Reporting Time	Incident	Tool	Linked actor	Response	Source 1	Source 2	Source 3	Source 4
2025	Lazarus Group, a North Korean state-sponsored APT, is known for financially and politically motivated cyberattacks. First gaining attention in 2013 with DarkSeoul, it targeted South Korean broadcasters and financial institutions. In 2014, it breached Sony Pictures, stealing and leaking sensitive data. In 2024, South Korea's National Police Agency, National Intelligence Service, and National Cyber Risk Management Unit revealed that Lazarus, along with Andariel and Kimsuky, had breached the internal networks of 10 South Korean defense companies, stealing sensitive technical data. In 2025, Kaspersky reported Operation SyncHole, a Lazarus-led campaign targeting at least six South Korean organizations in sectors like software, finance, semiconductors, and telecommunications.	Cyberattack	North Korea	Capability enhancement, Public awareness	https://apt	https://kore	https://ww	https://www.bbc.com/news/articles/c2kgndwwd7lo
2025	In February 2025, Kaspersky ICS CERT uncovered Operation SalmonShalom, a cyberattack campaign targeting industrial organizations across the Asia-Pacific region, including Taiwan, Malaysia, China, Japan, Thailand, Hong Kong, South Korea, Singapore, the Philippines, and Vietnam. The attackers used Chinese cloud services, such as myqcloud and Youdao Cloud Notes, to host and deliver multi-stage malware payloads, evading detection through DLL sideloading and encryption techniques.	Cyberattack	Unidentified hacker		https://ics-	https://apt.etda.or.th/cgi-bin/showcard.cgi?g=Operation%20SalmonSlalom		
2025	In January 2025, Jiji Press and the South China Morning Post, reported on a South Korean court case revealing that North Korea had directed a clandestine group—including a former executive of the Korean Confederation of Trade Unions—to incite anti-Japanese sentiment in South Korea. The directives, sent between 2018 and 2022, aimed to exploit public outrage over issues like wartime labor disputes and Japan's release of treated radioactive water from the Fukushima nuclear plant. The court documents indicated that the group received 89 instructions from North Korean handlers and sent back 13 detailed reports on their activities. The Suwon District Court sentenced three individuals, including the former KCTU executive, to prison terms ranging from five to 15 years for espionage under South Korea's National Security Act.	Narrative and information campaigns, Foreign interference	North Korea	Legislative and regulatory, Capability enhancement, Public awareness	https://ww	https://kore	https://ww	https://sp.m.jiji.com/english/show/37728
2025	Between June 2022 and April 2025, SK Telecom, South Korea's largest telecom provider, suffered a major cyber breach that went undetected for nearly three years. Hackers infiltrated 23 internal servers and extracted sensitive data from nearly 27 million mobile users, including SIM authentication keys and personal information. The malware used, linked to state-sponsored espionage, raised concerns about long-term surveillance risks. In response, the South Korean government launched a joint investigation, ordered free SIM replacements for affected users, and pledged to strengthen cybersecurity regulations and oversight across the telecom sector.	Cyberattack	China	Legislative and regulatory, Capability enhancement, Public awareness	https://ww	https://tech	https://cyt	https://koreajoongangdaily.joins.com/news/2025-05-19/business/industry/The-malware-in-the-SKT-hack-has-links-to-a-Chinese-group-This-may-just-be-the-beginning/2310662

2025	In early 2025, the North Korean cyber espionage group Kimsuky (also known as Velvet Chollima and Emerald Sleet) launched several sophisticated campaigns targeting South Korean government officials, media, and critical sectors like energy and finance. These included phishing attacks, malicious PDF lures, and exploitation of the BlueKeep vulnerability to deploy spyware and keyloggers. In response, South Korea's National Intelligence Service issued public warnings and partnered with international agencies, including Germany's BfV, to counter the group's evolving tactics.	Cyberattack	North Korea	Diplomatic, Legislative and regulatory, Capability enhancement, Public awareness	https://ww https://cybe https://ww https://gjia.georgetown.edu/2024/07/10/ai-and-cybersecurity-in-digital-warfare-on-the-korean-peninsula/
2025	In March 2025, North Korea launched multiple short-range ballistic missiles (SRBMs) into the Yellow Sea from an inland site in Hwanghae Province around 1:50 p.m. local time. The launch coincided with the beginning of the annual U.S.–South Korea "Freedom Shield" joint military exercises, which Pyongyang denounced as a "dangerous provocative act" that could escalate tensions. South Korea's Joint Chiefs of Staff identified the projectiles as close-range ballistic missiles (CRBMs) with a range of under 300 kilometers.	Military and paramilitary coercion	North Korea	Diplomatic, Military and paramilitary, Capability enhancement, Public awareness	https://kor https://apne https://www.reuters.com/world/asia-pacific/north-korea-calls-us-south-korea-drills-dangerous-provocative-act-2025-03-09/
2025	On 6 January 2025, North Korea launched an intermediate-range ballistic missile from the area of its capital city, Pyongyang, according to the South Korean Joint Chiefs of Staff. The suspect hybersonic missile reportedly flew about 1,100km before falling into the sea off its east coast. JCS stated that, in coordination with U.S. intelligence, they have heightened surveillance and vigilance, and are fully prepared to respond decisively to any North Korean military provocations under the joint defense posture.	Military and paramilitary coercion	North Korea	Diplomatic, Capability enhancement, Public awareness	https://the https://www.reuters.com/world/asia-pacific/north-korea-confirms-mondays-launch-new-hypersonic-missile-yonhap-says-2025-01-06/
2025	In January 2025, South Korean prosecutors indicted the CEO and lead designer of a Chinese company for attempting to manufacture and export semiconductor cleaning equipment using stolen technology from Samsung subsidiary SEMES. Between 2021 and 2022, they acquired blueprints and process documents from former SEMES employees and used them to build prototype machines, one of which was exported to China. The stolen technology, classified as national core technology, had taken 30 years and over ₩218 billion to develop. The defendants also signed a ₩7.82 billion investment deal with a Chinese firm, intending to transfer all personnel and technology.	Economic coercion	IP theft	Legislative and regulatory, Capability enhancement, Public awareness	https://hol https://www.businesskorea.co.kr/news/articleView.html?idxno=233993

2025	In February 2025, a former Samsung Electronics senior manager, Kim, was sentenced to seven years in prison and fined ₩200 million for leaking 18nm DRAM process technology—a national core technology—to China's ChangXin Memory Technologies. After joining CXMT in 2016, Kim allegedly used proprietary Samsung data, obtained through insider collaboration, to accelerate CXMT's DRAM development. Additional accomplices, including a partner company employee, received prison terms or suspended sentences.	Economic coercion	IP theft	Legislative and regulatory, Capability enhancement, Public awareness	https://ww https://www https://biz.chosun.com/en/en-society/2025/02/19/MD674HGEOFANNDLCJIJKJEL5TA/
2025	On January 19, 2025, in the early morning hours, a group of supporters of impeached South Korean President Yoon Suk-yeol stormed the Seoul Western District Court in protest of an arrest warrant issued against him. The crowd, estimated in the hundreds, breached court premises, clashed with security personnel, and caused significant property damage. Over 50 police officers were injured, and 86 individuals were arrested during the riot. In response, the Ministry of Justice and National Police Agency launched a joint investigation into the organization and financing behind the unrest.	Diplomatic coercion	IMVE	Legislative and regulatory, Capability enhancement, Public awareness	https://ww https://en.wikipedia.org/wiki/2025_Seoul_Western_District_Court_riot
2025	In January 2025, ESET uncovered a cyber-espionage campaign by a China-aligned APT group dubbed PlushDaemon, active since at least 2019. The group targeted individuals and organizations in China, Hong Kong, Taiwan, South Korea, the United States, and New Zealand. ESET revealed that PlushDaemon had compromised the installer of IPany, a South Korean VPN service, redirecting legitimate update traffic to attacker-controlled servers. This supply-chain attack delivered a custom backdoor named SlowStepper, a modular malware with over 30 components capable of stealing documents, credentials, and user data from infected systems.	Cyberattack	China		https://ww https://thehackernews.com/2025/01/plushdaemon-apt-targets-south-korean.html
2024	Between 2013 and 2024, APT29 (also known as The Dukes or Cozy Bear), a cyberespionage group linked to Russia's Foreign Intelligence Service (SVR), conducted multiple operations targeting South Korea. While most known for attacking Western governments and NATO-aligned institutions, APT29 also extended its reach to South Korean government entities, defense contractors, and research organizations. These operations primarily used spear-phishing campaigns and custom malware to gain long-term access to sensitive networks	Cyberattack	Russia		https://ww https://apt.(https://www.hivepro.com/wp-content/uploads/2024/07/TA2024255.pdf

2024	In September 2020, the U.S. Department of Justice indicted seven individuals linked to APT41 (Winnti, Barium, Wicked Panda, Wicked Spider) for hacking over 100 global targets, including South Korean video game companies. The group stole source code, customer data, and ran ransomware and cryptojacking schemes. Two Malaysian businessmen were arrested for profiting from the attacks. The operation used advanced techniques like supply chain compromises and DNS-based command-and-control.	Cyberattack	China		https://ww https://blog https://apt.etda.or.th/cgi-bin/showcard.cgi?g=APT%2041
2024	In February 2024, a major data leak exposed that the Chinese cybersecurity contractor I-Soon (also known as Anxun Information Technology) had carried out cyber-espionage activities targeting South Korea. Leaked internal documents—shared anonymously via GitHub—revealed that I-Soon had infiltrated South Korean government departments and telecommunications companies, including LG U+, from which they allegedly exfiltrated 3 terabytes of call log data between 2019 and 2021.	Cyberattack	China		https://the https://harf; https://asia.nikkei.com/Politics/International-relations/China-data-leak-spotlights-cyber-spying-across-Southeast-Asia
2024	In March 2024, Trend Micro revealed that the Chinese state-linked APT group Earth Krahang have conducted a global cyber espionage campaign beginning in early 2022. The group primarily targeted government entities across Southeast Asia, including South Korea, as well as regions in Europe, the Americas, and Africa. Earth Krahang exploited vulnerabilities in public-facing servers and leveraged compromised government infrastructure—such as email servers and websites—to launch cross-government spear-phishing attacks. In some cases, they used one government's compromised systems to infiltrate another, abusing intergovernmental trust.	Cyberattack	China		https://apt https://www.trendmicro.com/en_us/research/24/c/earth-krahang.html
2024	In November 2024, North Korea launched seven short-range ballistic missiles along its east coast following the test of its new solid-fuel ICBM, Hwasong-19 ("Mars-19"), in protest of joint military drills by the U.S., South Korea, and Japan. The South Korean Joint Chiefs of Staff condemned the launches as a provocation and diversion from reports of North Korea deploying over 10,000 troops to Russia. In response, South Korea conducted missile drills, participated in trilateral air exercises involving a U.S. B-1B bomber, and warned of further provocations, citing preparations for hypersonic missile and SLBM tests.	Military and paramilitary coercion	North Korea	Diplomatic, Military and paramilitary, Capability enhancement, Public awareness	https://kor https://engl https://www.abc.net.au/news/2024-11-01/north-korea-releases-hwasong19-missile-launch-images/104551852

2024	In October 2024, North Korea claimed that it had used explosives to destroy a road and railway section on the eastern and western borders, each about 60 meters long, in order to "completely separate from South Korea." This move was seen as a practical action after it officially defined South Korea as a "hostile country." In response, the South Korean Joint Chiefs of Staff stated that the South Korean military had fired warning shots in the area south of the Military Demarcation Line, and was working with the US military to closely monitor further developments of the North Korean military and maintain a high state of alert.	Military and paramilitary coercion, Infrastructure sabotage	North Korea	Diplomatic, Capability enhancement, Public awareness	https://edi https://www.aljazeera.com/news/2024/10/17/north-korea-blows-up-road-rail-links-with-hostile-state-south-korea
2024	In November 2024, North Korea began jamming GPS signals near the western border islands of South Korea, with disruptions continuing for at least ten consecutive days. The jamming was first detected in areas near Yeonpyeong Island and later spread to Gyeonggi and Gangwon provinces. South Korea's Joint Chiefs of Staff confirmed the activity and linked it to North Korea's military training exercises against drones. The JCS condemned the actions, urging Pyongyang to halt the provocations and warning that North Korea would be held accountable.	Cyberattack, Infrastructure sabotage, Military and paramilitary coercion	North Korea	Diplomatic, Capability enhancement, Public awareness	https://kor https://www.koreatimes.co.kr/southkorea/defense/20241112/north-korea-jams-gps-signals-for-fifth-consecutive-day-jcs
2024	In January 2024, the National Intelligence Service warned that hackers backed by the North could wreak greater havoc online as South Korea gers up for its general election in April 2024. According to an official from the spy agency who spoke to reporters at a closed door briefing, over 80 percent of the 1.62 million hacking attempts committed against South Korean companies and public institutions last year ave been traced back to the North's agents.	Cyberattack, Foreign interference	North Korea	Public awareness	https://kor https://thedefensepost.com/2024/01/26/north-korea-hackers-generative-ai-cyberattacks/
2024	Since late May to mid-October 2024, North Korea launched around 6,000 trash-filled balloons into South Korea, many carrying garbage, dirt, and even GPS transmitters. The balloons landed across Gyeonggi, Gangwon, and Seoul, prompting public safety alerts. South Korea's military condemned the campaign as a violation of international law, warning of a stern response if civilian harm occurred.	Territorial violation	North Korea	Diplomatic, Capability enhancement, Public awareness	https://edi https://kore https://kor https://www.abc.net.au/news/2024-05-31/what-north-korea-s-trash-balloons-mean/103918722

2024	In September 2024, two former Samsung executives were arrested on suspicion of stealing semiconductor technology data worth more than US$3.2 billion and establishing a chip company called "Chengdu Gaozhen" in China. One of them served as the CEO of the joint venture, and the other was a former senior researcher at Samsung. They allegedly copied Samsung's 20nm process technology and recruited several Korean semiconductor experts to participate in the project.	Economic coercion	IP theft	Legislative and regulatory, Capability enhancement, Public awareness	https://kor https://www https://ww https://www.reuters.com/technology/south-korean-chip-executive-detained-again-over-alleged-technology-leak-china-2024-09-06/
2024	In February 2024, South Korea's National Intelligence Service and Defense Counterintelligence Command announced that they were investigating several Indonesian engineers who were suspected of storing confidential data of the KF-21 "Bora Me" fighter in unauthorized USB devices and attempting to take it out of the country. The data includes approximately 4,000 to 6,600 technical documents, including 3D design drawings and sensitive flight control system information. At present, the persons involved in the case have been banned from leaving the country and the investigation is still ongoing.	Economic coercion	IP theft	Legislative and regulatory, Public awareness	https://wor https://en.yr https://theindonesian.id/2024/05/15/two-indonesian-engineers-still-under-investigation-over-kf-21-jet-data-theft/
2024	In June 2024, South Korea's Joint Chiefs of Staff reported that North Korea launched a suspected solid-fuel hypersonic missile from the vicinity of Pyongyang at approximately 5:30 a.m. The missile traveled about 250 kilometers before exploding midair over the East Sea, dispersing debris over several kilometers. The JCS noted that the missile emitted more smoke than usual, indicating potential combustion issues, and suggested it was a solid-fueled hypersonic missile.	Military and paramilitary coercion	North Korea	Diplomatic, Capability enhancement, Public awareness	https://ww https://www.reuters.com/world/asia-pacific/north-korea-claims-successful-test-develop-multiple-warhead-missile-2024-06-26/
2024	In April 2024, North Korea conducted a “super-large warhead” power test for its Hwasal-1 Ra-3 strategic cruise missile and also test-fired a new anti-aircraft missile named Pyoljji-1-2 in the Yellow Sea. According to North Korean state media, the tests were part of regular weapons development activities and achieved their intended goals. South Korea's Joint Chiefs of Staff confirmed the detection of multiple cruise and anti-aircraft missile launches around 3:30 p.m. and stated that the military is analyzing their specifications. Seoul emphasized it is maintaining a strong combined defense posture and closely monitoring for further provocations.	Military and paramilitary coercion	North Korea	Diplomatic, Capability enhancement, Public awareness	https://kor https://www https://www.globalsecurity.org/wmd/library/news/dprk/2024/dprk-240420-kcna01.htm

2024	On January 2, 2024, South Korean opposition leader Lee Jae-myung, head of the Democratic Party, was stabbed in the neck during a public event in Busan while visiting the site of a proposed airport development. The attacker, a 67-year-old man posing as a supporter, approached Lee under the pretense of requesting an autograph before stabbing him with an 18-centimeter knife. The injury caused significant bleeding, damaging Lee's jugular vein, and he was airlifted for emergency surgery.	Military and paramilitary coercion	IMVE	Legislative and regulatory, Public awareness	https://ww https://en.wikipedia.org/wiki/Attempted_assassination_of_Lee_Jae-myung
2024	Since October 2022, North Korea's Andariel hacking group has targeted South Korean defense firms, subcontractors, and infrastructure to steal technical data and credentials. Using phishing, software exploits, and malware like Dora RAT, the group infiltrated networks via outdated systems and compromised IT vendors. In 2024, South Korea, the US, and UK jointly warned of Andariel's global espionage campaign targeting military, nuclear, and aerospace sectors, alongside ransomware attacks used to fund North Korea's weapons programs.	Cyberattack	North Korea	Diplomatic, Legislative and regulatory, Capability enhancement, Public awareness	https://the https://kore https://www.theguardian.com/world/article/2024/jul/25/north-korea-backed-cyber-espionage-campaign-targets-uk-military
2024	In February 2024, South Korea joined a multinational cybersecurity advisory with the U.S., U.K., and other allies to address threats posed by APT28, a Russian state-sponsored cyber group linked to GRU Unit 26165. The advisory highlighted APT28's use of compromised Ubiquiti EdgeRouters for credential harvesting and malware deployment.	Cyberattack	Russia	Diplomatic, Legislative and regulatory, Capability enhancement, Public awareness	https://me https://apt.etda.or.th/cgi-bin/showcard.cgi?g=Sofacy%2C%20APT%2028%2C%20Fancy%20Bear%2C%20Sednit
2024	In February 2024, South Korea President Yoon Suk Yeol's office said that presumed North Korean hackers breached the personal emails of one of the president's staff members ahead of the presidential trip to Europe in November. The office said the breach onl affected the personal account of the unidentified employee, who violated security protocols by partially using commercial email services to handle office duties. Officials did not specify what type of information was stolen from the staff members' personal emails but stressed that the office's overall security system was not affected.	Cyberattack	North Korea	Public awareness	https://ww https://apnews.com/article/north-korea-hacking-south-korean-presidential-office-4248cc5ddc964c2c6c89ba2ab4f139fc

2023	APT27 (also known as Emissary Panda, LuckyMouse, or Bronze Union) is a Chinese state-sponsored cyberespionage group that has conducted long-term campaigns against critical sectors such as aerospace, government, defense, and telecommunications. According to Cybereason's DeadRinger report, APT27 used strategic web compromises to target organizations in countries including South Korea, Australia, India, Japan, and others. The group's South Korea targeting focused on telecom and technology sectors, aligning with broader Chinese intelligence objectives.	Cyberattack	China		https://apt https://www.cybereason.com/blog/research/deadringer-exposing-chinese-threat-actors-targeting-major-telcos
2023	Between November 2023 and April 2024, cybersecurity researchers from Recorded Future's Insikt Group observed the Chinese state-sponsored APT group RedJuliett (also known as Flax Typhoon) conducting cyber-espionage operations targeting government, education, and technology sectors in South Korea and other countries. The group exploited vulnerabilities in internet-facing appliances such as VPNs and firewalls to gain initial access, followed by post-exploitation using web shells and privilege escalation tools. Although Taiwan was the primary focus, South Korea was among the countries where compromised communications with RedJuliett-controlled servers were detected, indicating likely infiltration.	Cyberattack	China		https://go. https://www https://socradar.io/dark-web-profile-flax-typhoon/
2023	In June 2023, a former Samsung executive and six accomplices were arrested and charged for stealing factory blueprints and clean-room designs to build a copycat semiconductor plant in Xi'an, China. Backed by Chinese and Taiwanese investors, the executive had recruited over 200 engineers from Samsung and SK Hynix, attempting to replicate core national technologies worth an estimated $236 million.	Economic coercion	IP theft	Legislative and regulatory, Capability enhancement, Public awareness	https://ww https://www https://www.ft.com/content/fc7f6ea0-08f6-40f3-897f-e723cff9fd8c
2023	In January 2023, South Korean prosecutors indicted a group of five individuals—among them a former Samsung SEMES employee, a Chinese broker, and subcontractor personnel—for leaking key semiconductor equipment technology to a Chinese company (PNC Process System). The stolen information involved blueprints for wet cleaning systems used in advanced chip fabrication, which the South Korean government classifies as "national core technology." The former SEMES employee allegedly obtained the designs through KakaoTalk and transferred them via an intermediary to the Chinese firm, in a deal worth nearly ₩248 billion per equipment set.	Economic coercion	IP theft	Legislative and regulatory, Capability enhancement, Public awareness	https://kor https://www https://kei https://www.koreatimes.co.kr/business/tech-science/20240206/korea-to-toughen-penalties-for-technology-theft

2023	In mid 2023,GambleForce, a China-based cyber threat group, has conducted SQL injection attacks using publicly available tools like sqlmap, Cobalt Strike, and dirsearch. The group targets sectors including gambling, government, and retail, compromising over 20 websites in countries such as South Korea, Australia, India, and the Philippines. Despite using basic methods, GambleForce has exfiltrated login data, hashed passwords, and database structures. A confirmed South Korean target was a gambling platform. The use of tools containing Chinese-language commands.	Cyberattack	China		https://ww https://cybersecurityasia.net/asia-pacific-hit-by-gambleforce-hacker-group-with-sql-injection-attacks/
2023	Between November 2022 and January 2023, three North Korean state-sponsored cyber groups—Ruby Sleet, Diamond Sleet, and Sapphire Sleet—conducted coordinated cyberattacks on maritime and defense sectors, including South Korean naval shipyards. Microsoft and South Korea's National Intelligence Service confirmed that these actors aimed to steal naval technologies through phishing campaigns and compromised IT maintenance networks. At least two South Korean defense contractors, including Daewoo Shipbuilding & Marine Engineering, had previously been breached in earlier attacks.	Cyberattack	North Korea	Legislative and regulatory, Capability enhancement, Public awareness	https://ww https://www Digital thre https://www.inss.re.kr/upload/bbs/BBSA05/202404/F20240425131646465.pdf
2023	In January 2023, China implemented restrictions on issuing short-term visas to South Korean and Japanese citizens in retaliation for COVID-19 testing requirements these countries imposed on travelers from China. The restrictions included suspending the issuance of port visas and stopping the 72/144-hour visa-free transit policy for these nationals.	Diplomatic coercion	China	Diplomatic	https://ww https://apne https://www.abc.net.au/news/2023-01-11/china-suspends-issuing-visas-retaliate-covid-test-travellers/101842880
2023	In March 2023, North Korea conducted a series of high-profile weapons tests, including the trial of a new underwater nuclear attack drone named Haeil and the launch of four strategic cruise missiles (two Hwasal-1 and two Hwasal-2) tipped with simulated nuclear warheads. The underwater drone, launched off the coast of Riwon County, cruised for over 59 hours before detonating near Hongwon Bay, while the cruise missiles, launched from Hamhung, flew up to 1,800 km in programmed patterns before striking targets in the East Sea. North Korea framed the tests as a response to U.S.-South Korea joint military drills. South Korea's military confirmed the cruise missile launches and, with the U.S., analyzed the details. Defense officials in Seoul acknowledged North Korea's significant progress in miniaturizing nuclear warheads for tactical use.	Military and paramilitary coercion	North Korea	Diplomatic, Military and paramilitary, Capability enhancement, Public awareness	https://en. https://en.y https://www.mofa.go.kr/viewer/skin/doc.html?fn=20230621040037933.pdf&rs=/viewer/result/202505

2023	On July 12, 2023, North Korea launched an intercontinental ballistic missile (Hwasong-18) that flew approximately 1,000 km over a 74-minute flight, reaching an altitude of over 6,000 km before landing in the sea west of Japan. The launch followed threats from Pyongyang over alleged U.S. spy plane incursions and coincided with a trilateral military meeting between the U.S., South Korea, and Japan in Hawaii. South Korea and the U.S. strongly condemned the missile test as a grave provocation and a violation of UN Security Council resolutions, while North Korean state media framed the action as a response to perceived military threats.	Military and paramilitary coercion, Diplomatic coercion	North Korea	Diplomatic, Capability enhancement, Public awareness	https://ww https://www https://www.theguardian.com/world/2023/jul/12/north-korea-fires-ballistic-missile-towards-japan
2023	In November 2023, South Korea's intelligence said it has identified 38 Korean-language news websites that are suspected of being run by Chinese companies with some allegedly spreading pro-China and anti-US content. South Korea's National Intelligence Service said two Chinese public relations firms were involved in creating fake websites in the country masquerading as members of the Korea Digital News Association. A month earlier in October 2023, the Global Engagement Center, a State Department Agency that's tasked with combating foreign propaganda and disinformation and that released the 58-page report, warned that Beijing's information campaign could eventually sway how decisions are made around the world and undermine its interests.	Narrative and information campaigns	China	Legislative and regulatory, Capability enhancement, Public awareness	https://ww https://kore https://www.koreaherald.com/article/3256236
2023	In January 2023, South Korea-based AhnLab identified a cyber campaign by RedEyes (APT37 or ScarCruft), a North Korea-linked group, targeting individuals using a steganography-laced HWP exploit (CVE-2017-8291) and a new malware called M2RAT. Victims included defectors and activists. While no direct government response was noted, KrCERT/CC has previously tracked this actor.	Cyberattack	North Korea	Capability enhancement	https://ase https://usa.i https://thorcert.notion.site/TTPs-ScarCruft-Tracking-Note-67acee42e4ba47398183db9fc7792aff
2022	On 26 December 2022, five North Korean drones crossed into South Korea and South Korea responded by scrambling jets and attack helicopters and opening fire to try to shoot down the North Korean aricraft, according to the South Korean military. In reponse, South Korea sent a surveillance aricraft into North to photograph its miltiary intelligence and scrambled fighter jets and attack helicopters, and fired shots.	Military and paramilitary coercion, Territorial violation	North Korea	Military and paramilitary, Capability enhancement, Public awareness	https://edi https://www https://ww https://www.kci.go.kr/kciportal/landing/article.kci?arti_id=ART002962095

2022	On 13 October 2022, North Korea launched a series of provacations within 24 hours in a continuing offensive posture, including a ballistic missile test, a dispatch of military planes, and the firing of hundreds of rounds of artillery along both coasts of the Korean Peninsula.In response, South Korea scrambled F-35A fighter jets and also announced unilateral sanctions against North Korea for the first time in the last five years from the reporting time.	Military and paramilitary coercion, Territorial violation	North Korea	Diplomatic, Military and paramilitary, Capability enhancement, Public awareness	https://ww https://www https://www.nknews.org/2022/10/south-korea-announces-first-unilateral-sanctions-on-north-korea-in-five-years/
2022	In March 2022, North Korea test-launched the Hwasong-17 intercontinental ballistic missile (ICBM) for the first time. The missile flew approximately 1,090 kilometers and reached a peak altitude of around 6,248 kilometers before falling into the Sea of Japan. As North Korea's largest known ICBM, the Hwasong-17 is capable of carrying multiple nuclear warheads and potentially striking targets across the continental United States.	Military and paramilitary coercion	North Korea	Diplomatic, Capability enhancement, Public awareness	https://ww https://www https://www.asahi.com/ajw/articles/14581981
2022	Between March 2018 and December 2021, former employees of SEMES, a key semiconductor equipment subsidiary of Samsung Electronics, stole proprietary technology used to manufacture 14 wafer-cleaning machines—a critical part of Samsung's chipmaking process. The stolen equipment, worth 71 billion won (~$54 million), was sold to a Chinese company, which built a factory in Cheonan to replicate the technology. In 2022, seven individuals were indicted by the Suwon District Prosecutors' Office, and some were later sentenced to 18 months in prison by the Seoul Central District Court under the Unfair Competition Prevention and Trade Secret Protection Act.	Economic coercion	IP theft	Legislative and regulatory, Capability enhancement, Public awareness	https://wo https://www.sammobile.com/news/ex-samsung-employees-sentenced-to-jail-leaking-tech-to-china/
2022	On March 7, 2022, Song Young-gil, then-leader of the Democratic Party of Korea, was attacked during a campaign event in Seoul's Sinchon area. A man in his 70s, dressed in traditional Korean hanbok and identified as a YouTuber, approached Song and struck him multiple times on the head with a hammer. The assailant reportedly shouted slogans opposing South Korea–U.S. military exercises during the attack. Song sustained head injuries and was taken to the hospital for treatment. The attacker was arrested at the scene and later found dead in his prison cell in April 2022, with authorities indicating suicide as the cause.	Military and paramilitary coercion	IMVE	Legislative and regulatory, Public awareness	https://ww https://cn.yna.co.kr/view/ACK20220307003700881

2022	In 2022, ESET revealed Chian-aligned cyberespionage group named Worok, active since at least late 2020. The group targeted governments and high-profile organizations primarily in Asia, the Middle East, and Africa. Worok uses a custom toolset, including a C++ loader (CLRLoad), a PowerShell backdoor (PowHeartBeat), and a C# loader (PNGLoad) that extracts hidden malicious payloads from PNG image files using steganography.	Cyberattack	China		https://ww https://cybe https://www.welivesecurity.com/en/eset-research/eset-apt-activity-report-q4-2024-q1-2025/
2022	In August 2022, Mandiant identified the HaïEnergy campaign as a pro–People's Republic of China information operation targeting the U.S. and its allies. Triggered by U.S. House Speaker Nancy Pelosi's planned visit to Taiwan, the campaign disseminated narratives urging her to "stay away" and portraying the U.S. as an unreliable ally. According to RSIS, the operation leveraged a network of at least 72 suspected inauthentic news sites—some impersonating local media in countries like South Korea and Singapore—to amplify PRC-aligned messaging.	Narrative and information campaigns	China		https://clo https://www.rsis.edu.sg/wp-content/uploads/2024/10/PR241025_Networks-of-Inauthentic-News-Sites-the-Risk-of-Hostile-Information-Campaigns-in-SG.pdf
2021	In April 2021, thousands of posts in languages including English, Japanese, and Korean, images, and videos were posted across multiple platforms by accounts Mandiant assess to be part of this broader activity set that called on Asian Americans to protest racial injustices in the U.S.	Narrative and information campaigns	China		https://cloud.google.com/blog/topics/threat-intelligence/pro-prc-influence-campaign-expands-dozens-social-media-platforms-websites-and-forums/
2021	In mid-2020, ESET linked the Gelsemium APT group—active since at least 2014—to cyberespionage targeting governments, universities, and electronics firms in East Asia and the Middle East. While not explicitly confirmed, South Korea may be among its targets. The group uses spear-phishing, watering holes, and Exchange exploits (e.g., CVE-2020-0688), showing evolving capabilities.	Cyberattack	Unidentified hacker		eset_gelse https://www.theregister.com/2021/06/09/eset_gelsemium_research/

2021	On October 19, 2021, North Korea test-fired a new type of submarine-launched ballistic missile (SLBM) from waters near Sinpo, claiming it was launched from the 8.24 Yongung submarine. The missile flew about 590 km and featured advanced maneuverability to evade missile defenses. South Korea confirmed the launch but could not verify the platform. The U.S. condemned the test as a violation of UN Security Council resolutions, and the UN held an emergency meeting in response.	Military and paramilitary coercion	North Korea	Diplomatic, Capability enhancement, Public awareness	https://kor https://www.aljazeera.com/news/2021/10/20/n-korea-confirms-test-of-new-type-submarine-launched-missile
2021	In September 2021, North Korea test-fired the Hwasong-8, its first missile equipped with a hypersonic glide vehicle (HGV), from Toyang-ri in Jagang Province. North Korean state media hailed the missile as a strategic weapon and a key component of its five-year military development plan. In response, South Korea's Joint Chiefs of Staff assessed that the missile was still in early development and not yet combat-ready, estimating its speed at around Mach 3 and affirmed that existing South Korea-U.S. missile defense systems could still detect and intercept it.	Military and paramilitary coercion	North Korea	Diplomatic, Public awareness	https://kor https://opennuclear.org/sites/default/files/OBSERVATIONS%20ON%20THE%2028.9.2021%20HYPERSONIC%20MISSILE%20TEST-compressed.pdf
2020	Between 2017 and 2024, a civilian employee at South Korea's Korea Defence Intelligence Command, formerly a military officer, leaked at least 30 classified military documents to Chinese intelligence agents. The breach began after the employee was detained in April 2017 by Chinese authorities at Yanji Airport, where he was allegedly coerced into cooperation. Over the next seven years, he used covert methods—including silent camera apps and encrypted cloud uploads—to smuggle sensitive materials, including details of undercover agents. His activities went undetected until June 2024, and he was indicted on August 27, 2024, on charges of violating military secrecy and receiving bribes.	Narrative and information campaigns, Diplomatic coercion	China	Legislative and regulatory, Capability enhancement, Public awareness	https://ww https://www.chosun.com/english/national-en/2024/08/29/MWBXZUFKNBDRNKUMYZ6IET7ARE/
2020	On 16 June 2020, North Korea blew up the inter-Korean liaison office in Kaesong, a building funded by South Korea as a symbol of cooperation. The act, following threats by the Korean People's Army to reoccupy border areas, was condemned by Seoul as a betrayal of peace efforts. In response, South Korea boosted surveillance and, in June 2023, the Unification Ministry sued Pyongyang for 45 billion won ($35.2 million) in damages over the destruction.	Infrastructure sabotage	North Korea	Diplomatic, Legislative and regulatory, Capability enhancement, Public awareness	https://en.y https://kore https://www.reuters.com/article/world/north-korea-destroys-inter-korean-liaison-office-in-terrific-explosion-idUSKBN23M31T/

2020	On May 3, 2020, North Korean troops fired multiple gunshots at a South Korean guard post in the Demilitarized Zone (DMZ), striking the outer wall of the post. In response, South Korea's military returned fire with two warning volleys and issued broadcast warnings. No casualties were reported. The United Nations Command (UNC) later concluded that both Koreas violated the armistice agreement, though it could not determine whether the North's initial gunfire was intentional. South Korean officials initially assessed the shots as accidental, and the incident occurred just one day after Kim Jong Un's reappearance following a long public absence.	Military and paramilitary coercion, Territorial violation	North Korea	Military and paramilitary, Capability enhancement, Public awareness	https://ww https://www https://www.koreatimes.co.kr/southkorea/defense/20200526/unc-concludes-both-koreas-violated-armistice-agreement-in-gunfire-exchange-in-dmz
2020	In October 2020, U.S. agencies publicly warned about the North Korea-linked BeagleBoyz APT group, which had been conducting financially motivated cyberattacks since at least 2015. The group targeted banking institutions worldwide—including in South Korea—using sophisticated tools like Cobalt Strike, PowerShell-based malware, and custom backdoors to breach SWIFT networks and steal large sums. While South Korean incidents were not detailed, the country was named among affected targets.	Cyberattack	North Korea		https://ww https://apt.etda.or.th/cgi-bin/showcard.cgi?g=Subgroup%3A%20BeagleBoyz
2020	In March 2020, North Korea conducted a series of short-range ballistic missile (SRBM) launches, intensifying regional tensions during the global COVID-19 crisis. On March 21, it launched two SRBMs from Sonchon, North Pyongan Province, which flew about 410 kilometers at an altitude of 50 kilometers. North Korean state media reported that Kim Jong-un oversaw the test of a new "tactical guided weapon" with enhanced precision. A week later, on March 29, two more SRBMs were launched from Wonsan, flying approximately 230 kilometers at an altitude of 30 kilometers. South Korea's Joint Chiefs of Staff condemned the launches as "highly inappropriate" and urged Pyongyang to cease such military provocations, especially amid the global pandemic.	Military and paramilitary coercion	North Korea	Diplomatic, Public awareness	https://en. https://en.y https://ww https://www.aljazeera.com/news/2020/3/29/n-korea-fires-more-missiles-than-ever-amid-coronavirus-pandemic
2020	In April 2020, North Korea test-fired the Kumsong-3 (KN-19), a ground-launched anti-ship cruise missile based on the Soviet Kh-35. The missiles, launched from near Munchon on the east coast, flew over 150 km before landing in the East Sea. The Kumsong-3 is believed to have a range of 130–250 km and features advanced guidance systems, including active radar and infrared homing.	Military and paramilitary coercion	North Korea	Capability enhancement, Public awareness	https://mis https://en.yna.co.kr/view/AEN20200414006452325?section=nk/nk

2019	In 2019, CyberX uncovered a cyber-espionage campaign known as “Gangnam Industrial Style” targeted over 200 companies, with more than half based in South Korea. Attackers used spear-phishing emails disguised as business inquiries to deliver malware that stole credentials and exfiltrated sensitive industrial data, aiming to obtain trade secrets and intellectual property.	Cyberattack	Unidentified hacker		https://apt https://www https://www.csoonline.com/article/568783/hackers-use-free-tools-in-new-apt-campaign-against-industrial-sector-firms.html
2019	In late 2019, a cyber-espionage group dubbed RATicate launched a series of malspam campaigns targeting industrial companies in South Korea, Europe, and the Middle East. Using malicious email attachments disguised as legitimate installers, the group deployed remote access tools (RATs) and information-stealing malware like LokiBot and AgentTesla. The activity, which continued into early 2020, aimed to steal sensitive corporate data and credentials.	Cyberattack	Unidentified hacker		https://ww https://news.sophos.com/en-us/2020/05/14/raticate/
2019	Between August and November 2019, North Korea unveiled and tested the KN-25, a "super-large" multiple rocket launcher system. Across at least four tests, including a rapid-fire launch on November 28, the system demonstrated growing accuracy, a range of around 380 km, and the ability to fire in quick succession—highlighting its potential as a short-range ballistic missile system capable of overwhelming missile defenses.	Military and paramilitary coercion	North Korea	Diplomatic, Capability enhancement, Public awareness	https://ww https://missilethreat.csis.org/north-korea-tests-kn-25-in-salvo-launch/
2019	In October 2019, North Korea test-fired the Pukguksong-3, a two-stage, solid-fueled submarine-launched ballistic missile (SLBM), from waters off Wonsan. The missile reached an altitude of approximately 910 km and traveled about 450 km before landing in Japan's exclusive economic zone. Analysts estimate its potential range to be around 1,900 km if launched on a standard trajectory. In response, South Korea's Joint Chiefs of Staff confirmed the launch and identified it as a Pukguksong-type SLBM. The South Korean government expressed grave concern, viewing the test as a violation of United Nations Security Council resolutions and a provocation that undermines regional peace and stability.	Military and paramilitary coercion	North Korea	Diplomatic, Legislative and regulatory, Capability enhancement, Public awareness	https://mis https://kore https://www.globalsecurity.org/wmd/world/dprk/pukguksong-3.htm

2019	In August 2019, North Korea conducted two test launches of the KN-24, a short-range ballistic missile resembling the U.S. ATACMS. The first launch on August 10 showed a range of 400 km, followed by a second test on August 16 with a shorter flight.	Military and paramilitary coercion	North Korea	Public awareness	https://mis https://www https://en. https://en.yna.co.kr/view/AEN20190825000353325?section=nk/nk
2019	Between May and August 2019, North Korea conducted four test launches of the KN-23, a short-range ballistic missile resembling Russia's Iskander-M. The missile demonstrated ranges up to 690 km and featured a quasi-ballistic trajectory with terminal maneuverability, enhancing its ability to evade missile defenses. South Korean government condemned these launches as violations of United Nations Security Council resolutions and as actions escalating military tensions on the Korean Peninsula. The Republic of Korea's Joint Chiefs of Staff closely monitored the tests and maintained a high state of readiness.	Military and paramilitary coercion	North Korea	Diplomatic, Capability enhancement, Public awareness	https://mis https://en.yna.co.kr/vie https://en.yna.co.kr/view/AEN20190725000858325?section=national/defense
2019	In July 2019, cybersecurity analysts reported that APT10—also known as Stone Panda, menuPass, and Red Apollo—had continued targeting countries in East and Southeast Asia, including South Korea, as part of its cyber espionage operations. The Chinese state-linked group used spear phishing, backdoors, and tools like QuasarRAT and PlugX to compromise managed service providers and their clients across strategic sectors. South Korea was explicitly listed among the targeted countries, and reports indicated that APT10 had used command and control servers located in South Korea during operations earlier that year.	Cyberattack	China		https://apt https://www.cyware.com/blog/apt10-a-chinese-hacking-group-targeting-managed-service-providers-through-spear-phishing-8da0
2019	On July 1, 2019, Japan's Ministry of Economy, Trade and Industry announced tighter export controls on three key materials—fluorinated polyimide, photoresists, and hydrogen fluoride—essential for South Korea's semiconductor and display industries. South Korea filed a complaint with the World Trade Organization in September 2019, arguing that Japan's export restrictions were politically motivated and violated international trade norms.	Economic coercion	Japan	Diplomatic, Legislative and regulatory, Capability enhancement, Public awareness	https://ww https://www https://economiccoercion.com/2019/07/31/chemicals-high-tech-list-south-korea-japan/

2018	In July 2018, cybersecurity researchers from Trend Micro reported the resurgence of the China-linked Blackgear cyberespionage campaign—also known as Topgear and Comnie—targeting public sector agencies and high-tech industries in South Korea, Japan, and Taiwan. Blackgear's operators were observed using deceptive methods, such as hiding command-and-control (C&C) configurations within legitimate blog and social media posts to avoid detection and prolong access within compromised systems. The group employed custom tools like the Marade downloader and Protux backdoor, delivered through spear-phishing emails containing malicious decoy documents	Cyberattack	China		https://ww https://social.cyware.com/news/decade-old-blackgear-cyberespionage-campaign-returns-to-exploit-social-media-sites-for-cc-communication-13e3204a
2018	In March 2018, McAfee reported on "Operation Honeybee," a targeted cyber espionage campaign focused on inter-Korean affairs, particularly humanitarian aid efforts in North Korea. Believed to be run by a nation-state actor, likely Korean-speaking, the campaign used spear-phishing emails with malicious documents referencing North Korean political topics. These documents deployed malware such as a new SYSCON backdoor variant and a dropper named MaoCheng, sometimes disguised as legitimate files. The campaign targeted entities in South Korea, Southeast Asia, and the Americas, including NGOs and international organizations.	Cyberattack	Unidentified hacker		https://ww https://www https://attack.mitre.org/campaigns/C0006/
2018	Since 2018, the threat group known as Wassonite, identified by Dragos, has been targeting industrial control system sectors across East Asia, including South Korea, Japan, and India. The group uses nuclear energy-themed spear-phishing emails written in Korean to deliver malware such as AppleSeed, a backdoor capable of taking screenshots, logging keystrokes, and executing remote commands. Although Wassonite shares some technical overlaps with North Korea's Lazarus Group, there is no definitive attribution.	Cyberattack	North Korea		https://apt https://malp https://www.dragos.com/threat/wassonite/
2018	In July 2018, The Diplomat reported that North Korea was operating over 160 propaganda websites—including news, tourism, and community platforms—with the goal of spreading pro-North Korean ideology and cultivating sympathizers, particularly in South Korea. A Seoul-based think tank, the Korea Institute of Liberal Democracy, estimated that Pyongyang had around 7,000 agents dedicated to these efforts, including 300 specialized in manipulating South Korean online discourse. These agents used stolen South Korean identities to infiltrate online communities and influence public opinion through posts, videos, and comments.	Narrative and information campaigns, Foreign interference	North Korea	Legislative and regulatory, Capability enhancement, Public awareness	https://the https://www https://www.refworld.org/reference/annualreport/freehou/2018/en/122276

2017	In December 2017, South Korea's NIS attributed a cyberattack on the Bithumb cryptocurrency exchange to North Korean hackers, who stole $7 million in digital assets (later valued at $82.7 million) and the personal data of 30,000 users. The hackers also demanded a $5.5 million ransom. In response, the South Korean government formed a special task force to address cryptocurrency security and regulation, while the Korea Communications Commission fined Bithumb for inadequate data protection. These actions marked the beginning of stricter oversight of the country's crypto sector.	Cyberattack, Economic coercion	North Korea	Legislative and regulatory, Capability enhancement, Public awareness	https://ww https://mon https://www.reuters.com/article/us-southkorea-northkorea-cryptocurrency/south-korea-says-north-stole-cryptocurrency-worth-billions-of-won-last-year-idUSKBN1FP0EW/
2017	In March 2017, shortly after South Korea finalized a land-swap deal with Lotte Group to deploy the U.S. THAAD missile defense system, Chinese authorities reportedly issued unofficial instructions to domestic travel agencies to suspend group tours to South Korea. Although Beijing denied issuing a formal travel ban, South Korean industry sources confirmed a sudden and sharp decline in Chinese group tourism—Chinese tourist arrivals fell from approximately 590,000 in February to 360,000 in March, according to data from the Korea Tourism Organization. South Korean government lodged diplomatic protests but refrained from public accusations of retaliation.	Economic coercion	China	Legislative and regulatory, Capability enhancement, Public awareness	https://ecc https://www https://www.reuters.com/article/%20world/south-korea-complains-to-wto-over-china-response-to-missile-system-idUSKBN16R03D/
2017	On September 3, 2017, North Korea conducted its sixth and most powerful nuclear test at the Punggye-ri test site, claiming it had successfully detonated a hydrogen bomb capable of being mounted on an intercontinental ballistic missile (ICBM). The explosion triggered a magnitude 6.3 earthquake, signaling a yield estimated between 100 and 250 kilotons. The test marked a major escalation in North Korea's weapons program and drew strong condemnation from South Korea, which responded with live-fire drills, lifted missile restrictions in coordination with the U.S., and called for tougher international sanctions.	Military and paramilitary coercion	North Korea	Diplomatic, Military and paramilitary, Capability enhancement, Public awareness	https://ww https://www https://ww https://thediplomat.com/2017/09/south-korea-carries-out-live-fire-drill-after-north-korean-nuclear-test/
2017	In 2017, North Korea tested the Hwasong-12 (KN-17) intermediate-range ballistic missile multiple times, with notable launches on May 14, August 29, and September 15. These tests demonstrated significant advancements in range and capability, with two missiles flying over Japan and landing in the Pacific Ocean. The missile is believed to have a potential range of up to 4,500 km, putting U.S. bases in Guam within reach. South Korea responded with live-fire drills, joint exercises with the U.S., and accelerated its missile defense and retaliation strategies, condemning the tests as direct provocations and violations of UN Security Council resolutions.	Military and paramilitary coercion	North Korea	Diplomatic, Military and paramilitary, Capability enhancement, Public awareness	https://mis https://www.washingtc https://missilethreat.csis.org/south-korea-conducts-live-fire-drills-us-eases-missile-restrictions/

2017	In July 2017, North Korea conducted two tests of the Hwasong-14 (KN-20) intercontinental ballistic missile (ICBM), marking its first demonstrated capability to strike parts of the continental United States. The first test on July 4 flew about 930 km, reaching an altitude of 2,800 km, while the second on July 28 reached 3,700 km in altitude and traveled 1,000 km, suggesting a potential range of over 10,000 km. In response, South Korea conducted joint live-fire drills with the U.S. and moved to enhance its missile defense, including accelerating the deployment of the THAAD system.	Military and paramilitary coercion	North Korea	Diplomatic, Military and paramilitary, Capability enhancement, Public awareness	https://mis https://www https://thediplomat.com/2017/07/north-koreas-icbm-celebration-concert-reveals-never-before-seen-missile-imagery/
2017	In 2017, North Korea conducted two tests of the Pukguksong-2 (KN-15), a solid-fuel, road-mobile medium-range ballistic missile (MRBM). The first successful launch occurred on February 12, followed by a second on May 21, both reaching altitudes over 500 km and landing in the Sea of Japan.	Military and paramilitary coercion	North Korea	Diplomatic, Legislative and regulatory, Capability enhancement, Public awareness	https://mis https://www http://edition.cnn.com/2017/02/11/asia/north-korea-missile/
2017	In May, 2017, North Korea test-fired the KN-18 (Scud MaRV), a short-range ballistic missile equipped with a maneuverable reentry vehicle (MaRV), from a site near Wonsan. The missile flew approximately 450 km before landing in the Sea of Japan. This test demonstrated North Korea's attempt to improve missile accuracy and evade missile defenses using a guided, finned warhead. In response, South Korea's Joint Chiefs of Staff condemned the launch as a violation of UN Security Council resolutions and a serious threat to regional stability, emphasizing the need for continued vigilance and international pressure on Pyongyang.	Military and paramilitary coercion	North Korea	Diplomatic, Legislative and regulatory, Capability enhancement, Public awareness	https://mis http://www https://www.globalsecurity.org/wmd/world/dprk/kn-18.htm
2016	In August 2016, China began imposing informal restrictions on South Korean entertainment and cultural exports, including K-pop concerts, TV shows, and celebrity advertising, in what has become widely referred to as the "K-pop ban" or "Hallyu ban." The restrictions followed South Korea's July 2016 decision to deploy the U.S. THAAD missile defense system, which Beijing claimed threatened Chinese national security.	Economic coercion	China		https://eco https://www.cnbc.com/2016/11/23/china-korea-feud-over-thaad-is-hurting-k-pop-in-mainland-market.html

2016	In December 2016, the Chinese government began a coordinated campaign of regulatory crackdowns, inspections, and indirect pressure on South Korea's Lotte Group, a major conglomerate operating retail and entertainment businesses across China. This pressure followed Lotte's decision to provide land to the South Korean government for deployment of the U.S. THAAD missile defense system. By March 2017, 74 out of 99 Lotte stores in China were shut down.	Economic coercion	China		https://ecc https://www https://www.koreatimes.co.kr/opinion/editorial/20170917/ed-lottes-pullout-from-china
2016	In 2016, between April and October, North Korea conducted eight launch attempts of the BM-25 Musudan (Hwasong-10) intermediate-range ballistic missile. Most of these tests failed, but one launch in June was partially successful, demonstrating a potential range of over 3,000 km. The South Korean government strongly condemned the launches, stating they were clear violations of UN Security Council resolutions and serious threats to regional and international security. The Joint Chiefs of Staff closely monitored the tests and emphasized readiness, while the Ministry of Foreign Affairs coordinated with allies to increase diplomatic and economic pressure on North Korea.	Military and paramilitary coe	North Korea	Diplomatic, Legislative and regulatory, Capability enhancement, Public awareness	https://mis https://kore https://koreajoongangdaily.joins.com/2016/10/16/politics/Musudan-missile-test-fails-explodes-on-launch/3025001.html
2016	In 2016, North Korea launched the No-Dong (Hwasong-7) medium-range ballistic missile twice — once in August and again in September. The South Korean government strongly condemned both launches, calling them clear violations of UN Security Council resolutions and serious threats to regional peace and security. The Joint Chiefs of Staff emphasized military readiness in response, while the Ministry of Foreign Affairs urged North Korea to cease provocations and adhere to international norms.	Military and paramilitary coercion	North Korea	Diplomatic, Legislative and regulatory, Capability enhancement, Public awareness	https://mis https://editi https://www.nytimes.com/2016/08/03/world/asia/north-korea-missile-test.html
2016	In 2016, North Korea conducted two nuclear tests—the first on January 6 and the second on September 9. These marked its fourth and fifth nuclear tests, with the latter being its most powerful to date at the time, estimated at around 10–12 kilotons. The South Korean government strongly condemned both tests, calling them grave violations of UN Security Council resolutions and direct threats to regional and global security. In response, the Joint Chiefs of Staff heightened military readiness, while the Ministry of Foreign Affairs worked closely with allies and the United Nations to coordinate a firm international response. This included pushing for and supporting the adoption of UN Security Council Resolutions 2270 and 2321, which significantly strengthened sanctions against North Korea.	Military and paramilitary coercion	North Korea	Diplomatic, Legislative and regulatory, Capability enhancement, Public awareness	https://ww https://www https://ww https://sgp.fas.org/crs/nuke/IN10428.pdf

2016	In 2016, North Korea conducted at least three test launches of the Pukguksong-1 (KN-11) submarine-launched ballistic missile (SLBM), with the most notable and successful test occurring on August 24, when the missile flew about 500 km into Japan's Air Defense Identification Zone. This demonstrated significant progress in North Korea's underwater launch capability and second-strike potential.	Military and paramilitary coercion	North Korea	Diplomatic, Capability enhancement, Public awareness	https://mis https://www.bbc.com/news/world-asia-37171608