Communication Technologies for Engaging Citizens in North Korea: A Viability Assessment

---

Executive Summary

There is no current technology that allows a foreign organization to communicate two-way and securely with an ordinary North Korean citizen without exposing that citizen to serious risk. Every channel that exists today — including the smuggled Chinese cell phones that defector communities often rely on — places the person inside the country in jeopardy. The question is therefore not which technology is "safe," but which combination of tools, tradecraft, and partner networks minimizes risk to the user inside of North Korea while still enabling meaningful contact.

This report assesses technologies that would enable two-way communication: satellite phones (Thuraya, Iridium, and Inmarsat-based services, including the Garmin inReach line), smuggled Chinese cellular phones for use near the China border, mesh networking apps (Briar, Bridgefy), and low-earth-orbit (LEO) satellite internet (Starlink). It also compares these options with existing one-way communication options: shortwave and mediumwave radio, USB and SD card distribution, and steganographic communication disguised inside ordinary media. It examines all of these against North Korea's documented detection and surveillance capabilities, then ranks them by viability.

The abbreviated version of the ranking is that the smuggled Chinese cellular phone, brokered through established defector and Korean-Chinese broker networks at the China border, is currently the most practically functional two-way voice channel today, despite its severe risks. For asynchronous text rather than voice, a compact Iridium-based satellite messenger like the Garmin inReach Mini or Messenger is technically the most concealable two-way option, but it faces a hard legal barrier in that Iridium does not service North Korea due to United States embargo rules, and the device's radio signature is highly detectable by the same radio-wave surveillance infrastructure already used along the China-North Korea (Sino-Korean) border. Thuraya is geographically possible but is also a thoroughly compromised satellite network in terms of interception. Starlink is the most promising emerging option in principle but is not currently deployable inside North Korea in any meaningful scale, in contrast to Iran where at least 50,000 terminals have reportedly been smuggled in.[1] Mesh networking applications like

[1] Aisha Down, "An ecosystem of smuggled tech holds Iran's last link to the outside world," The Guardian, Jan. 13, 2026, https://www.theguardian.com/world/2026/jan/13/ecosystem-smuggled-tech-iran-last-link-outside-world-internet

Briar are interesting as a complement for in-country use but do not solve the cross-border problem and have recorded security issues.[2]

The most viable strategic posture is arguably a layered one: use existing broker-mediated Chinese cellular channels for two-way voice; continue radio, balloon, and USB distribution for one-way information flow inward; treat satellite devices as a special option for trained, high-risk operatives rather than ordinary citizens; and invest in research for LEO satellite internet as a potential future option, while pursuing policy changes that would make this viable on a large scale.

---

1. The Challenge of Two-Way Communication

Most successful interventions into North Korea's information environment over the past two decades have been one-way: radio broadcasts beamed in, USB sticks smuggled across the border, content burned to DVDs and SD cards. These work because the person inside North Korea is a passive receiver who does not have to emit any detectable signal. Thus, the risk falls on possession, not on transmission.

Two-way communication is fundamentally different. The moment a North Korean citizen transmits a signal, that emission is detectable in principle, and potentially in practice. North Korea's Ministry of State Security (MSS) Bureau 10 — also known as the State Information Bureau, which specializes in radio wave surveillance — has reportedly planted radio frequency detectors that can localize a phone signal within minutes and to within roughly five meters.[3]

---

2. Assessment of the Surveillance Environment

An evaluation of the threat is prudent for any viability assessment. The following capabilities are well-documented through defector testimony, NGO investigation, and academic research:

Radio frequency detection along the China border. High-performance radio-wave detectors have been installed and are regularly upgraded in border provinces including Yanggang, North

[2] A mesh networking application is software that allows devices to communicate directly with each other without relying on a traditional router or cellular tower.
[3] Kang Jae-Jun, "Border security supplies new phone detectors… '3 minutes, 5 meters,'" NK Insider, Apr. 9, 2025. https://www.nkinsider.org/border-security-supplies-new-phone-detectors-3-minutes-5-meters/

Hamgyong, North Pyongan, and Chagang. They are utilized for tracking frequencies emitted by unauthorized cellphones and other digital devices, and their gradual increase in strength over the years has caused the length of illegal calls made from inside the country to decrease over time.[4] In 2025, Radio Free Asia reported the distribution of new handheld portable detectors to officers in Uiju County in North Pyongan Province, deployed specifically to track Chinese mobile phone use.[5] Sources reported in NK Insider in 2025 that the latest detectors can identify a phone signal "within three minutes, to within five meters," after which mobile teams move in to apprehend the user. [6]

IMSI catchers (Stingrays) for cellular interception.[7] Amnesty International's 2016 Connection Denied report, based on interviews with seventeen defectors, described backpack-sized devices used in the border region that an independent analysis identified as sharing the same features as IMSI catchers, the same family of cell-site simulators also known as Stingrays.[8][9] These devices impersonate legitimate cell towers, attract the signals of nearby handsets, and steal identifying information (the IMSI and IMEI of every mobile device within range), including the content of calls and SMS, and devices' approximate location.[10] Their use against Chinese mobile networks at the border means that even when a North Korean evades the Koryolink domestic network by using a Chinese SIM card, they remain exposed.[11]

Mandatory device censorship and surveillance on domestic phones. The 2017 Compromising Connectivity by InterMedia documented that domestic North Korean smartphones running customized Android variants run signature-checking software that deletes unauthorized media files, take periodic forced screenshots that the user cannot delete and that are inspected later by inspectors, and apply cryptographic signing so that only state-approved files can be opened.[12][13]

---

[4] Kim Chae Hwan, "N. Korea replaces radio wave detectors on border with the latest models," Daily NK, Nov. 3, 2022. https://www.dailynk.com/english/north-korea-replaces-radio-wave-detectors-border-latest-models/
[5] Hyemin Son, "North Korea deploys handheld signal detectors to crack down on cross-border calls," Radio Free Asia, May 20, 2025. https://www.rfa.org/english/korea/2025/05/20/north-korea-phone-detectors/
[6] Kang Jae-Jun, "Border security supplies new phone detectors… '3 minutes, 5 meters,'" NK Insider, Apr. 9, 2025. https://www.nkinsider.org/border-security-supplies-new-phone-detectors-3-minutes-5-meters/
[7] IMSI stands for International Mobile Subscriber Identity, a surveillance tool that acts like a cell tower, connecting to mobile devices via a signal and harvesting their identifying data.
[8] "North Korea: Connection Denied: Restrictions on mobile phones and outside information in North Korea," Amnesty International, March 9, 2016, https://www.amnesty.org/en/documents/asa24/3373/2016/en/
[9] Ben Bryant, "North Korea Is Apparently Using Sophisticated Tech to Jail Citizens Contacting the Outside World," VICE News, March 9, 2016, https://www.vice.com/en/article/north-korea-is-apparently-using-modern-surveillance-to-jail-citizens-contacting-the-outside-world-1/
[10] Electronic Frontier Foundation, "Cell-Site Simulators / IMSI Catchers," Street Level Surveillance. https://sls.eff.org/technologies/cell-site-simulators-imsi-catchers
[11] Koryolink is North Korea's primary mobile telecommunications provider.
[12] Nat Kretchun et al., "Compromising Connectivity: Information Dynamics Between the State and Society in a Digitizing North Korea," InterMedia, p. 47, 2017. https://gwern.net/doc/sociology/technology/2017-kretchun.pdf
[13] "How Information and Technology are Changing North Korea" George W. Bush Presidential Center, April 3, 2017,

These systems make any communication app installed on a domestic phone effectively impossible to download or hide.

Satellite communications interception. Commercial systems sold by Indian and Israeli signals-intelligence vendors openly market interception of Thuraya-2, Thuraya-3, Iridium, and Inmarsat IsatPhone Pro signals, capturing voice, SMS, data, and call-related information including terminal location.[14] Whether North Korea has acquired such systems is not publicly confirmed, but the technology exists on the commercial market, and Pyongyang's network of state arms-trade entities like Hyoksin and Sinheung Trade Company make it reasonable to assume that the regime would be able to procure surveillance gear through similar channels.[15]

Jamming and electronic warfare. According to South Korean officials, North Korea allegedly operates Russian-made GPS jamming systems that have disrupted GPS signals across the border and into the South, including incidents that affected hundreds of South Korean fishing boats and airliners.[1617] In 2025, the International Civil Aviation Organization formally condemned both Russia and North Korea for GPS interference.[18] The same electronic warfare units that conduct jamming operations are responsible for spectrum monitoring.[19]

Legal escalation and collective punishment. Daily NK has documented amendments to Article 60 of the North Korean criminal code, which pertains to attempts to overthrow the state, that explicitly criminalize "illegal phone contact with foreigners, including South Koreans," and listening to foreign broadcasts.[20] Linking these to subversion of the state makes them prosecutable as treason. The North Korean principle of guilt-by-association means family members face punishment alongside the accused.[21]

---

https://www.bushcenter.org/publications/articles/2017/03/how-information-and-technology-are-changing-north-korea.html

[14] "Satellite Phone Monitoring | Thuraya | Iridium | Inmarsat," Shoghi Communications, https://www.shoghicom.com/products/intelligence-surveillance-reconnaissance/satellite-phone-gmpcs-monitoring

[15] "New Devices Catch Illicit Phone Calls," Daily NK, Nov. 12, 2014, https://www.dailynk.com/english/new-devices-catch-illicit-phone-ca/

[16] "Space Threat 2018: North Korea Assessment," Aerospace, April 12, 2018, https://aerospace.csis.org/space-threat-2018-north-korea/

[17] "N. Korea Now Jamming GPS Signals," VOA News, April 1, 2016, https://www.voanews.com/a/north-korea-now-jamming-gps-signals/3264272.html

[18] "ICAO condemns Russia and North Korea over GPS signal jamming," Aerotime, Oct. 6, 2025. https://www.aerotime.aero/articles/icao-condemns-russia-north-korea-gps-interference-2025

[19] "N. Korea readies deployment of new GPS jamming device," Daily NK, May, 1 2020, https://rntfnd.org/2020/05/01/n-korea-readies-deployment-of-new-gps-jamming-device-link-to-funeral-prep-daily-nk-ibt/

[20] Stephan Haggard, "Controlling the Border," Peterson Institute for International Economics, August 21, 2014, https://www.piie.com/blogs/north-korea-witness-transformation/controlling-border

[21] George W. Bush Presidential Center, "Han Nam-su: Three Generations of Punishment," 2016, https://www.bushcenter.org/freedom-collection/han-nam-su-three-generations-of-punishment

The practical assumption is that any radio frequency-emitting device used inside North Korea is operating in an actively monitored environment, and the operator must assume the worst case: that signals are being detected, that location can be triangulated, and that consequences include lengthy imprisonment, political prison camp internment for the user and their family, or execution.

---

3. The Established Baseline: Smuggled Chinese Cell Phones at the Border

An assessment of new technologies should be calibrated against what defector communities and NGOs are already doing successfully. A baseline to be considered is the smuggled Chinese cell phone, brokered through Korean-Chinese intermediaries.

The mechanics are straightforward; Chinese mobile carriers operate cell towers along the Yalu and Tumen rivers whose signal reaches several kilometers into North Korean territory. A North Korean in a border city who possesses a smuggled Chinese handset with a Chinese SIM card can connect to that network and make calls without being intercepted by the Koryolink domestic system. North Korean defectors can contact brokers in border Chinese cities, arrange a window of time, locate the family member in North Korea (sometimes traveling on foot to fetch them), and place the call. Through this method, millions of dollars per year are also sent in remittances through brokers from North Korean defectors to their families still in the country.[22][23][24]

This system has been working at scale since around 2003, when Chinese telecom companies began aggressive border expansion. Roughly 20,000 North Koreans were estimated to have access to Chinese cell phones in early reporting.[25][26]

The strengths of this approach for two-way communication are considerable. It utilizes existing commercial infrastructure on the Chinese border. The broker network provides operational

---

[22] Yonho Kim, "Cell Phones in North Korea: Has North Korea Entered the Telecommunications Revolution?", US-Korea Institute at SAIS, 2014, https://usakoreainstitute.org/wp-content/uploads/2014/03/Kim-Yonho-Cell-Phones-in-North-Korea.pdf

[23] "How a North Korean Defector Sends Money Back Home," Liberty in North Korea, July 22, 2022, https://libertyinnorthkorea.org/blog/how-a-north-korean-defector-sends-money-back-home

[24] "Cellphones smuggled into N. Korea allow defectors to hear from families and get them cash," Fox News / Associated Press, Dec. 10, 2015, https://www.foxnews.com/world/cellphones-smuggled-into-n-korea-allow-defectors-to-hear-from-families-and-get-them-cash

[25] Rebecca MacKinnon, "Chinese Cell Phone Breaches North Korean Hermit Kingdom," Yale Global Online, Jan. 17, 2005, https://archive-yaleglobal.yale.edu/node/48986

[26] Rebecca Mackinnon, "North Korea: Chinese cellphones spawn an information boom," New York Times, https://www.nytimes.com/2005/01/24/opinion/north-korea-chinese-cellphones-spawn-an-information-boom.html

tradecraft, including timing of calls to coincide with surveillance gaps and the use of mountainous areas with poor detection coverage. Additionally, though there is significant risk with this method of communication, there is credibility due to its longstanding use.

The risks are also severe and increasing. Under Kim Jong-un, possession of foreign-made cell phones has been redefined as effectively a national security offense, and the MSS's "mop-up war" since the COVID-19 pandemic has intensified arrests at the border.[27] RFA's June 2017 reporting documented that even "potential cell phone users" (people with defector family members who might be expected to receive a call) were being preemptively investigated, and that Kim Jong-un personally ordered the rooting out of Chinese mobile phone users with links to South Korea.[28] Reports also indicate the regime has begun to coerce brokers themselves to surrender Chinese phones to authorities under threats and inducements.[29]

For foreigners trying to communicate with North Koreans, working through the existing broker network is the only established channel for two-way voice contact. It is also the channel against which the regime has invested the most countermeasure resources. Any new technology under consideration should be evaluated against whether it improves on this baseline in either security, scalability, or geographic reach.

---

4. Technology Assessment

4.1 Satellite phones and satellite messengers

Satellite communications are an obvious candidate for evading the Sino-Korean border surveillance corridor, since they bypass terrestrial cell networks entirely. Three constellation types are commercially available:

Iridium (66 active satellites in low earth orbit at roughly 781 km, polar orbit, global coverage including poles). Handsets include the Iridium 9555 and Iridium Extreme, and the satellite

---

[27] Kim Chae Hwan, "N. Korea replaces radio wave detectors on border with the latest models," Daily NK, Nov. 3, 2022. https://www.dailynk.com/english/north-korea-replaces-radio-wave-detectors-border-latest-models/

[28] Jung Min Noh et al., "North Korea Targets Potential Illegal Cell Phone Users With Links to Defectors," Radio Free Asia, June 14, 2017, https://www.rfa.org/english/news/korea/north-korea-targets-potential-illegal-cell-phone-users-with-links-to-defectors-06142017163255.html

[29] Kim Yoo Jin, "N. Korea pressures some border residents to hand in foreign cell phones," Daily NK, Oct. 16, 2020, https://www.dailynk.com/english/north-korea-pressures-some-border-residents-hand-in-foreign-cell-phones/

messenger ecosystem built on Iridium includes the Garmin inReach Mini, Mini 2, Messenger, and Messenger Plus, as well as the older Iridium GO! hotspot.[303132]

Thuraya (two geostationary satellites covering Europe, Africa, Asia, and Australia, with North Korea inside the footprint; in fact the first Thuraya satellite, Thuraya 1, was positioned over Korea for testing in 2000).[3334] Handsets include Thuraya XT-PRO, X5-Touch, and the dual-mode Thuraya One.[35]

Inmarsat (geostationary, global except polar regions).[36] Handsets include the IsatPhone Pro and IsatPhone 2.[3738]

The viability of using these technologies inside of North Korea is questionable for a few reasons.

Legal and service-provider restrictions. U.S.-based Iridium complies with US embargo restrictions and explicitly does not provide service in North Korea, Cuba, Iran, Syria, Sudan, or Taliban-controlled Afghanistan.[3940] An Iridium handset taken into North Korea will not be able to register on the network or complete calls to the local phone system; this effectively eliminates Iridium-based devices, including the Garmin inReach line, as a sanctioned tool for ordinary use inside the country. Organizational use cases that rely on Iridium would have to navigate either legal grey areas or specific US State Department licensing of the sort that has been used for Starlink in Iran.[41]

---

[30] See live map at http://iridiumwhere.com/
[31] "Iridium Adds to Constellation Resilience with Launch of Spare Satellites," Iridium, https://investor.iridium.com/2023-05-20-Iridium-Adds-to-Constellation-Resilience-with-Launch-of-Spare-Satellites
[32] "Products," Iridium, https://www.iridium.com/products
[33] "Thuraya Coverage Maps," Global Satellite Group, https://globalsatellite.us/global-satellite-knowledge/thuraya-coverage-maps/
[34] "Space42 (aka Yahsat)," Skybrokers, https://sky-brokers.com/supplier/space42-aka-yahsat/
[35] "Products," Space42 Thuraya, https://www.thuraya.com/en/products-list/
[36] "Inmarsat Coverage Maps," Global Satellite Group, https://globalsatellite.us/global-satellite-knowledge/inmarsat-coverage-maps/
[37] "Inmarsat IsatPhone Pro," Northern Access, https://www.northernaxcess.com/inmarsat-isatphone-pro
[38] "Inmarsat IsatPhone 2 Satellite Phone Standard Package," Satellite Phone Store, https://satellitephonestore.com/catalog/sale/details/inmarsat-isatphone-2-satellite-phone-kit-322
[39] "Banned or Restricted Satellite Phones in Certain Countries," Apollo Satellite, https://apollosat.com/docs/countries-where-satellite-phones-are-banned-or-restricted/
[40] "Satellite Phones: Critical or Contraband?," U.S. Overseas Security Advisory Council, Feb. 15, 2019, https://www.osac.gov/Content/Report/1a7f1fde-f79c-431e-b567-15f4ae87b64b
[41] "U.S. Smuggled Thousands of Starlink Terminals Into Iran After Protest Crackdown," Wall Street Journal, Feb. 12, 2026, https://www.wsj.com/world/middle-east/u-s-smuggled-thousands-of-starlink-terminals-into-iran-after-protest-crackdown-69a8c74f

Thuraya, headquartered in the United Arab Emirates and owned by Yahsat / Space42, does not follow US embargo restrictions and technically provides coverage into North Korea. This makes it the most viable satellite handset from a pure-availability standpoint.[42]

Radio frequency detection and direction finding. The RF detection equipment that North Korea has deployed along the border was originally designed for cell phone monitoring, but the underlying principle of detecting a signal's emission and triangulating its source generalizes to any RF transmitter. Satellite phone uplinks transmit at L-band frequencies (around 1.6 GHz for Iridium and Thuraya) at output powers typically between 0.5 and 2 watts, which is comparable to or higher than a cellular phone. Most satellite handsets do not use directional antennas, meaning the uplink signal radiates in a broadly omnidirectional or upward-hemispheric pattern that ground-based monitoring equipment can detect.[43] The Open Internet Project's satellite safety guide notes flatly that "most satellite phones do not have directional antennas," and that handheld and vehicle-mounted RF monitoring tools, including inexpensive ones built on software-defined radios, can detect and locate such uplinks. If the MSS Bureau 10's detectors can find a Chinese cell phone in five meters in three minutes, a satellite phone is not categorically harder.

Communications interception. Commercial systems explicitly designed to intercept Thuraya, Iridium, and Inmarsat IsatPhone traffic — including voice content, SMS, and location — are sold openly by companies like Shoghi Communications and Stratign for law enforcement and military markets.[44][45] The technical literature has proposed some prevention methods to protect satellite communication uplink signals (SCUS) from being intercepted.[46] It is prudent to assume that North Korea, with its sophisticated electronic warfare units, has access to similar capability when assessing the threat landscape.

Physical detection. Even setting aside RF detection, the physical presence of a satellite phone in North Korea is itself a death sentence in a checkpoint search. There is no plausible cover story; the regime explicitly bans all unauthorized communication devices and possession can lead to severe penalties. The Garmin inReach Messenger weighs 4 ounces and measures 3.1 x 2.5 inches, which is small enough to conceal in clothing or modified objects, but not small enough to be plausibly something else if found.[47] Concealment in modified household items, electronics, or

---

[42] "Coverage Area," Thuraya, http://www.thuraya.it/thuraya/area_en.html
[43] "Satellite Communication Threats," Open Internet Project, https://satellitesafety.openinternetproject.org/en/
[44] "Unified Satellite Phone Monitoring System," Shoghi, https://www.shoghicom.com/all-products/unified-satellite-phone-monitoring-system
[45] "Satellite Phone Interception Systems," Stratign, https://www.stratign.com/satellite-phone-interception-systems/
[46] Wang et al., "LPI-based cooperative tactic for satellite communication uplink signal accompanied by directed and power limited jamming," Institute of Engineering and Technology, August 2021, https://ietresearch.onlinelibrary.wiley.com/doi/full/10.1049/sil2.12070
[47] "Comparing the inReach Mini, inReach Mini 2, and inReach Messenger Series," Garmin, https://support.garmin.com/en-US/?faq=evV7F5dyBJ3ghypusS3OQ9

vehicle compartments is possible but introduces a new failure mode where the device itself is found during routine inspection.

The Garmin inReach Mini 2 deserves a separate note because it is the smallest two-way satellite messenger commonly available. At 3.5 ounces and up to 14 days of battery life in tracking mode, it is essentially a pager-sized device offering two-way text via Iridium. Concealability is its strongest attribute. Its weaknesses are (a) the Iridium embargo issue described above, (b) GPS jamming by North Korea may disrupt its location-tagging features, (c) it transmits not only outbound but also receives, meaning it has an active duty cycle visible to spectrum monitoring, and (d) its activation requires a sustained subscription account tied to identity, which raises questions about who holds the account and how it is funded.

Assessment. For a foreign organization trying to enable a North Korean civilian to communicate, satellite phones offer geographic reach beyond the China border (which Chinese cellular service cannot) but at the cost of dramatically higher physical detection risk and continued radio frequency detection vulnerability. They might be most appropriate for trained operatives in specific operational contexts rather than for ordinary citizens. Among satellite options, Thuraya is the only constellation that legally services North Korea, but is thoroughly commercially compromised. Iridium-based two-way messengers like the Garmin inReach Messenger are the most concealable but face a hard embargo barrier and are still susceptible to tracking.

4.2 Radio (one-way, but worth noting as the established channel inward)

Radio is a one-way technology from foreign broadcaster to North Korean listener, so it does not solve the two-way problem. It is included here because it is the dominant historical channel for information flow into the country, and because any conversation about the two-way problem benefits from understanding what radio does and does not enable.

Voice of America Korean Service and Radio Free Asia broadcast shortwave and mediumwave into North Korea, supplemented by other NGOs like Free North Korea Radio, North Korea Reform Radio, and Voice of the People (Unification Media Group).[48] Defectors consistently report that radio was their primary or initial gateway to outside information; a former North Korean signal corps officer told RFA that the broadcasts were “the key influence for his decision to defect.”[49]

The advantage of radio is asymmetric risk: the listener is a passive receiver, and unless they are caught with the radio itself or with the volume audible, the act of listening produces no

[48] “A Secret Program Allowed VOA to Broadcast Television into North Korea. Now It's Gone,” Columbia Journalism Review, June 26, 2025, https://www.cjr.org/news/trump-lake-secret-program-voice-of-america-north-korea-tv-broadcast-gone.php
[49] “North Korean Soldier Jailed for Listening to Radio Free Asia on Duty,” U.S. Agency for Global Media, Aug. 31, 2020, https://www.usagm.gov/2020/08/31/north-korean-soldier-jailed-for-listening-to-rfa/

detectable signal. Detection requires physical search and informer reports, not radio frequency surveillance. Punishment when caught is still severe (for instance a North Korean soldier was sent to a political prison camp in 2020 for forgetting to retune the dial after listening to RFA on duty), but the operational tempo of catching listeners is much slower than catching phone users.[50]

There are two important recent developments to note: first, the Trump administration's effective dismantling of the US Agency for Global Media operations in 2025 has reportedly cut external Korean-language broadcasting by approximately 85 percent according to a 38 North assessment cited in subsequent press coverage.[51] Smaller NGO stations like Free North Korea Radio remain on air but cannot replace VOA and RFA's hours or production capacity. Second, North Korea's jamming has historically been overwhelmed by sheer volume of broadcasts; reducing the number of broadcasts proportionally increases the regime's per-broadcast jamming capability.[52]

Radio remains a complementary tool. It cannot enable two-way contact, but it builds the audience and trust on which two-way contact depends.

4.3 USB and SD card distribution (one-way baseline for content distribution)

The Human Rights Foundation's Flash Drives for Freedom campaign, which began in 2016, has delivered more than 140,000 USB drives and SD cards loaded with K-dramas, defector memoirs, foreign news, and the Universal Declaration of Human Rights, among other content.[53][54] Distribution methods include hand-carry by brokers, balloon launches from South Korea, and packages dropped in rivers. Kim Yo-jong, Kim Jong-un's sister, has reportedly confirmed in official statements that some balloon-borne USB packages have been reaching deep inside the country.[55]

Like radio, USB distribution is one-way. However, it is operationally important because it demonstrates a successful logistical chain that outside organizations already have experience operating: identifying smuggling methods, training allies as distributors, navigating border regulations, and adjusting tactics as the regime adapts. That same logistical chain can in principle

---

[50] Ibid.
[51] "Collapse of VOA broadcasts leaves North Koreans with sharply reduced access to uncensored foreign news," Milwaukee Independent, Dec. 2, 2025, https://www.milwaukeeindependent.com/newswire/collapse-voa-broadcasts-leaves-north-koreans-sharply-reduced-access-uncensored-foreign-news/
[52] Martyn Williams, "Digital Trenches: North Korea's Information Counter-Offensive," HRNK, 2019, https://www.hrnk.org/wp-content/uploads/2020/08/Williams_Digital_Trenches_Web_FINAL.pdf
[53] Flash Drives for Freedom, Human Rights Foundation, https://flashdrivesforfreedom.org/
[54] Seongmin Lee, "HRF's Flash Drives for Freedom May Be Reaching Deep Inside North Korea via Balloon-Borne Packages: Kim Yo-Jong Confirms," NK Insider, Jan. 8, 2025, https://www.nkinsider.org/hrfs-flash-drives-for-freedom-may-be-reaching-deep-inside-north-korea-via-balloon-borne-packages-kim-yo-jong-confirms/
[55] "North Korea Denounces Flash Drives for Freedom," Human Rights Foundation, Sept. 6, 2018, https://hrf.org/latest/north-korea-denounces-flash-drives-for-freedom/

support distribution of two-way communications hardware, with appropriate adjustments for the much higher physical risk of carrying a transmit-capable device.

4.4 Mesh networking applications (Briar, Bridgefy, FireChat)

Mesh networking applications create peer-to-peer networks among nearby devices over Bluetooth or local Wi-Fi, without requiring internet or cellular infrastructure. They have been featured prominently in protests where governments have shut down the internet, most notably Hong Kong (2014 Umbrella Movement with FireChat, 2019 protests with Bridgefy), Myanmar (1.3 million Bridgefy downloads in 24 hours following the 2021 coup), and Iran (950,000 Bridgefy downloads in 40 days during the Mahsa Amini protests).[56][57][58]

For North Korea, the appeal is in principle that two North Koreans within Bluetooth range (roughly 10 to 30 meters in practice) could communicate without any signal leaving their immediate vicinity, and that messages could relay through multiple devices to extend range across a neighborhood or market. This would not solve the cross-border problem, but it could theoretically enable an underground domestic network.

There are three significant problems, though.

First, North Korean domestic smartphones run customized Android variants with mandatory state surveillance software that takes forced screenshots, signature-checks files, and prevents installation of unauthorized applications. Installing Briar or Bridgefy on such a device is essentially impossible without rooting the phone, which itself is detectable and prohibited.

Second, even for users with smuggled phones or laptops capable of running such apps, the security analysis is unfavorable. The Royal Holloway and University of London security audit of Bridgefy in 2020 found that the protocol "permitted its users to be tracked, offered no authenticity, no effective confidentiality protections and lacked resilience against adversarially crafted messages."[59] Bridgefy has since added Signal Protocol encryption, but the underlying mesh architecture still leaks metadata about who is talking to whom. Briar is more robust cryptographically but, as the same paper notes, it is not truly a mesh network; it opens point-to-point Bluetooth connections to one-hop neighbors, limiting reach.

---

[56] Matthew De Silva, "Hong Kong protestors are once again using mesh networks to preempt an internet shutdown," Quartz, July 20, 2022, https://qz.com/1701045/hong-kong-protestors-use-bridgefy-to-preempt-internet-shutdown
[57] "Bridgefy: The Offline Messaging App Revolutionizing Crisis Communication Worldwide," Alchemist Accelerator, July 29, 2025, https://www.alchemistaccelerator.com/blog/bridgefy-the-offline-messaging-app-revolutionizing-crisis-communication-worldwide
[58] Ernestas Naprys, "People tired of internet shutdowns and privacy violations explore off-grid messengers," Cybernews, Jan. 19, 2026, https://cybernews.com/security/iran-sparks-interest-in-bluetooth-based-messengers/
[59] Martin R. Albrecht et al., "Mesh Messaging in Large-Scale Protests: Breaking Bridgefy," University of London, p. 1, 2021, https://eprint.iacr.org/2021/214.pdf

Third, Bluetooth itself is detectable. The MSS already monitors Bluetooth file transfers as part of its anti-impure media crackdowns, since file-sharing of K-dramas via Bluetooth between phones is a primary distribution mechanism the regime is trying to suppress.[6061] A Bluetooth mesh app running in a North Korean apartment block would emit detectable signals that pattern-match to forbidden activity even before the contents are read.

Assessment. Mesh networking is a technology to watch and to support development of, particularly for hardened protocols designed for the North Korean threat model. However, it is not currently a deployable two-way solution for ordinary North Koreans communicating with outside contacts.

4.5 Starlink and low-earth-orbit satellite internet

Starlink and similar LEO satellite internet constellations (OneWeb, Amazon LEO) are emerging as a category that could potentially transform the closed-society information problem. The Starlink case in Iran provides the most directly relevant precedent.

In September 2022, following the death of Mahsa Amini and the protests that followed, Elon Musk activated Starlink service over Iran with US Treasury sanctions relief.[6263] By the start of 2026, an estimated 50,000 terminals had been smuggled into Iran through covert logistics networks, reportedly including more than 6,000 terminals delivered with direct US State Department involvement during the January 2026 unrest.[64] Iranian authorities have responded with raids, arrests, criminalization of possession (years in prison under national-security laws), and reported jamming attempts, though the LEO architecture makes Starlink significantly harder to jam than geostationary satellite services.[65]

For North Korea, there are several circisumtantial differences to consider when evaluating the potential for LEO-based internet communication.

---

[60] Nat Kretchun et al., "Compromising Connectivity: Information Dynamics Between the State and Society in a Digitizing North Korea," InterMedia, 2017, https://gwern.net/doc/sociology/technology/2017-kretchun.pdf
[61] Choe Sang-Hun, "North Korea, Fearing K-Pop and Porn, Warns Against Smartphones' Influence," New York Times, Dec. 18, 2018, https://www.nytimes.com/2018/12/18/world/asia/north-korea-smartphones.html
[62] Karl Vick, "Receivers for Elon Musk's Starlink Internet Are Being Smuggled Into Iran," TIME, Oct. 22, 2022, https://time.com/6223999/starlink-iran-elon-musk/
[63] "SpaceX activates Starlink satellite internet in Iran to bypass blackout," Middle East Online, Jan. 9, 2026, https://middle-east-online.com/en/spacex-activates-starlink-satellite-internet-iran-bypass-blackout
[64] "Smuggling ring funnels Starlink into blacked-out Iran," The National / BBC, May 2, 2026, https://www.thenationalnews.com/news/mena/2026/05/03/smuggling-ring-funnels-starlink-into-blacked-out-iran-report-says/
[65] "As Iranian regime shuts down internet, even Starlink seemingly being jammed," Times of Israel, Jan. 10, 2026, https://www.timesofisrael.com/iran-appears-to-jam-starlink-after-shutting-down-comms-networks/

First, Iran has a population of 93 million with vast urban centers, porous land borders with Iraq, Turkey, Pakistan, Afghanistan, Armenia, and Azerbaijan, and an enormous expatriate community capable of funding and organizing smuggling.[66] North Korea has 25 million people, two land borders (China and the heavily militarized DMZ), a limited expatriate population, and a much smaller domestic civil society capable of receiving and operating sophisticated hardware.

Second, the Starlink terminal itself, while smaller than older satellite antennas, is still a roughly pizza-box-sized dish that must be placed with clear sky view.[67] Concealment options are more limited than for a handheld device, and the terminal's radio frequency signature is detectable in the same way that any large transmitter is. Because the satellites must orbit close to the Earth's surface, their movements are more predictable and they are more susceptible to signal disruption and tracking. In the case of Iran, for instance, the government has been successful in causing "about 30-80% packet loss, radio-frequency jamming, seizures of satellite equipment, and cracking down on possession and use of satellite terminals in the country, punishable by up to 10 years imprisonment." [68]

Third, the use case for Starlink in Iran has been primarily for activists with somewhat protected positions in cities to maintain external communications during state-imposed blackouts. North Korea's threat environment for ordinary citizens is qualitatively more severe; the Iranian activist who is publicly known to authorities faces beating and prison, while the North Korean caught with comparable equipment faces a political prison camp or execution and the same fate for their family.

Fourth, there remain the legal limitations. SpaceX has not been authorized to operate in North Korea and there is no current diplomatic precedent comparable to the Iran sanctions relief. Activation would require changes in policy or operating illegally outside of the embargo. The potential for what satellite technology could achieve in regard to communication in North Korea is huge, but it would likely require lengthy and complex navigation of legal policy.[69]

Despite these challenges, Starlink is the technology most worth strategic investment if the long-term goal is two-way communication. The barrier to entry is high, but the upside is dramatic: a single working terminal in a North Korean border city would, in principle, give a defector network or humanitarian organization a fully encrypted, bidirectional, video-capable

---

[66] "Iran Population (2026)," Worldometer, https://www.worldometers.info/world-population/iran-population/
[67] "SpaceX Starlink From Mini Dishes to Commercial for Remotes Bases and Towns," Next Big Future on Substack, March 2, 2025, https://nextbigfuture.substack.com/p/spacex-starlink-from-mini-dishes-to-commercial-for-remotes-bases-and-towns html
[68] Dinah Van Der Geest, "What Iran's Internet Shutdown Reveals About Starlink," Tech Policy Press, Feb. 4, 2026, https://www.techpolicy.press/what-irans-internet-shutdown-reveals-about-starlink/
[69] Martyn Williams, "New Satellite Could Provide Internet Access to North Korea…Someday," 38North, Oct. 20, 2023, https://www.38north.org/2023/10/new-satellite-could-provide-internet-access-to-north-korea-someday/

channel — at least until the regime catches up. It is also important to remember that the risk of operating a satellite-powered device would still carry severe consequences in the case that a North Korean citizen would be tracked and caught by the government, such as in the case of Iran. Starlink terminals in Iran have enabled video footage of crackdowns and arrests to reach the world directly, which could be huge for advocacy and information spreading in North Korea, assuming someone in North Korea would be willing to take the risk to spread the message.

4.6 Steganography in approved content

Though more dated, steganography is a method still worth mentioning: communication channels hidden inside permitted media. Steganographic techniques embed messages inside images, audio, or video files in ways that survive copying and that are invisible to casual inspection. A K-drama episode delivered on USB could in principle contain hidden text or files extractable by a recipient with the right software.

This is asymmetric and one-way in practice, since North Koreans may not have the technical capability to embed return messages. But for time-sensitive content distribution, like alerts about specific local events or coded messages for a smaller network of trained recipients, steganography is hard to detect because the carrier file is itself permitted content. The Open Technology Fund has supported steganography research as part of its broader portfolio.[70]

---

5. Lessons from Other Closed Societies

Several cases offer transferable lessons for North Korea.

Cuba and SNET. Beginning in the early 2000s, Cuban technologists built a clandestine national wired network called SNET (Street Network) by stringing Ethernet cables and Wi-Fi repeaters between rooftops and apartments, with no internet connection at all. By the late 2010s, SNET reached thousands of users and offered chat, gaming, dating, marketplaces, and Wikipedia-like services entirely outside government control. The Cuban government tolerated SNET for years because it was non-political (the explicit rules of SNET forbade religion, politics, and pornography), and absorbed it into a state-run system in 2019.[71][72][73] The lesson for North Korea is

[70] Open Tech Fund, https://www.opentech.fund/
[71] Priscila Bellini, “The life and death of SNET, Havana’s alternative internet,” Rest of World, Oct. 8, 2020, https://restofworld.org/2020/the-life-and-death-of-snet-havanas-alternative-internet/
[72] Tim Padgett, “Snarled SNET: Seizure Of Cuba's Underground Network May Signal Cyber-Crackdown,” WLRN, Aug. 26, 2019, https://www.wlrn.org/show/latin-america-report/2019-08-26/snarled-snet-seizure-of-cubas-underground-network-may-signal-cyber-crackdown
[73] Michael Weissenstein, “Cuban youth build secret computer network despite Wi-Fi ban,” Associated Press, Jan. 26, 2015, https://apnews.com/international-news-general-news-89893aee47b944d19e2812b52c66b9ba

that a hyperlocal mesh-or-cable network can flourish in the vacuum left by no internet, but only with substantial domestic technical capacity. North Korea's restrictions on hardware ownership and the criminalization of unauthorized computing make a Cuban-style emergence less likely without external seeding.

Hong Kong and the protest mesh apps. During the 2014 Umbrella Movement and the 2019 pro-democracy protests, Hong Kong demonstrators adopted FireChat and then Bridgefy to organize during anticipated internet shutdowns. The 2019 mobilization saw approximately 500,000 Hong Kong residents download Bridgefy in weeks. The lesson here is twofold: mass adoption is possible and rapid when the population is motivated, but the security analysis of consumer mesh apps was inadequate to the threat model, and a sophisticated state adversary could have exploited the protocol vulnerabilities documented later.[74]

Iran's information war. Iran's pattern of escalating internet shutdowns since 2019, met with adoption of Briar, Bridgefy, VPNs, and eventually Starlink, represents one of the most active large-scale conflicts between a population and a state over information access. Iranian activists have demonstrated that smuggled satellite hardware can be operated despite jamming and physical risk, that distributed networks of in-country supporters can sustain logistics chains, and that diaspora funding plus U.S. government coordination can deliver thousands of terminals into the country during a crisis. The relevance for North Korea is that the operational template (diaspora fundraising plus broker logistics plus targeted U.S. licensing) is now established and tested, providing a roadmap for Starlink in North Korea.

The China comparison and contrast. China's information environment is the closest analogy to North Korea's in terms of state capability, but it is qualitatively different because of the scale and sophistication of the population. China has 1.4 billion people, an enormous technical class capable of building and circumventing Great Firewall controls, and a domestic civil society (however constrained) that conducts public discussion within the bounds of permitted topics. The cat-and-mouse VPN dynamic in China does not transfer well to North Korea, where the equivalent of "having a VPN" is a multi-year imprisonable offense for most of the population.

6. Operational Security Considerations

The technologies discussed above are only as safe as the tradecraft around them. Below are some suggestions to consider.

Compartmentalization. No single person should know the full chain. The defector broker should not know the operational details of the foreign NGO; the North Korean family member

[74] Martin R. Albrecht et al., "Mesh Messaging in Large-Scale Protests: Breaking Bridgefy," University of London, 2021, https://eprint.iacr.org/2021/214.pdf

receiving the call should not know the identity of the donor funding the call. Each link is a potential point of failure (and torture victim) if a chain is compromised.

Burst transmission and timing discipline. Radio-frequency emissions can only be detected if a monitor is listening at that moment in that location. Coordinating calls or transmissions to brief windows, to mountainous areas with limited surveillance coverage, and to times when known surveillance vehicles are positioned elsewhere reduces (though does not eliminate) detection risk. Residents often travel to remote locations to make calls; the regime has responded by extending detection coverage to those areas.[75]

Plausible cover devices. Any hardware in North Korea must have a cover story or be concealed in something innocuous. Memory cards inside legal MP3 players, satellite messengers concealed inside larger devices, and software running on phones the user can credibly claim are personal possessions are all preferable to dedicated, single-purpose hardware that has no innocent explanation.

Account hygiene. Subscriptions to satellite services, mesh apps, or any contracted communications service create paper trails. Account ownership, payment methods, and IP-level metadata should be held by parties with no documented connection to the in-country end user. Using prepaid services, cryptocurrency payments, and accounts registered under third-country identities reduces forensic exposure.

Content discipline. What is said matters. Discussion of politics, defection, leadership, or organized resistance dramatically elevates the consequences of detection. Conversations limited to family contact, financial remittance, and personal information are still illegal but are sometimes treated as commercial smuggling rather than treason, with shorter sentences and bribery-resolvable outcomes.[76]

Two-person rules and counter-coercion planning. Brokers and in-country contacts are the most exposed nodes and the most likely to be flipped or coerced. Building in cross-verification (reporting the same content through two independent channels) and pre-arranged duress codes may be useful to consider.

Digital hygiene kits. Digital hygiene kits composed of anti-surveillance and anti-censorship tools tailored to North Korean technologies and risk environments would be extremely useful

---

[75] Kang Jae-Jun, "Border security supplies new phone detectors… '3 minutes, 5 meters,'" NK Insider, Apr. 9, 2025. https://www.nkinsider.org/border-security-supplies-new-phone-detectors-3-minutes-5-meters/

[76] "North Korea: Connection Denied: Restrictions on mobile phones and outside information in North Korea," Amnesty International, March 9, 2016, https://www.amnesty.org/en/documents/asa24/3373/2016/en/

tools.[77] This means software that defeats specific North Korean device-level surveillance (the forced screenshots, the file signing, the audit trail) tailored to the specific Android variants in use. This could be a potential Open Technology Fund research investment.[78]

---

7. Viability Ranking

Below is a ranking of the technologies, by viability, for the specific goal of two-way communication with everyday citizens in North Korea. Viability, in this context, should be understood as a function of detection risk, legal accessibility, operational maturity, and investment required, with the order as follows.

1. Smuggled Chinese cellular phones brokered through Korean-Chinese networks. The only currently functional two-way voice channel. Operational maturity is high; broker networks are established; the in-country user does not need to operate unfamiliar hardware. Risks are severe and rising — with detection technology now reaching five-meter accuracy in three minutes — but the channel works at scale and has worked for many years. Any humanitarian program should integrate with existing broker networks rather than building parallel infrastructure. This method is limited to border provinces where Chinese cell towers reach.

2. Garmin inReach Messenger or inReach Mini 2 (Iridium-based satellite messengers). The most concealable two-way option in principle, with global coverage and text capability sufficient for life-and-death communication. However, there are two hard barriers: the U.S. embargo means Iridium does not service North Korea, and radio frequency detection along the border is mature enough to find the device's transmissions. This method could be made viable through (a) U.S. government licensing comparable to the Starlink-Iran precedent and (b) careful operational planning to minimize transmissions and avoid known detection corridors. It is arguably best suited for trained operatives in defined operational contexts rather than ordinary citizens, until the legal and detection issues are addressed.

3. Thuraya satellite handsets (Thuraya XT-PRO, Thuraya One). The only major satellite constellation with both geographic coverage of North Korea and no U.S. embargo restrictions. However, Thuraya is a thoroughly commercially compromised network; interception equipment is widely available and likely accessible to the North Korean state. Concealment of the handset is also harder than the Garmin inReach Messenger. Thuraya handsets are best treated as a niche tool for specific defectors, journalists, and operative networks where the threat from interception can be managed through code words and compartmentalization.

---

[77] "Digital Security Resource Hub for Civil Society," Amnesty International, https://securitylab.amnesty.org/digital-resources/
[78] Open Tech Fund, https://www.opentech.fund/

4. Starlink (or comparable LEO satellite internet). Highest theoretical upside as a fully bidirectional, encrypted, high-bandwidth channel that largely bypasses surveillance vectors (based on current knowledge). Iran precedent shows that smuggling and operation at scale is achievable. Currently limited by lack of authorized service in North Korea, hardware form factor that is harder to conceal than handheld devices, and the absence of a diaspora and civil-society infrastructure comparable to Iran's. Worth substantial strategic investment as the next-generation answer to the two-way problem.

5. Mesh networking apps (Briar over Bluetooth, hardened protocols under development). Useful for hyperlocal communication among in-country users, particularly in dense urban areas where Bluetooth range covers a neighborhood, and where Bluetooth file-sharing is already a familiar practice. Does not solve the cross-border problem. Limited by the mandatory surveillance software on domestic phones and by detectability of Bluetooth emissions. Best treated as a complementary tool that becomes more valuable as other channels (satellite internet, smuggled smartphones with hardened operating systems) become available.

Other supporting infrastructure (one-way):

Steganography in approved content. Useful for asymmetric, one-way, time-sensitive communication to in-country recipients with technical capability. Hard to detect because the carrier file is permitted media. Limited by the technical capacity required for both ends. Best treated as a specialized tool for content distribution rather than two-way contact with ordinary citizens.

Radio (shortwave and mediumwave). One-way only, but builds the audience and trust that any two-way effort depends on. The reduction in VOA and RFA broadcasting in 2025 is a substantial setback that smaller organizations and broadcaster operations cannot fully replace.[7980]

USB and SD card distribution. One-way, but the proven logistical chain (Flash Drives for Freedom, balloon launches, broker-mediated distribution) is the same chain that any two-way hardware would have to travel on.

---

[79] "A Secret Program Allowed VOA to Broadcast Television into North Korea. Now It's Gone," Columbia Journalism Review, June 26, 2025, https://www.cjr.org/news/trump-lake-secret-program-voice-of-america-north-korea-tv-broadcast-gone.php

[80] "Collapse of VOA broadcasts leaves North Koreans with sharply reduced access to uncensored foreign news," Milwaukee Independent, Dec. 2, 2025, https://www.milwaukeeindependent.com/newswire/collapse-voa-broadcasts-leaves-north-koreans-sharply-reduced-access-uncensored-foreign-news/

8. Caveats and Limitations

This report cannot assess the current internal politics of broker networks, which fluctuate with Chinese-North Korean diplomatic conditions and have tightened substantially since the COVID-19 era border closures. It cannot evaluate any specific foreign organizations' existing operational tradecraft. It does not address satellite imagery and open-source intelligence, which are separate categories of remote sensing rather than two-way communication. It does not cover the specific software and protocol layer choices (end-to-end encryption implementations, key management, app selection) that any communication program would have to make, since those choices depend on the specific use case and partner relationships.

Every two-way communication channel that exists today asks the in-country end user to take on substantial risk for the objective of communication. The defector contacting family for personal reasons is making that calculation for themselves and their kin. A North Korean recruited as a journalistic source, or as a participant in an information access program, is asked to do so on behalf of a project they did not design and people they may never meet. The gravity, scale, and nature of human rights violations in North Korea hardly have a parallel in the modern world. An organization that organizes two-way communication is, by definition, recruiting the in-country participant into a system the regime classifies as treason.

This does not mean such work should not be done. It does mean that the choice of technology cannot be separated from the question of consent, of how meaningful the in-country participant's understanding of the risks is, and of what duty of care a foreign organization owes to that person and their family if the worst happens. The most technically sophisticated platform may not be worth deploying if the support system for compromise (legal aid, exfiltration, family support, financial assistance to surviving relatives) is not in place. That is a question for a different chapter of this work.

---

9. Next Steps for This Research

- Direct interviews with active defector broker networks about their current operational reality and what new technology they would actually find useful
- Technical consultation with Open Technology Fund and similar organizations about active research projects relevant to North Korea
- Closer analysis of the legal pathway to a U.S. government license analogous to the Iran-Starlink precedent
- Assessment of specific concealment techniques and supply chain options for any hardware that would actually be deployed

- Cost modeling for the different two-way communication technology options and their respective infrastructures
- Advocate for U.S. government to restore funding to radios broadcasting into North Korea
- Constant review of the most recent reporting on North Korean surveillance equipment upgrades and changes, since the regime's capabilities are evolving