

The Kim Regime: Sanctions, Diplomacy, and Nuclear Survival

By Major Mithun P. Sheth

Despite being subjected to one of the most comprehensive sanction regimes in history, the Democratic People's Republic of Korea (DPRK) has continued to develop its nuclear arsenal, posing a persistent challenge to global security and nonproliferation efforts. Through a combination of cyber operations, illicit trade networks, the procurement of dual-use technologies, and diplomatic maneuvering, North Korea has successfully circumvented restrictions to acquire critical materials and technologies. This article examines the strategies, technologies, and networks that enable the DPRK to sustain and expand its nuclear capabilities, highlighting the broader implications for regional stability and the effectiveness of international counterproliferation measures.

After China's first nuclear test in 1964, Kim Il Sung, founder and First Supreme Leader of North Korea, tried to purchase nuclear technology from Beijing and Moscow, both of whom refused due to their fear of Kim's intent to build nuclear weapons.¹ Kim assured the Chinese and Russian powers that the nuclear intentions of the DPRK were peaceful. Diplomatic maneuvering soon established relationships with the Union of Soviet Socialist Republics (USSR) to provide technical support, training, and nuclear fuel, and North Korean scientists were trained in nuclear physics in the USSR. By 1965, the USSR provided the DPRK a 2-megawatt light-water research reactor at the Yongbyon Nuclear Scientific Research Center. The North Koreans quickly reverse-engineered this technology, using Soviet education to repurpose the reactor for military applications. The Kim regime repeatedly insisted to its world allies that its actions were for peaceful purposes.

In 1977, the DPRK signed a trilateral safeguard agreement with the International Atomic Energy Agency (IAEA), bringing its Soviet-supplied IRT-2000 reactor under international safeguard. The DPRK also signed the Nuclear Nonproliferation Treaty in 1985.² These political actions seemed to suggest cooperation, but they were largely a superficial gesture used to gain and maintain Soviet support and nuclear fuel. While the DPRK allowed limited inspections of the reactor, it concealed its plutonium reprocessing efforts. For almost 7 years, the Kim regime delayed fulfilling the treaty's requirement to allow IAEA inspections. During this time, it clandestinely pursued nuclear weapon development.

North Korea also used the suspension of the Nuclear Nonproliferation Treaty as a bargaining tool for light

water reactors (LWRs) and oil while continuing uranium and missile development. By the early 1990s, the United States became aware of construction activities near Yongbyon, leading to suspicions that the DPRK was developing nuclear weapons. After coalition forces threatened air strikes, North Korea (as a stalling tactic) agreed to IAEA inspections. However, the DPRK repeatedly blocked inspectors from accessing two facilities at Yongbyon, where it was suspected of producing plutonium. The DPRK also provided false declarations regarding the accountability of nuclear material. When discrepancies were uncovered, the IAEA demanded access to the restricted facilities. In 1993, the situation worsened when North Korea announced its planned withdrawal from the Nuclear Nonproliferation Treaty. Just 1 month later, after the United States considered nuclear strikes, the DPRK suspended its withdrawal and signaled its willingness to discuss IAEA safeguards and inspections in exchange for modern LWR technology. This laid the foundation for the 1994 Agreed Framework between the DPRK and the United States, which required the DPRK to freeze the construction of its weapons-based nuclear reactor in exchange for two proliferation-resistant LWRs and 500,000 metric tons of fuel oil annually until the two reactors were completed.³ In 2002, evidence emerged that the Kim regime had violated the 1994 Agreed Framework by acquiring centrifuge components, enrichment materials, and short-range ballistic missile technology. Satellite imagery also revealed ongoing activities (such as the expansion of missile test sites and uranium enrichment facilities) at Yongbyon and other locations.⁴ North Korean diplomats then walked away from the negotiation table and removed all IAEA personnel from North Korea.

In 2008, the Six-Party Talks brought North Korea back to the bargaining table. They agreed to disable the Yongbyon reactor in exchange for fuel aid, economic incentives, and political concessions (such as their removal from the U.S. State Sponsors of Terrorism list).⁵ The Kim Regime partially disabled Yongbyon, but they refused to provide a full accounting of their nuclear program. While receiving aid, the DPRK continued the development of a uranium enrichment program. By the end of the Six-Party Talks, North Korea had significantly advanced their nuclear and missile programs. By 2009, the DPRK had walked away from the talks, resumed nuclear development, and conducted additional nuclear tests—all while keeping the agricultural support aid packages, food aid, and tons of fuel oil to address

their chronic energy shortages. Remaining off the State Sponsors of Terrorism list, the DPRK improved its image internationally and opened the door to limited financial transactions. However, in 2017, President Donald J. Trump put North Korea back on the list, effectively promising to punish third-party countries that financially dealt with North Korea.

The DPRK also uses cyber operations to forge shipping manifests, alter tracking systems, and create fake companies. Agents often use front companies and intermediaries to acquire materials such as aluminum tubes, high-strength steel, and centrifuge components under the guise of civilian use. In 2013, a shipment of graphite cylinders used in missile nose cones was intercepted in South Korea. The cylinders were *en route* to the DPRK, falsely labeled as industrial equipment.⁶ Additionally, the regime sources technologies with civilian and military applications through front companies and regional intermediaries. In 2017, investigations revealed that North Korean leaders used Glocom, a front company based in Malaysia, to sell military communications equipment internationally. The proceeds were funneled back to support DPRK weapon programs.⁷


The current DPRK has leveraged cyber operations as a critical tool to circumvent international sanctions, steal resources, and procure the technologies necessary to sustain and expand its nuclear program. In 2018, the DPRK Reconnaissance General Bureau (the DPRK intelligence agency) forced the transfer of \$10 million from Banco de Chile to accounts in Hong Kong.⁸ The proceeds have reportedly funded as much as 40 percent of the cost of the weapons of mass destruction program of North Korea.⁹

North Korea has become resilient to sanctions by relying on sophisticated smuggling operations, including ship-to-ship transfers of oil and other sanctioned goods. The *Wise Honest*, a DPRK ship seized by the United States in 2018, was involved in illicit coal exports and equipment imports for its nuclear program.¹⁰ In 2019, the United Nations reported that DPRK vessels engaged in illegal ship-to-ship transfers of refined petroleum products, often in the East China Sea. These transfers involved turning off automatic identification system trackers to avoid being monitored.¹¹ DPRK ships have been caught transporting banned coal to countries such as China and receiving refined petroleum products at sea in violation of United Nations sanctions.

North Korean cyber units, particularly the Lazarus Group, have conducted large-scale cryptocurrency heists, stealing billions of dollars from exchanges, wallets, and mining operations. In 2022, the Lazarus Group's crypto heists enabled the DPRK to steal \$615 million from Ronin Network, \$100 million from Horizon, and \$100 million from crypto portfolios in the form of Atomic Wallet, Bitcoin, Ethereum, Binance Smart Chain, and Polygon.¹² Pyongyang leaders continued cyberattacks and, by 2023, had netted the regime around \$3 billion over 6 years. The DPRK has also targeted brick and mortar financial institutions. The Lazarus Group funneled \$81 million in fraudulent Society

for Worldwide Interbank Financial Telecommunications transactions through the Bank of Bangladesh.¹³ These funds bypass traditional banking systems and provide the regime a significant financial lifeline.

While not openly supportive, certain states provide tacit support or overlook violations, enabling North Korea to bypass sanctions. Chinese companies and brokers have been heavily implicated in aiding the smuggling efforts of the DPRK, often providing logistical support, financial services, and access to restricted materials. In 2018, the U.S. Treasury sanctioned Dalian Sun Moon Star International Logistics Trading Co., a Chinese firm that helped North Korea facilitate illicit fuel shipments and evade sanctions.¹⁴ The DPRK also partnered with Russian actors to acquire materials and technologies. Between 2022 and 2025, North Korea traded arms and ammunition with—and supplied workers and troops to—Russia in exchange for satellite technology and fuel. Russia helped the DPRK develop a military reconnaissance satellite, and Kim Jong Un, Third Supreme Leader of North Korea, supported Russia's invasion of Ukraine, providing millions of shells, rockets, labor workers, and troops. U.S. President Joseph R. Biden attempted to resume negotiations, but Pyongyang leaders showed little interest as they continued missile testing and formally ended efforts to reunify with South Korea.

The DPRK nuclear program has been marked by a pursuit of nuclear weapons despite widespread sanctions and diplomatic agreements. Through clandestine nuclear development, diplomatic maneuvering, cyber operations, and illicit trade networks, Pyongyang has consistently bypassed sanctions and pursued its nuclear ambitions. The regime has repeatedly used international agreements as tools to gain economic aid and diplomatic concessions while continuing to secretly expand its nuclear capabilities. Despite periods of diplomatic engagement, DPRK nuclear and missile programs have advanced, and its reliance on smuggling networks and support from allies such as China and Russia further complicate efforts to curb proliferation. The response of the global community must evolve to address a multifaceted approach to the DPRK, emphasizing both sanctions and strategies to disrupt illicit financial and trade networks while leveraging information warfare and diplomatic pressure on its remaining supporters. 

Endnotes:

¹Balazs Szalontai and Sergey Radchenko, "North Korea's Efforts to Acquire Nuclear Technology and Nuclear Weapons: Evidence from Russian and Hungarian Archives," *Woodrow Wilson International School for Scholars*, August 2006, <https://www.wilsoncenter.org/sites/default/files/media/documents/publication/WP53_web_final1.pdf>, accessed on 9 April 2025.

²International Atomic Energy Agency, "Fact Sheet on DPRK Nuclear Safeguards," *www.iaea.org*, 25 July 2014, <<https://www.iaea.org/newscenter/focus/dprk/fact-sheet-on-dprk-nuclear-safeguards>>, accessed on 9 April 2025.

³Kelsey Davenport, "The U.S.-North Korean Agreed Framework at a Glance," *Armscontrol.org*, 2022, <<https://www.armscontrol.org/assess/the-us-north-korean-agreed-framework-at-a-glance>>.

[.armscontrol.org/factsheets/us-north-korean-agreed-framework-glance](https://armscontrol.org/factsheets/us-north-korean-agreed-framework-glance)>, accessed on 14 April 2025.

⁴Jayshree Bajoria and Beina Xu, “The Six Party Talks on North Korea’s Nuclear Program,” *Council on Foreign Relations*, 30 September 2013, <<https://www.cfr.org/background/six-party-talks-north-koreas-nuclear-program>>, accessed on 9 April 2025.

⁵Joseph S Bermudez, “Undeclared DPRK: The Yongnim Missile Operating Base,” *Beyond Parallel*, 14 November 2024, <<https://beyondparallel.csis.org/undeclared-north-korea-the-yongnim-missile-operating-base/>>, accessed on 9 April 2025.

⁶Mary Beth Nikitin, “North Korea’s Nuclear Weapons: Technical Issues,” *Congressional Research Service*, 3 April 2013, <<https://www.congress.gov/crs-product/RL34256?q=%7B%22search%22%3A%22RL34256%22%7D&s=6&r=6>>, accessed on 9 April 2025.

⁷James Pearson and Rozanna Latiff, “North Korea Spy Agency Runs Arms Operation out of Malaysia, U.N. Says,” *Reuters*, 27 February 2017, <<https://www.reuters.com/article/world/north-korea-spy-agency-runs-arms-operation-out-of-malaysia-un-says-idUSKBN1650YE/>>, accessed on 9 April 2025.

⁸Julian Ryall, “How Crypto Heists Help North Korea Fund Its Nuclear Program,” *Deutsche Welle*, 26 March 2024, <<https://www.dw.com/en/how-crypto-heists-help-north-korea-fund-its-nuclear-program/a-68669802>>, accessed on 7 April 2025.

⁹Jayshree Bajoria and Beina Xu.

¹⁰Office of Public Affairs, “Department of Justice Announces Forfeiture of North Korean Cargo Vessel,” *U.S. Department of Justice*, 21 October 2019, <<https://www.justice.gov/opa/pr/department-justice-announces-forfeiture-north-korean-cargo-vessel>>, accessed on 9 April 2025.

¹¹Department of the Treasury, “Updated Guidance on Addressing DPRK’s Illicit Shipping Practices,” *Office of Foreign Assets Control*, 21 March 2019, <<https://ofac.treasury.gov/media/16506/download?inline>>, accessed on 9 April 2025.

¹²Hugh Griffiths et al., “Report of the Panel of Experts Established pursuant to Resolution 1874,” *un.org*, 3 April 2013, <<https://documents.un.org/doc/undoc/gen/n19/028/82/pdf/n1902882.pdf>>, accessed on 9 April 2025.

¹³FBI National Press Office, “FBI Confirms Lazarus Group Cyber Actors Responsible for Harmony’s Horizon Bridge Currency Theft,” *Federal Bureau of Investigation*, 23 January 2023, <<https://www.fbi.gov/news/press-releases/fbi-confirms-lazarus-group-cyber-actors-responsible-for-harmonys-horizon-bridge-currency-theft>>, accessed on 9 April 2025.

¹⁴“Dalian Sun Moon Star International Logistics Trading Co., Ltd,” *Open Sanctions*, 15 August 2015, <<https://www.opensanctions.org/entities/NK-PqXkeFYJQrsSemMbfzCnsc/>>, accessed on 9 April 2025.

Major Sheth is the Education Branch Chief for the U.S. Army Nuclear and Countering Weapons of Mass Destruction Agency, Fort Belvoir, Virginia. He holds a Doctor of Medicine (M.D.) degree from Poznan University of Medical Sciences, Poland; a master’s degree in environmental management from Webster University; and a master’s degree in strategic technology intelligence from National Intelligence University, Bethesda, Maryland.