38 NORTH

North Korea's Illicit Cyber Operations: What Can Be Done?

BY: STEPHANIE KLEINE-AHLBRANDT
FEBRUARY 28, 2020

It should surprise no one that the DPRK is a sophisticated cyber actor. Over the past several years, Kim Jong Un's regime has earned up to $2 billion *(https://undocs.org/S/2019/691)* through illicit cyber operations, providing North Korea with a significant cushion against the effects of international sanctions imposed on it and the efforts to leverage sanctions to generate greater pressure on Pyongyang to reach an acceptable agreement on denuclearization. The proportion of revenue generated by the DPRK through cyber operations has grown in relation to income generated through other illicit activities and its ability to adapt and move into areas such as cryptocurrency and the cybercrime underground make attacks harder to prevent and trace. This essay puts forward recommendations to achieve greater success in curbing this activity. The Appendix *(https://www.38north.org/wp-content/uploads/pdf/2020-0228_SKA_NK-Cyber-Operations.pdf)* provides a historical overview of the North's illicit cyber operations and a description of the various methods Pyongyang has used to continually improve its cyber capabilities to generate revenue in evasion of sanctions.

Background

The DPRK's advanced capabilities are consistent with the country's national objectives, state organizations and military strategy *(https://www.recordedfuture.com/north-korea-cyber-activity/)*. Given the relative weakness of its conventional military, the ability to carry out asymmetric and irregular operations is key to the North's strategic objectives.

The low cost of entry and high yield, the difficulties in attribution, a lack of effective deterrents, and the international community's high level of monitoring traditional weapons capabilities—such as nuclear weapons—also make cyber capabilities a natural regime focus.

Furthermore, cybercrime is a logical extension of the country's reliance on activities to evade sanctions such as counterfeiting, smuggling of precious metal, gems and cash, arms trading, gambling and illegal shipping operations. As a consistent innovator in sanctions evasion, it would have been surprising if the DPRK didn't take advantage of the vulnerabilities inherent in cyberspace, including the anonymity it provides, to generate illicit income. North Korean cyber actors have committed dozens of cyber attacks targeting financial institutions and cryptocurrency exchanges in at least 17 countries. The United Nations Panel of Experts stated *(https://undocs.org/S/2019/691)* in its 2019 midterm report that these actors raise money for the country's weapons of mass destruction programs and that the increasing scale, capacity and sophistication of attacks show the DPRK's ability to continually adapt and develop its capabilities.

It is also worth keeping in mind that the new strategic domain of cyber is not just a question of financial crimes but also speaks to a larger set of DPRK strategic assets. These assets are applicable to cyber espionage, disruptive attacks in the United States and its allies, and the use of the internet to access prohibited knowledge and skills *(https://www.wsj.com/articles/behind-north-koreas-nuclear-advance-scientists-who-bring-technology-home-1504711605)* enabling the development of its nuclear and ballistic missile programs.

If the United States is going to have a serious approach to North Korea in the cyber domain it needs to recognize this reality and take the necessary steps to get ahead of Pyongyang's capabilities. Catch-up does not work in cyberspace where the attacker always has the advantage. Moreover, that approach needs to be integrated into the broader strategy to deal with North Korea including diplomacy, sanctions and military measures. This will require developing a coherent understanding of how to deter and respond to North Korean cyber attacks and the role and responsibilities of federal agencies in this process. However, to date, the international community's approach to North Korea continues to focus more narrowly on its WMD capabilities and a list of sanctioned commodities, while its cyber capabilities remain unaddressed.

Some Options

It is time for policymakers to devise an approach to deal with the DPRK's growing cyber capabilities by adopting measures to mitigate the country's sophisticated and lucrative attacks to gain foreign currency and evade sanctions. While private security firms and intelligence agencies prioritize North Korea's cyber attacks, policymakers lag far behind. They seem almost oblivious to the financial gains from these attacks that comprise an increasing proportion of revenue from the country's overall illicit activities as well as the North's movement into areas such as cryptocurrency and the cybercrime underground.[1] Given the characteristics of cyber, diplomacy should play a critical role in laying the groundwork for curtailing actions in this new strategic domain.[2]

It is critical that the United States develop in deed, not just word, an actual whole-of-government approach to North Korea that includes cyber. While there are questions about whether or not the National Security Council (NSC) should be "operational," the fact remains that it is the only element of government that has both the convening power and the ability to arbitrate across the entire government. Therefore, the NSC should lead a task force to address how to integrate cyber with broader North Korea policy, bringing together cyber command, the intelligence community, the US Department of State, US Department of the Treasury, and other elements of the US government.

The task force would serve three objectives. First, it would signal that Washington intends to place greater priority on this issue. Second, and more important, it would develop the array of policy options needed to integrate cyber into any strategy to deal with North Korea. One area that will require special attention is the reality that it is increasingly meaningless to attempt to structure sanctions to leverage WMD negotiations without addressing how North Korea is obtaining its funds and the knowledge to advance these programs. These issues are now all intertwined since punitive and isolating sanctions only drive DPRK to cyber operations, as opposed to deterring them from them. The Task Force would develop a multilayered strategy drawing on all instruments of US national power given that deterrence operates completely differently in the cyber domain than in military domains (see Appendix *(http://bit.ly/2Pzgujk)*). Finally, an NSC-led task force would provide an opportunity to review and assure that sufficient resources are devoted to the issue, through the intelligence community, the military and elsewhere. It would also ensure that significant efforts are directed at disrupting the virtual currency financing that the DPRK is using to continue to build its cyber infrastructure, and de-anonymizing cryptocurrency.

Energize Multilateral Diplomacy

Given that many DPRK attacks involve the most vulnerable institutions worldwide, the US government, led by the State Department, should actively engage partners, allies and other relevant countries (including in Southeast Asia) as well as industry to identify emerging technologies that North Korea could exploit to evade sanctions and facilitate cyber attacks. An example of such a technology is the dark web—a network designed for anonymity and frequented by criminals that the DPRK uses to buy and sell malware, hire hackers, launch cyber attacks and trade in virtual currencies completely undetected.

One model which could be considered in assisting other countries would be the Belt and Road Initiative (BRI) "strike teams" deployed by the United States to help educate countries and provide technical assistance, expertise and capacity building to better negotiate (and renegotiate) BRI deals with China. Interagency teams should be deployed to assist weak links identified in cyberspace as well. This approach will require making cyber a major focus in sanctions consultations with like-minded and other countries, allocate significantly more funding to this issue, and require the State Department to share information with relevant countries on attacks carried out by DPRK actors against their nationals, banks and cryptocurrency exchanges.

Law Enforcement

Efforts to build capacity, share information and encourage local law enforcement in relevant countries to investigate and take action on cyber activity are key. Law enforcement officials in countries used and targeted by DPRK cyber actors in their operations require the knowledge and tools to investigate attacks as well as shut down the infrastructure in countries being used to launch attacks. For example, Bulletproof Hosting Servers (BPHS) are hosting facilities for malicious content that can be used by the DPRK and other Advanced Persistent Threat (APT) actors to launch attacks. They generally operate in countries with lax regulations that may not have the tools to determine if BPHPs are in their country, and/or lack the will or capacity to shut them down (especially where officials have been bribed by them).

Cooperating with foreign law enforcement is also important to tackle the issue of the hundreds of DPRK programmers working abroad, many of whom are subordinate to the UN-designated Munitions Industry Department (MID). These individuals generate revenue for the DPRK through operations in China, Russia, Africa, Southeast Asia and

the Middle East (see Appendix section, "DPRK programmers study and work abroad"). Hackers are generally more adept at collaborating across geographies than law enforcement.

Cryptocurrency

Better regulation of cryptocurrency markets is essential to clarify responsibility for attacks and laundering of funds, monitoring suspicious transactions, providing governments with information on attacks, and blocking transactions from accounts controlled by or associated with sanctioned actors. While regulation is usually the task of government regulatory agencies, cryptocurrencies are designed to be financially autonomous, operate with various degrees of anonymity, and do not require interaction with fiat (government-issued) currency including the US dollar (upon which most methods of regulating currency depend).

Given these facts, self-regulation should be encouraged to bridge the gap between the status quo and future government regulatory actions and involves the cryptocurrency exchange industry adopting its own guidelines and codes of conduct, which can eventually create market pressure to adopt best practices. For examples of how this is done, see Appendix section, "Self-Regulation of Cryptocurrency." Some countries are creating a regulatory sandbox to experiment with fintech and cryptocurrency regulation such as Switzerland. A larger proportion of the State Department grant money currently dedicated to training local government officials and financial institutions in developing countries on how to better enforce sanctions regimes should be dedicated to regulatory best practices for cryptocurrency.

Information Sharing

Banks, governments, cryptocurrency exchanges and other targets have been reluctant to share information on cyber attacks despite the utility of such information in helping to thwart and reduce the damage of attacks (see Appendix section, "Need for Information Sharing"). While more information sharing has taken place in recent years, including through the Financial Services Information Sharing and Analysis Center (FS-ISAC), convincing industry and government to share information on cyber threats is still a heavy lift. The US should model such information sharing itself while supporting other countries to establish inter-agency working groups to enable policymakers, regulators, supervisors, law enforcement authorities and other relevant authorities to cooperate with each other to develop and implement effective policies, regulations,

and other measures to address cyber attacks with a view to addressing security gaps, developing regulatory approaches to cryptocurrencies, and sharing information on investigations. Public-private partnerships for information sharing should also be supported and expanded.

Enhanced Cybersecurity Measures

The US should also support efforts to improve cybersecurity protocols in financial institutions, cryptocurrency exchanges, and other potential targets worldwide to mitigate, thwart, delay and reduce the damage of attacks.[3] While these measures will not in themselves curb cyber attacks unless and until the United States fully integrates cyber issues into its broader North Korea policy, the US should nevertheless do all that it can to ensure that financial institutions, including central banks, private financial institutions (FIs), and designated non-financial businesses and professions (DNFBPs) including cryptocurrency exchanges, take independent steps to adopt enhanced cybersecurity measures and protect against malicious DPRK cyber activities worldwide.

With a small investment, financial institutions could enforce defensive measures as part of "defense in depth"—a cybersecurity principle whereby multiple security controls are employed to thwart cyber attacks from sophisticated actors such as the DPRK. Such measures include: 1) performing regular asset inventories; 2) maintaining strong access controls; 3) developing and regularly testing incident response plans; and 4) determining how, when and with whom information about security incidents should be shared. While incurring more cost, banks could also institute better network segmentation (limiting an attacker's movement across the network), deploy next-generation Intrusion Prevention Systems (IPSs), and integrate data-logging infrastructure such as Security Information and Event Management (SIEM) systems. These latter two examine network traffic flows to detect and prevent vulnerability exploits while empowering security operations analysts to respond to incidents quickly and effectively.

Finally, the Society for Worldwide Interbank Financial Telecommunication (SWIFT) could mandate members to adopt, institute and enforce policies designed to frustrate social engineering attacks, the DPRK's primary attack vector. By encouraging the use of free, online anti-social engineering tools, such as policy templates, training exercises

and demonstration videos, members will be better situated to reduce and/or delay successful DPRK network penetrations, thereby decreasing the overall risk to the SWIFT messaging system.

Conclusion

In the end, containing and constraining North Korea's cyber activities will require a wholescale rethinking of how to integrate cyber defense, starting with the financial services sector, into both measures the international community needs to take in its own defense as well as into a broader strategy for dealing with North Korea. Pyongyang has already proven that it is determined to forge an asymmetric advantage in this new strategic domain. So far, the United States and the international community have been slow to recognize how this fast-developing problem affects broader efforts to cope with the security challenge posed by North Korea. The only remaining question is whether the international community will be resilient, agile and cohesive enough to finally deal with this challenge.

***

DOWNLOAD PDF

"North Korea's Illicit Cyber Operations: What Can Be Done?" by Stephanie Kleine-Ahlbrandt (Article and appendix) ***(http://bit.ly/2Pzgujk)***

[1] This piece focuses on the cyber operations carried out by DPRK actors in an attempt to generate illicit finance in evasion of sanctions.

[2] With regard to the issue of China's theft of US intellectual property, it was only after it was made a priority by the US, including through the 2015 Sino-US agreement on economic espionage, that the economic IP theft abated for a period. Diplomacy is key given that deterrence does not work in cyberspace (see Appendix *(http://bit.ly/2Pzgujk)*).

[3] See Interagency Guidelines Establishing Information Security Standards *(https://www.federalreserve.gov/supervisionreg/interagencyguidelines.htm)*, Board of Governors of the Federal Reserve System; Joint Statement on Heightened Cybersecurity Risk *(https://www.occ.gov/news-issuances/bulletins/2020/bulletin-2020-5a.pdf)*, January 16, 2020, by the Federal Deposit Insurance Corporation (FDIC) Office of the Comptroller of the Currency; and resources provided by the Federal Financial Institutions Examination Council (FFIEC).