecutive years, CSIS has been named the world's number one think tank for defense and national security by the University of Pennsylvania's "Go To Think Tank Index."

The Center's over 220 full-time staff and large network of affiliated scholars conduct research and analysis and develop policy initiatives that look to the future and anticipate change. CSIS is regularly called upon by Congress, the executive branch, the media, and others to explain the day's events and offer bipartisan recommendations to improve U.S. strategy.

CSIS does not take specific policy positions; accordingly, all views expressed herein should be understood to be solely those of the author(s).