Sanctions Practitioners
Compliance Trainers

Compliance & Capacity Skills
International, LLC

12 July 2019

Digital Methods for Circumventing UN Sanctions
A Case Study of the Democratic People's Republic of Korea's Cyber Force

By Ashley Taylor

Introduction

The cyber sphere is a new frontline in the implementation and circumvention of UN sanctions. Because the Internet provides a virtual space for instantaneous communication and transaction, it inherently opens cheaper and unregulated avenues for rogue actors to violate international norms. Illicit uses of digital technologies outpace the advancements of licit technologists, who generally do not prioritize international security in their business.

The Democratic People's Republic of Korea (DPRK) in particular has become increasingly adept at employing digital tools to circumvent sanctions. They have developed digital techniques to generate revenues to fund their illegal proliferation efforts, gain intelligence and technical know-how, and harm the business and reputation of their foreign adversaries, including to disrupt those that monitor the implementation of the DPRK sanctions regime adopted with UN resolution 1718 in October 2006. Kim Jong-un recently boasted that "cyber warfare, along with nuclear weapons and missiles, is an 'all-purpose sword' that guarantees our military's capability to strike relentlessly."[1] A North Korean military defector has reported that the cyber force is viewed as the strongest weapon in the "Secret War"[2] and its members are considered part of the elite, being one of few well-paid positions.

Where will they go from here? Evidence suggests that North Korean state actors and non-state proxies are increasingly making use of new anonymizing technologies like cryptocurrencies, the dark web, encryption, and advanced hard-to-detect cyberattacks. The UN Panel of Experts Report on the DPRK estimated they have earned $571 million USD from stealing cryptocurrencies alone.

[1] according to a report by Washington-based think tank the Centre for Strategic and International Studies

[2] https://www.reuters.com/article/us-sony-cybersecurity-northkorea/in-north-korea-hackers-are-a-handpicked-pampered-elite-idUSKCN0JJ08B20141205

This case study will first focus on the origins of North Korea's cyber force by looking at documented attacks conducted using traditional hacking methods, outline tactics observed from past intrusions and attacks, and look at reports on North Korean adaptations to more advanced technologies. This article will conclude with recommendations of cybersecurity measures and regulatory guidelines to be adopted.

Cybersphere and UN Sanctions: The Regulatory Context

Technology entrepreneurs exploiting the richly rewarding disruptive and transformative potential of digital technologies were historically incentivized by soft regulatory standards. However, recognition of the potentially harmful impact of these new technologies to political, social, and security matters is now mobilizing European and US regulators to intervene against, and discipline, technology companies that are trespassing national and international standards.

While national cyber-regulatory frameworks have been adopted by 138 countries, most focus on domestic crime-prevention while remaining blissfully detached from the international security implications of a weaponized cybersphere.[3] The UN Security Council has addressed cyberthreats only in a spotty and inconsistent manner, despite having 20 years worth of reports and evidence about how digital technology has been driving conflicts and benefitted sanctioned actors. To date, only the Financial Action Task Force (FATF) is gradually amending its 40 recommendations to prevent and protect against digital variations of anti-money laundering (AML), counterterrorism financing (CTF), and nonproliferation financing.

There have been some unilateral steps in the direction of cyber sanctions. For example, the US sanctioned two cryptocurrency accounts owned by Iranian individuals, and the EU has released some guidance, including a cyber diplomacy toolkit. Yet these steps are far from the comprehensive approach that is needed.

As outlined in the following sections, North Korea's diverse use of digital technologies exemplifies the multifaceted challenge of enforcing sanctions in the cyber sphere. The DPRK's demonstrated ability to conduct monumental, but barely perceptible, and cheap cyber raids on data or financial assets belonging to governments, companies, and individuals is a huge motivator to adopt offensive digital and information warfare tools. There is also a need for industry leaders and policy makers to address the role that seemingly innocuous civilian applications like cryptocurrencies or online identity-shields play.

[3] https://unctad.org/en/Pages/DTL/STI_and_ICTs/ICT4D-Legislation/eCom-Cybercrime-Laws.aspx

At the international level, existing sanctions against North Korea do not categorize abuses of the international cyber-infrastructure as sanctionable acts. Considering the nebulous nature of addressing cyber threats related to North Korea, passive government and industry leaders run the risk of:
(1) North Koreans attacking or preparing to attack their computer systems, leading to loss of revenue, critical data, and operational capacities;
(2) compliance failures and reputation loss from enabling North Korean actions that result in sanctions violations; and
(3) being left behind in efforts and initiatives to regulate the technology industry, with potentially far-reaching implications for their economy and national security.
Additionally, in regions where the cybersecurity industry and government oversight do not have well-established pathways for knowledge sharing and collaboration, there is less potential to respond effectively and/or responsibly to cyber-attacks.

DPRK Cyber Networks

It is estimated that the DPRK has up to 6,000 cyber warriors, organized into different groups known as Lazarus, Bureau 121, Hidden Cobra, Bluenoroff, Apt 38, TEMP.Hermit, and Andariel. A major contributor to North Korea's cyber arsenal is the funneling by North Korea's education system, from a young age, of the best technical minds in science and mathematics towards computer science and engineering courses, and eventually to Pyongyang University of Science and Technology (PUST), the only foreign funded university in the country. PUST was opened in 2010 with a contract between the North Korean government and the North East Asia Foundation for Education and Culture (NAFEC). Some foreign volunteers work at the university, while others come for a few weeks to teach a course.

In 2015, North Korean defector Jang Se-yul, who says he was part of Pyongyang's cyber warfare command, reported that the trainings at PUST prepare students for hacking. PUST rejects these allegations, claiming inadequate evidence. Regardless, it is true that a byproduct of learning computer engineering and security is acquiring the foundation for how to hack. Computer science basics, such as how to write computer programs, create algorithms (procedures for analyzing data) and interface with a computer operating system are also integral to hacking. Any legitimate student of cyber security eventually will conduct 'white hat' hacking experiments, where they attempt to break into information networks so as to expose their vulnerabilities.

Once properly trained, some students join the cyber force located in North Korea, while others join overseas teams to conduct hacking efforts, or go abroad to start front companies to aid in the circumvention of sanctions.[4] Private security firms have analyzed the internet activities of

[4] https://www.reuters.com/article/us-sony-cybersecurity-northkorea/in-north-korea-hackers-are-a-handpicked-pampered-elite-idUSKCN0JJ08B20141205

DRPK-based users to understand the network of supporters abroad, and found evidence of supporters physically located or living in Bangladesh, China, India, Indonesia, Kenya, Mozambique, Nepal and Thailand.[5]

A major weapon for this pipeline of talent is the use of the most advanced technologies, such as anonymizing techniques that enable anonymous attacks, and cryptocurrencies, which enable new ways to generate funds and secretly transfer hacked gains. Demonstrating its ability to adopt the latest cyber trends, the DPRK hosted a blockchain and cryptocurrency conference at PUST in April 2019, organized with the help of a UK entrepreneur.[6]

The most important anonymizing technologies North Korea uses, and ancillary ones, are explained in the following table.

Technologies for Anonymous Attacks and Sanctions Circumventions

technologies	Description & use by the DPRK
Intranet	a closed network not connected to the free and open world wide web; an internal collection of networked servers and computers that only allows access to certain pages and files (e.g. the DPRK Internet infrastructure is an Intranet called Kwangmyong that is only accessible from inside North Korea's borders)
dark web	the portion of the Internet which is not indexed by popular search engines such as Google or Yahoo, meaning the pages are not easy to discover unless the user knows where to look; where illegitimate activity can occur undetected, such as forums and marketplaces for acquiring weapons, stolen intellectual property, etc.
Tor	a browser that allows access to the dark web. It can be freely downloaded by anyone who has access to the Internet
encryption	encoding data with secret codes only possessed by the intended participants. It is used for encrypted messaging, so that the information can pass through Internet protocols undetected, and it is also used as a fundamental design element in creating cryptocurrencies. The North Koreans used the Chinese encrypted messaging app WeChat to coordinate ship-to-ship transfers

[5] https://www.recordedfuture.com/north-korea-internet-usage/

[6] https://www.independent.co.uk/life-style/gadgets-and-tech/news/north-korea-cryptocurrency-blockchain-conference-pyongyang-a8643391.html

technologies	Description & use by the DPRK
cryptocurrencies	a type of digital money, where each version has specific rules for how coins come into existence and how they can be used. It uses encryption to make the coins hard-to-fake and provide anonymity to the users, meaning real world identity is not necessary to acquire or trade them. Each cryptocurrency, of which there are thousands, has its own rules and market demand for obtaining coins. Transactions are recorded on a shared ledger, called blockchain
blockchain	a database that is comprised of a specific cryptocurrency's ledger of transactions. Once entries are made, they are very difficult/costly to change, thus it is a useful way to track 'trusted' data over time. Each transaction is forever visible to the entire network. The native currency of each blockchain is generally required to interact on the network. These blockchain networks and their currencies can be public, such as Bitcoin, or private, only useable by a select group
virtual private network (VPN)	a service that allows a user to create a private portal to anonymously access the public internet, so their data, information, and access to the web cannot be tracked and/or content cannot be observed or censored
virtual private server (VPS)	a service for hosting web applications that does not require the use of a third-party server such as Google, Microsoft, or Amazon
transport layer security (TLS)	an additional level of encryption added to information networks to ensure that all data transferred over the network is difficult to obtain/observe
social media	online neighborhoods, or the places in the digital sphere where people interact. In the case of the DPRK, social media is useful to promote their propaganda to their supporters abroad, as well as to create fraudulent accounts to promote front businesses and accomplish other hacking tactics without disclosing their real identity

Starting in April 2018, security researchers found a 1,200% increase in the use of these private Internet services, which aid North Koreans in their research and attacks. These tools, combined with the DPRK's highly censored Intranet Kwangmyong, limit the ability of foreign cyber intelligence and security agencies to fully understand North Korea's cyber force.[7]

[7] https://krebsonsecurity.com/2014/12/the-case-for-n-koreas-role-in-sony-hack/#more-29249
internet usage report

The North Koreans do still use the public web, especially social media, to coordinate sanctions circumventions. They have been switching away from Western social networks and media since late 2017 in favor of Chinese versions, where they more easily assimilate without being identified. A notable exception is the continued usage of LinkedIn, which likely remains useful to create false personas (i.e. one with no North Korean affiliations) to promote front companies, create relationships with potential cyber-attack victims and understand how to best hack them, and to promote business opportunities such as new digital currencies. These incidences are further outlined in the next sections.

Techniques used by DPRK to Circumvent Sanctions

The following table is a description of the techniques employed by the North Koreans in a variety of attacks.

Techniques	Description
malware	hackers install a harmful computer program on the victims' computer that can accomplish any number of goals, such as giving the hacker access to the computer
botnet	when hackers take over many computers and build an infrastructure for coordinating attacks that need large amounts of processing power, such as DDOS (next)
distributed denial of service (DDOS)	using many computers (often botnets) to attempt to access a certain webpage so that it is overloaded and ceases to function. The attack often aims to damage the business (e.g. inability for normal commerce to function)
phishing	sending false communications, such as a fake email, that trick users into entering their passwords on a web page owned by the hackers, and/or download a fake file that contains malware
Spearphishing	similar to phishing except that victims are more carefully targeted, after background research by the attackers, to determine what the victim will be most susceptible to, such as through creating a fake account and befriending them on social media
system vulnerability exploit	finding loopholes in infrastructure/operating systems such as Microsoft Windows that will give the hackers access to the computer. These loopholes are useful for hackers to coordinate widespread attacks on many victims at once who all use the same software with that vulnerability

Techniques	Description
virus	a computer program designed to infect computers and cause a specific outcome (e.g. destroy files, steal information) that self-propagates, meaning it finds a way to infect as many other computers as possible via the infected computer, therefore causing large scale damage in a short amount of time
cryptocurrency trading/exchanges	a thriving industry of services that allow users to transfer cryptocurrencies into other cryptocurrencies and fiat (state-backed currency). Concerning the North Koreans, these transfers can turn stolen coins into cash, and/or easily obfuscate a trail of ownership of stolen coins by switching from one cryptocurrency to another. There are many cryptocurrency exchanges that enable trading without any regulation.
cryptocurrency mining	each cryptocurrency has rules specified for how new coins can be earned, which often requires using specialized computers with powerful GPUs to process data constantly as they compete to win new coins released over a specified amount of amount of time
Initial Coin Offering (ICO)	the creation of a new cryptocurrency with a fundraiser conducted to pre-sale some portion of the coins, with promises of how the users will be able to use the coins, often with the subtext of a financial return
watering hole attack	the attacker compromises a website of interest to the intended target(s) and adds code to trick a user to go to a new webpage that will trick them into installing malware
ransomware (type of virus)	a malware that will encrypt the victims' hard drive and demand ransom in a limited time frame if they want their data to be returned and not destroyed

Specific Methods employed for Sanctions Circumvention

While the techniques described above can be standalone components of an attack or acquisition, often times they are combined together into the following methods and repeated across multiple incidences.

Methods to Harm Adversaries, Steal Information, and Sometimes Demand Ransom

North Koreans have a history of conducting cyber-attacks to harm their adversaries. They have been able to cause massive damage, such as with the case of the attack on Sony Pictures. Responding to the upcoming release of a film that portrayed the assassination of Kim Jong-un, DPRK hackers destroyed files, leaked sensitive information, such as employee pay information that led to a gender equality crisis for the company, and caused an estimated $100 million dollars in cyber related damage to the company.

As illustrated in the following table, the DPRK's attacks are evolving towards incorporating ways to generate revenue in addition to causing harm. The Wannacry virus in 2017 spread across the globe, infecting computers and encrypting all of their data. Wannacry then activated a time-sensitive demand for a ransom payment in bitcoin, if the users wanted their data back. Because bitcoins are difficult to associate with their real-world owners, it is very difficult to know how much the North Koreans actually generated from this attack. At least $140,000 USD was tracked, although the real number is probably much higher. However, the damage done to infected businesses was in the millions and often caused catastrophic outcomes, such as shutting down critical computers at UK hospitals.

Incidences (order of time)	Techniques Used	Known Harm Done
DDOS (2009)	botnet, ddos	$31 million to $46 million USD in harm
DDOS (20011)	botnet, ddos	40 websites, 820 hard drives affected
320 Dark Seoul (2013)	spearphishing, malware	destroyed data, $75 million USD in repairs
Sony Pictures (2014)	spearphishing, malware	unsuccessful ransom attempt of stolen sensitive information, then leaked the information causing reputation damage, and cost to repair computer systems ~$100 million
Korea Hydro & Nuclear Power Attack (2014)	spearphishing, malware	attacked 3,571 Korea Hydro employees and tried to destroy their PC disks. The hackers obtained and released blueprints for six nuclear power plants over six different occasions on Twitter and demanded $10 billion USD
Interpark (2016)	malware	leaked private information of 10.3 million users. attempted ransom in Bitcoin of $2.7 million USD
undisclosed companies in the defense industry (2016)	system vulnerability exploit	obtained and leaked classified data, such as aircraft blueprints

Incidences (order of time)	Techniques Used	Known Harm Done
Polish Financial Supervision Authority (2017) among other targets	watering hole attack, malware	sent banks visiting the website to an alternative page where victims were prompted to download malware. Perhaps was used in the Swift attacks (next section)
Wannacry Virus (2017)	system vulnerability exploit to insert a ransomware that encrypted files of targets computers and demanded bitcoin ransom for files	at least $140,000 USD earned in cryptocurrencies, critical damage done to businesses and institutions like UK hospitals
DPRK UN Panel of Experts	unknown	sabotaged the committee by delaying the release of their report on the DPRK

Purely Revenue Generating Methods

In recent years the North Koreans have shown a preference for generating funds with their cyber expertise. In February 2016, North Korean hackers spearphished employees of the Bangladesh Central Bank and installed malware to obtain their legitimate credentials for the SWIFT global interbank messaging system. They then compromised the Bangladesh account at the US Federal Reserve and attempted to transfer $951 million USD of the bank's funds to accounts around the world, while only managing to acquire $81 million USD. The money went to an account in the Philippines and was laundered through multiple bank accounts, a money remitting business, and casinos.[8] This same attack was attempted many other times at banks worldwide, with successful other hacks gaining $10-15 million USD each.

After these attacks, North Korean hackers began to focus their efforts on cryptocurrency exchanges, the services that act as online banks for exchanging the multitude of cryptocurrencies. Perpetrators target the digital wallets where cryptocurrency exchanges store the funds held in between transactions for clients. These wallets are very lucrative targets because they contain huge volumes of customer funds. Stealing the digital signatures (passwords) that control these wallets and re-appropriating the funds yields very significant gains.

[8] https://www.thecipherbrief.com/kim-digs-cybercrime-coin-sanctions-cant-snatch

The DPRK was responsible for 75% of globally reported cryptocurrency exchange hacks (a total of ~$882 million USD) from late 2016 to Fall 2018. This digital income is hard to trace and can therefore be used to circumvent or contravene asset freezes and other UN sanctions.

Notable Incidences (order of time)	Techniques Used	Harm Done / estimated Impacts
Bangladesh Bank cyber heist (2016)	spearphishing, malware, fraudulent Swift bank transfer	stole $81 million USD
Hacked online casinos (2016, 2017)	malware, inserted a cheat into the gambling game	unknown
Far Eastern International Bank (2017)	spearphishing, malware, fraudulent Swift bank transfer	$60 million USD transferred, but most recovered
Standard Chartered Plc - Bancomext (2018)	spearphishing, malware, fraudulent Swift bank transfer	unsuccessful attempt to hack $110 million USD, though $15 million USD was stolen from other attacks on Mexican banks
Banco de Chile (2018)	spearphishing, malware, fraudulent Swift bank transfer	$10 million USD acquired, transferred many to accounts in Hong Kong
Open Bazaar store for North Korean goods -(since 2016)	created a store to sell North Korean specialty items such as cigarettes, money, and stamps	unknown
Yazipon cryptocurrency exchange (2017)	spearphishing to gain password to the exchange account, cryptocurrency exchange	$5.3 million USD stolen
Andariel mining malware (2017)	installed malware that mined cryptocurrency on targets computer	70 onero coins, $26,000 USD earned
Coinis cryptocurrency exchange (2017)	spearphishing to gain password to the exchange account, cryptocurrency exchange	$7 million USD stolen

Notable Incidences (order of time)	Techniques Used	Harm Done / estimated Impacts
Youbit cryptocurrency exchange (2017)	spearphishing to gain password to the exchange account, cryptocurrency exchange	$5.6 million USD stolen
Coincheck cryptocurrency exchange (2018)	spearphishing to gain password to the exchange account holding a new cryptocurrency NEM Coin, cryptocurrency exchange	$534 million USD stolen
Bitthumb cryptocurrency exchange (2018)	spearphishing to gain password to the exchange account, cryptocurrency exchange	$32 million USD stolen
Interstellar, Stellar, HOLD, or HUZU (2018)	an Initial Coin Offering (ICO) for a new cryptocurrency; the name was changed many times to try to obfuscate the origins	unknown
MarineChain (2018)	an ICO for a new cryptocurrency that fraudulently claimed to sell ownership of large ships.	unknown funds earned as the project dissipated when exposed. However it points to a new means of evading sanctions on shipping by creating a new way to obfuscate the ownership of a vessel
Mining/exchanging cryptocurrencies (2015 - present)	using computers in North Korea to mine various cryptocurrencies and then convert them into usable currency, or trade for other goods	estimated $150k/$200k USD earned per year

It is clear that, over time, North Korean hackers are moving towards revenue generating attacks, especially those that take advantage of weak regulatory standards surrounding cryptocurrencies. North Koreans clearly show they are primed to take advantage of technological trends. Their cryptocurrency exchange hacks and ICOs coincide perfectly with a speculative craze in late 2017

- early 2018 when the market value of digital currencies reached its highest peak yet. The total market for these coins in 2018 fluctuated between $128.9 billion and $818.1 billion US dollars.[9]

Cybersecurity Recommendation Measures

In terms of addressing these threats, cybersecurity measures can be adopted and, where appropriate, required by regulation. The two most important areas to address for preventing cyber attacks are:

(1) Employee education of how to recognize hacking attempts like spearphishing and suspicious attachments

Regardless of the level of security of a new technology like blockchain, techniques such as spearphishing will prevail as a method of compromising systems. Two-factor authentication can reduce the impact of a breach, but it does not replace the need for education.[10] The best education program includes a curriculum showing past examples with tests where the employees can identify fraudulent appearing files / emails. Finally, the IT personnel should engage on an ongoing basis with routine 'white hat' attacks, where they try to fool employees with a simulated hacking attempt.

(2) Keeping IT system protocols in pace with cybersecurity industry standards, including staying up to date with recent cyber-attacks.

As mentioned in this report, many North Korean attacks focus on vulnerabilities in operation system protocols. IT/ security teams should stay up to date by:

- Creating strong passwords[11] and implementing a system that requires the regular changing of passwords and, if possible, use a password management system;
- Staying on top of all patch releases and applying them quickly;
- Replacing older operating systems with the latest versions;
- Maintaining up-to-date antivirus software, where appropriate, and scanning all software downloaded from the internet before executing;

[9] https://coinmarketcap.com/charts/

[10] two factor authentications is a security procedure that requires the user to verify their identity in addition to entering a password by entering in a code received to their mobile device. It is best to use an application for authentication rather than a mobile number because mobile numbers can be more easily switched to the hackers control.

[11] see https://www.us-cert.gov/ncas/tips/ST04-002 for more information on creating strong passwords.

- Restricting users' abilities (permissions) to install and run unwanted software applications and applying the principle of least privilege to all systems and services;
- Scanning for and removing suspicious email attachments. Enterprises and organizations could block email messages from suspicious sources that contain attachments;[12] and
- Enabling a personal firewall on organization workstations and configure it to deny unsolicited connection requests.

Addressing Ransomware

- Backup systems regularly, and keep an encrypted copy of recent backups off-site and off-line
- There are softwares that claim to stop ransomware by blocking the unauthorized encryption of files. Have security personnel evaluate these tools.

Regulation and Jurisdiction

In cyber security, information warfare, and related policy making, the best strategy is to be ahead of the threat. For countries and industry leaders who are awaiting guidance on the cyber component of sanctions, it is wise to take steps to ensure that digital technology companies are working to ensure sanctions violations are not happening in cyberspace, and thus pave a way for industry to progress in accordance with already defined standards of human peace and security. It is also necessary for technology companies to communicate what measures they are taking to follow UN sanctions.

The top priority is for best practices in cyber activities to be treated as their equivalent in the real world. Ultimately, there is no difference between money laundering with conventional or cyber assets. The anonymity and the novelty of these technologies enhance the potential for deceptive practices and risky actions by already sanctioned entities and new threat actors. Because of the heightened risks, due diligence practices have to be more resolute. Actors who prefer to operate within blockchain-based or highly encrypted information networks are deviating from prevalent industry practices and existing reporting requirements. Therefore, added vigilance is required for any entity engaged in arms or financial transactions, maritime or aviation transportation, and interactions with North Korean workers or diplomats, where the use of such technologically advanced platforms is suggested.

[12] For information on safely handling email attachments, see Using Caution with Email Attachments. Follow safe practices when browsing the web. See Good Security Habits and Safeguarding Your Data for additional details. Restricting these privileges may prevent malware from running or limit its capability to spread through the network

Recommended measures include:

- Insist on the full disclosure of verifiable identification, purpose of proposed transactions, and any other relevant information that would be considered in a real-world transaction;
- Clarify the rationale of the proposed activity to ensure that all economic steps serve reasonable, logical, and legitimate purposes;
- Vet all parties involved when creating new cyber ventures, ensure that funding and capital - regardless whether paid in the form of digital currency or not – is not related to any sanctions violation or derived from assets that should be blocked;
- Impose disclosure requirements for any blockchain technology-based company or venture to authenticate the legitimacy of assets, contents of digital wallets, or purposes of smart contracts;
- Share information about any attacks to the cybersecurity community and increase cooperation with research and regulation;
- Insist on professional network security protections for financial institutions and companies, including cryptocurrency issuers or exchanges, starting with malware/phishing/password education and policy to better protect the national financial system from unauthorized intrusions;
- Ensure that Web hosting companies verify that the nature of the traffic of the sites they host does not contribute to sanctions violations;
- Ensure that digital/social media companies monitor advertisements to ensure they are not contributing to sanctions violations; and
- Impose integrity obligations on operators of cloud computing facilities to maximize protection and ensure they are not hosting sanctionable activities e.g. malware.

When dealing with individuals, companies or entities already under UN sanctions:

- Block all trade of embargoed goods, components or technologies;
- Block financial accounts and digital wallets, and flag suspicious transaction reports when appropriate; and
- Deny all digital activities or access to accounts on digital technology platforms, including social media, marketplaces, apps, cloud computing and email, if there are indications that activities may contribute to sanctions violations.

Conclusion

Acknowledging the expertise of the North Korean cyber force is especially important as the international community continues to strive for a nuclear non-proliferation agreement with the DPRK. Understanding the ways via which North Korea is acquiring technologies and secretly raising funds will need to be addressed in future negotiations. For deciphering the North Koreans' next moves, it will be important to pay attention to the direction of the anonymizing technology industry, especially the cryptocurrency and encrypted technology industries, and extrapolate the types of advantages that a rogue actor could gain from having little regulation in these fields. More ideas related to how they will advance will be left to a future study.

About Ashley Taylor

	A practitioner, entrepreneur and researcher, Ashley Taylor is deeply immersed in the intersection of digital technologies and international security. Being a member of the first generation of blockchain entrepreneurs, Taylor was drawn early to the potential ramifications of encrypted communications and distributed ledger technologies on the integrity of commerce and social development. Working with tech and finance organizations, she is now actively developing a humanistic framework involving new technologies and implementation criteria that support the maintenance of international peace and security.