Democratic People's Republic of Korea (DPRK)

January 2018

Chief of State: Kim Jong Un

Government: The Korean Workers' Party (Communist)

Capital: Pyongyang

National Holiday: 9 September, 15 August[1]

GDP by sector: Agriculture (25.3%), Industry (41.1%), Services (33.6%)

Export Partners: China (85.6%), India (3.5%), Pakistan, Thailand, Burkino Faso, Saudi Arabia, Chile, Brazil, Turkey and Hong Kong[2]

Import Partners: China (90.3%), India, Russia, Philippines, Singapore, Mexico, Ukraine, Peru, Germany, Switzerland and Senegal[3]

Exports: Minerals, metallurgical commodities, manufactures, textiles, agricultural and fishery products

Imports: Petroleum, coking coal, machinery, textiles, grain[4]

Conflict areas: South Korea, US, Japan

Major Religions: Buddhist, Confucian, Christian, syncretic Chondogyo, government-sponsored religious groups[5]

Current Landscape

International Relations

North Korea's foreign relations are defined by recent and ongoing conflicts with its neighbors and the rest of the world. The country was created in 1948 after the Second World War when Soviet leadership installed a Soviet military officer (who had received his formal education in China) as the leader of the new country (Kim Il-sung)[6]. A tightly controlled communist state manifested under Kim Il-sung, who had a very carefully engineered "cult of personality" developed around him[7]. Kim Il-sung was succeeded by his son Kim Jong-il, who was similarly succeeded by his own son Kim Jong-un, he present-day leader. The DPRK is largely cut off from the rest of the world, its isolation only worsening after the collapse of the Soviet Union in 1991. The country now relies heavily on fuel and food aid from China. It is still officially at war with South Korea and has a deep distrust of Japan. North Korea also feels threatened by the US due to the US' relationship and military protection of South Korea. Perceived and actual threats from external influences are a very real concern for the DPRK, who sees the development of nuclear weapons as access to regional leverage and as a US deterrent. International sanctions promoted by the United States government have had an impact on the DPRK nuclear programs in the past, but not enough to have stopped it altogether. China is a primary economic influencer on the DPRK. Although China has been in favour of preventing the Korean peninsula from developing nuclear weapons, it does not want to undermine the DPRK state. China does not

1. Founding of the DPRK was on 9th September 1948 and Independence from Japan was on the 15th August 1945
2. https://www.cia.gov/library/publications/the-world-factbook/geos/kn.html
3. https://www.cia.gov/library/publications/the-world-factbook/geos/kn.html and http://news.sky.com/story/which-countries-trade-with-north-korea-11021304
4. https://www.cia.gov/library/publications/the-world-factbook/geos/kn.html
5. Ibid
6. http://www.scmp.com/article/727755/kim-il-sungs-secret-history
7. https://www.theguardian.com/world/2015/feb/16/north-korea-kim-jong-il-birthday

ANOMALI®

want to destabilize the North Korean government as this would create instability on its borders, and they are trying to prevent increasing numbers of refugees and defectors entering China. North Korea is also a strategic buffer between China and Western influenced South Korea.

Internal security posture

Since its inception, North Korea's internal dynamics have been shaped by pervasive totalitarian control mechanisms. Deep suspicion runs throughout North Korean society. This has only been continued under the auspices of present day leader Kim Jong-Un. The people of the DPRK have experienced many violations of their human rights as defined under the United Nations charter[8]. Approximately 120,000 people are being held in political prison camps, many of them simply guilty by association (for being related to people that have been accused of wrongdoing or are deemed a threat to the state). Most people are denied access to the internet and international phone calls[9]. Those that have a computer and access to the internet are also likely to be using state-approved technology, including the linux-based "red star" operating system, with Internet provided by the "Kwangmyong network"[10] [11]. This way files can be watermarked and distribution of media through USB can be monitored. All domestic media outlets are owned by the state. Most forms of communication are also observed and reported on by a large network of informants for the State Security Department (SSD). Executions and public killings are perpetrated against defectors, dissenting individuals and any kind of "anti-DPRK" crime without judicial process[12]. What citizens see, hear, think and say is influenced and controlled by the DPRK government[13].

Economy

The DPRK publishes data on its economy only rarely[14]. However, a report from the Bank of Korea indicates real annual GDP increased by 3.9% in 2016[15]. The DPRK government reportedly directs over 20% of GDP towards its military[16]. Trade between South Korea and North Korea dropped 87.7% and then ceased altogether in 2016 due to the shutdown of the Kaesong industrial complex[17]. China has been North Korea's main trading partner for over a decade in both imports and exports. China has renewed efforts behind international sanctions and ordered North Korean-owned companies operating in China to close by January 2018[18]. Overall trade between China and North Korea appears to have slowed in September as exports to the DPRK fell 6.7% and imports fell 37.6%. Malaysia, the Philippines, and Thailand have also slowed or halted trade with the DPRK. Because of its dependence on China for its overall economic health, access to resources and funds to keep the state going is a primary security concern.

National Cyber-Strategy

North Korea's resource constraints, historic geopolitical influences, and regional ambitions makes an advanced cyber capability an attractive investment. It is the continuation of the DRPK's already existing asymmetric strategy. Operation Desert Storm may have influenced the DPRK's initial decision to pursue the development of tactics in cyber-space[19]. The lucrative nature of cybercrime has also not gone unnoticed by the regime, often cited as the motivation behind attacks on global financial institutions. Cybercrime, whether in highly targeted campaigns, use of ransomware or targeting cryptocurrencies is one way for the state to generate funds and evade the economic impact of international sanctions. Cyber-espionage, internally and on foreign adversaries, is also in alignment with the state's deeply suspicious and controlling culture.

8. https://www.hrw.org/world-report/2016/country-chapters/north-korea
9. https://www.amnesty.org/en/countries/asia-and-the-pacific/north-korea/report-korea-democratic-peoples-republic-of/
10. Download the "Red Star" OS: http://www.openingupnorthkorea.com/downloads-2
11. https://github.com/mandatoryprogrammer/NorthKoreaDNSLeak
12. https://www.state.gov/documents/organization/160466.pd
13. help to free information in North Korea: http://www.flashdrivesforfreedom.org/
14. http://www.nkeconwatch.com/north-korea-statistical-sources/
15. http://www.nkeconwatch.com/nk-uploads/GDP_of_North_Korea_in_2016_f.pdf
16. http://www.news.com.au/world/asia/north-korea-spends-whopping-22-per-cent-of-gdp-on-military-despite-blackouts-and-starving-population/news-story/c09c12d43700f28d389997ee733286d2
17. https://www.cia.gov/library/publications/the-world-factbook/geos/kn.html
18. http://www.aljazeera.com/news/2017/09/china-close-north-korean-firms-sanctions-170928133806365.html
19. https://csis-prod.s3.amazonaws.com/s3fs-public/legacy_files/files/publication/151216_Cha_NorthKoreasCyberOperations_Web.pdf

Intelligence and Cyber Services

The State Affairs Commission, which took over the National Defence Commission, appears to supervise and provide guidance on defence and intelligence matters. The commission reports directly to Kim Jong-Un. Other agencies, such as the SSD, are subordinate to and report to the commission.

State Security Department (SSD)/ Ministry of State Security (MSS) or "bowibu"

Chief Commander:	General Kim Won-Hong[20]
Areas of Concern:	Internal security and intelligence agency, surveillance of political and economic crimes
Branches:	7th Bureau (Oversees political prisons), 16th Bureau (electronic surveillance)[21]
Campaigns:	Surveillance of civil society through Koryolink (North Korea's mobile network), Kwangmyong network (Intranet) and "Red Star" computer operating system.

Reconnaissance General Bureau (RGB) (Unit 586 or Chongch'al Ch'ongguk)[22]

Head:	Kim Yong-chol[23], U Cho Il (Director of 5th Bureau[24])
Location:	Hyongjesan-Guyok, Pyongyang, DPRK; Nungrado, Pyongyang, DPRK[25]
Areas of Concern:	Overseas intelligence, IT Operations/Cyber (has been accused of training proxy groups such as Hezbollah in Lebanon, Syria and Iran), SIGINT
Branches:	110 Research Center, 1st Bureau (Operations), 2nd Bureau (Reconnaissance, Sniper brigade – Special Forces), 3rd Bureau (Foreign Intelligence), 4th Bureau, 5th Bureau (Inter-Korean), 6th Bureau (Technical), 7th Bureau (Rear Services), Bureau 121 (Cyber Warfare Guidance Bureau)[26].
Associated groups:	HIDDEN COBRA, Lazarus/DarkSeoul (believed to operate under Bureau 121)
Campaigns	Troy, DarkSeoul, Sony, Bangladesh Central Bank, WannaCry[27]

The Third Floor (Office 39 or Central Committee Bureau 39)[28]

Head:	Jon Il-Chun[29]
Created:	1974
Location:	Second KWP Government Building (Ch'o'ngsa), Chungso'ng, Urbon Tower (Dong) Chung-Guyok (Central District), Susong Street Kyongrim-Dong. Pyongyang PRK Chunggwang Street, Pyongyang PRK[30]

20. https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/653726/northkorea.pdf
21. http://www.nkleadershipwatch.org/state-security-department/
22. https://www.nknews.org/2017/05/on-the-great-leaders-secret-service-north-koreas-intelligence-agencies/ and https://www.un.org/sc/suborg/sites/www.un.org.sc.suborg/files/informal_compilation_of_original_script_korean_of_designated_entities_and_individuals_list.pdf
23. http://www.38north.org/wp-content/uploads/2010/06/38north_SR_Bermudez2.pdf
24. https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/653726/northkorea.pdf
25. https://www.treasury.gov/resource-center/sanctions/Programs/Documents/2270.pdf and https://www.justice.gov/opa/file/897046/download
26. http://english.chosun.com/site/data/html_dir/2009/12/18/2009121800317.html, smallwarsjournal.com/blog/journal/docs-temp/654-wege.pdf, https://www.recordedfuture.com/north-korea-cyber-activity/, and http://www.38north.org/wp-content/uploads/2010/06/38north_SR_Bermudez2.pdf
27. https://www.us-cert.gov/ncas/alerts/TA17-164A, https://www.group-ib.com/blog/lazarus, https://www.swiftinstitute.org/wp-content/uploads/2017/10/SIWP-2016-004-Cyber-Threat-Landscape-Carter-Final.pdf, and https://www.theguardian.com/technology/2017/jun/16/wannacry-ransomware-attack-linked-north-korea-lazarus-group
28. http://www.bbc.com/news/world-asia-39073839 and https://www.un.org/sc/suborg/sites/www.un.org.sc.suborg/files/informal_compilation_of_original_script_korean_of_designated_entities_and_individuals_list.pdf
29. https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/653726/northkorea.pdf
30. https://www.justice.gov/opa/file/897046/download

Areas of Concern: Generate funds, manages a number of trading companies (has been accused of international criminal activity[31] including gold smuggling, narcotics and counterfeiting foreign currency)[32].

Campaigns: Is believed to be behind campaigns targeting bitcoin and cryptocurrencies to generate revenue for North Korea[33].

Activity Overview

There are three areas that appear to be important to North Korea; state power, finance, and the control of information. This can be observed in the types of cyber-attacks that the RGB and Office 39 have been accused of engaging in. The enormous amount of pressure and insecurity caused by international sanctions can be tentatively linked to why the DPRK seems to target financial systems and cryptocurrencies. The state has a cultural tendency to eliminate anti-DPRK rhetoric, foreign propaganda, and imprison or execute dissenting individuals. This is in alignment with the type of destructive "wiper" malware observed that seeks to eliminate information as well as steal it. It would not be far-fetched to assume that the need to develop nuclear weapons for political leverage would be mirrored in cyber-space to increase state power.

The Lazarus Group in "Operation Blockbuster," as reported by Novetta, showed fairly advanced capability in attacks that sought to destroy, disrupt or steal data[34]. In 2016 the same group was accused of initiating the attack against the Bangladesh Central Bank and the SWIFT network[35]. They have also been accused of targeting South Korean ATMs to steal banking information[36]. More recently they have been accused of carrying out the WannaCry ransomware campaign, of which further propagation was prevented by British researcher Marcus Hutchins[37]. US-CERT reported on malware hitting South Korea called "DarkSeoul" which, whilst described as low in sophistication, was high damage because of the "wiper" functionality[38].

Organised Crime

The DPRK government has a long history of being accused of propagating illicit activity. It is described as a "criminal sovereignty" due to how it organises illegal activity using the "tools of the state"[39]. It hides behind non-intervention, using the proceeds to prop up the national economy and pursue its national goals. In contrast to other countries that have well established organised crime networks, in North Korea the relationship is different in that it actively pursues crime rather than simply letting it exist (and be profited from). This is why the DPRK government is more often compared to those countries that pursue a type of "warlord criminality" such as seen in Liberia and Sierra Leone[40]. In 2008 a Congressional Research Service (CRS) report for members of congress put the estimated value of North Korean criminal activity at $500 million in profits a year[41]. International sanctions have only seemed to increase the likeliness for criminality, encouraging business owners to circumvent trade restrictions by taking up smuggling routes (for example)[42].

Office 39 is believed to be the area of government that has the dedicated resources to pursue organised crime as a means to generate funds. It is believed to be involved in a number of activities including; counterfeiting money, money laundering, illegal drug production, cigarette smuggling and more. A recent report by the Global Initiative against Transnational Organised crime provides a number of examples for this active, government-controlled, criminal-political relationship. It details a history of how North Korean diplomats have been directly involved in a number of illegal activities. One diplomat, expelled from Zimbabwe

31. http://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX%3A32011R1355
32. http://www.thehigginsreport.com/uploads/5/7/9/9/57990497/the_criminal_empire_of_north_korea.pdf
33. https://www.fireeye.com/blog/threat-research/2017/09/north-korea-interested-in-bitcoin.html
34. https://www.operationblockbuster.com/wp-content/uploads/2016/02/Operation-Blockbuster-Report.pdf
35. https://securelist.com/files/2017/04/Lazarus_Under_The_Hood_PDF_final.pdf
36. http://online.wsj.com/public/resources/documents/print/WSJ_-A006-20170728.pdf
37. https://apnews.com/dc60584d4b214f0fa6eb9ef88fdf46a7
38. https://www.us-cert.gov/sites/default/files/publications/South%20Korean%20Malware%20Attack_1.pdf
39. http://ssi.armywarcollege.edu/pdffiles/pub975.pdf
40. https://www.swp-berlin.org/fileadmin/contents/products/research_papers/2014_RP13_vrr.pdf
41. https://fas.org/sgp/crs/row/RL33885.pdf
42. http://www.tandfonline.com/doi/pdf/10.1080/0163660X.2016.1232635

for smuggling Rhino horns, is now a prominent DPRK diplomat and is the UN ambassador to the United Nations (Han Tae-song). "Between 1976 and 2003, North Korea was "linked to more than 50 verifiable incidents involving drug seizures in at least 20 countries" and a "significant number" of cases involved North Korean diplomats and officials"[43] [44]. In light of the relationship, it can be assumed that the DPRK government would keep a close watch on what forms of criminality are most profitable. Cybercrime is one of those areas the regime is increasingly involved in.

One of the current trends in cybercrime, is the marked increase in different types of mining malware being sold in the underground. According to Recorded Future, this shift is indicative of criminals moving towards a low-risk, long-term means of a steady income over ransomware. This is the first significant shift since 2015 when cyber criminals seemed to gravitate towards ransomware over banking malware. This overall trend seems to have influenced the North Korean regime, as mining activity was first observed coming from the country in May 2017 shortly after the WannaCry ransomware attack[45]. FireEye has noted the interest in bitcoin; reporting three separate attacks on South Korean cryptocurrency exchanges, the use of a cryptocurrency miner and a wateringhole compromise of a bitcoin news site[46]. Their analysis of the code behind PEACHPIT, the malware used in spearphishing campaigns against the South Korean cryptocurrency exchanges, has been linked to HANGMAN malware previously attributed to North Korea[47]. The overall trend in cybercrime and the North Korean engagement in pursuing cryptocurrency as a target, is indicative of how the DPRK government sees it as a potential means of generating revenue.

Future Concerns

North Korea's culturally-embedded, high-levels of suspicion, sensitivity to information and need for funds only point to further attacks in the future. The financial sector (including cryptocurrency) is most at risk alongside those organizations that report on the country's internal affairs, embarrass the leadership or have links to defectors[48]. The DPRK's natural state adversaries are South Korea, Japan, and the United States

South Korea

North Korea is still officially in a war with South Korea, and its relations have deteriorated over the last year with the closure of Kaesong Industrial complex. The perceived threat from South Korea is evidenced by it requiring its own sub-unit within the RGB (5TH Bureau). Offensive cyber activity against South Korea has been ongoing for some time and has increased over the last ten years[49]. This is unlikely to stop. North Korea is likely to be keenly interested in the military cooperation between South Korea and its neighbors, including the United States. Therefore, the types of attacks levied against South Korea are likely to be multifaceted, for criminal or espionage purposes.

Japan

The occupation of Korea by Japan before the Second World War underlies the deep-seated distrust between Japan and North Korea. North Korea has kidnapped up to as many as 880 Japanese citizens (although the official figure is 17)[50]. Japan has sided with the Trump administration against the DPRK, and the country is home to a number of American military bases and up to 50,000 military personnel[51]. Recently the DPRK has threatened Japan and the US jointly following the imposition of new UN sanctions. The DPRK has even gone as far as to fire a medium-range ballistic missile over the Japanese island of Hokkaido[52]. Japan is threatened by this behavior, and has been investing in defensive measures ever since the Sony attack in 2014. Because of the anti-Japanese sentiment in North Korea, Japan is a very attractive and likely target for destructive cyber activity directed from the DPRK.

US

The United States has been an adversary to the DPRK since its inception. Because North Korea was a part of the communist bloc during the cold war, the United States has always been seen as a perceived threat to its existence. The US currently supports and is allied with two of North

43. http://globalinitiative.net/wp-content/uploads/2017/09/tgiatoc_diplomats_and_deceit_dprk_report_1868_web_.pdf
44. https://www.hrnk.org/uploads/pdfs/SCG-FINAL-FINAL.pdf
45. https://go.recordedfuture.com/hubfs/reports/cta-2017-1011.pdf
46. https://www.fireeye.com/blog/threat-research/2017/09/north-korea-interested-in-bitcoin.html
47. https://www.fireeye.com/content/dam/fireeye-www/global/en/blog/threat-research/FireEye_HWP_ZeroDay.pdf
48. https://go.recordedfuture.com/hubfs/reports/cta-2017-1011.pdf
49. https://jsis.washington.edu/news/north-korea-cyber-attacks-new-asymmetrical-military-strategy/
50. https://www.ncnk.org/resources/briefing-papers/all-briefing-papers/overview-north-korea-japan-relations
51. https://www.nytimes.com/2017/08/09/world/asia/north-korea-guam-japan-targets.html
52. https://www.theguardian.com/world/2017/sep/14/north-korea-threat-sink-japan-us-ashes-darkness

Korea's main adversaries: South Korea (who the DPRK is at war with) and Japan. Furthermore, the US is behind the international systems implementation of sanctions designed to hurt the DPRK economy and pressure them to halt progress in nuclear weapons. Overall, the US is an enemy as well as an ally to enemies, and this outlook is unlikely to change in the near future. Consequently, any opportunity to gain insight through espionage or to conduct well-orchestrated attacks are highly likely. This may occur against regional infrastructure in areas like Guam, which is also home to US military personnel and nuclear-equipped aircraft[53].

53. https://www.nytimes.com/2017/08/09/world/asia/north-korea-guam-japan-targets.html