(U) Non-Paper on ILLICIT DPRK CYBER ACTIVITIES

- (U) We are deeply concerned about malicious DPRK cyber activity and would like to provide your government with information on this threat so that you are able to better protect yourself against potential cyber operations. We look forward to working together on this important issue.

- (U) The DPRK poses a significant and growing cyber threat to the global financial sector, remains a cyber espionage threat, and retains the ability to conduct destructive cyber operations – all of which threaten the cybersecurity, economic security, and national security of your country, our country, and the broader international community. No country is immune from DPRK cyber threats that target infrastructure globally.

- (U) In fact, Pyongyang targets countries that have not yet built robust cyber defenses – in connection with numerous DPRK cyber-enabled heists on cryptocurrency exchanges, financial institutions, and blockchain technology companies around the world.

- (U) We expect the DPRK to continue its extensive use of cyber operations to raise funds and to gather intelligence or carry out disruptive, destructive, or otherwise destabilizing cyber activity. The DPRK's techniques and tools may achieve a range of disruptive effects with little or no warning, including distributed denial of service attacks, data deletion, social engineering, and deployment of ransomware.

- (U) In the UN Security Council 1718 (DPRK) Sanctions Committee's Panel of Experts (POE) 2019 midterm report, the POE cited investigations into numerous reported instances of DPRK actors targeting financial institutions and cryptocurrency exchanges, including dozens of cases in Southeast Asia, Africa, and South America.

- (U) Countries targeted by the DPRK include those which have maintained decades of friendly ties with the DPRK. Unfortunately, even these relationships did not deter DPRK cyber actors from attempting to steal hundreds of millions of U.S. dollars from their traditional friends and partners.

- (U) The Panel reported extensively on the DPRK's attempted evasion of Security Council resolutions through illicit cyber activities to force the transfer of funds from financial institutions and cryptocurrency exchanges. The Panel also highlighted the DPRK's increasingly sophisticated tools and tactics. We caution you against underestimating the sophistication of Pyongyang's cyber army.

- (U) These activities can generate significant funds for UN-designated DPRK entities, including those directly involved in the DPRK's unlawful WMD and ballistic missile programs. The DPRK continues to use these stolen funds to further develop these unlawful programs.

- (U) According to the Panel, the DPRK attempted to steal, through cyber means, as much as $2 billion between 2015 and 2019, and has stolen hundreds of millions of dollars since. Over the past several years, the Panel has reported on an increasing number of cyber operations against cryptocurrency exchanges and virtual asset service providers over traditional financial institutions.

- (U) In fact, according to one industry report, the DPRK stole an estimated $1.7 billion worth of cryptocurrency in 2022 alone.

- (U) In 2022, the DPRK stole the equivalent of $620 million through social engineering and cyber exploitation, the largest cryptocurrency heist in history, from a company in Asia and later stole $100 million in digital assets from another cryptocurrency company.

- (U) In addition to the financial sector, the DPRK has a long history of targeting individuals, private companies, critical infrastructure, and government agencies for Pyongyang's illicit cyber activities.

- (U) The POE has also reported that the DPRK conducts cyber operations against defense industries around the world in an attempt to illicitly access sensitive military technologies as well as to exfiltrate proprietary information that could be sold for financial gain.

- (U) This includes other countries' space research organizations, nuclear power plants, atomic energy research institutes, aerospace industries, and military targets.

- (U) The POE noted that recently claimed DPRK advances in hypersonic ballistic missile capabilities may have been achieved through DPRK cyber actors stealing the technical information needed to develop new missile systems.

- (U) We have also seen cases of the DPRK conducting cyber-enabled intrusions to steal intellectual property from pharmaceutical, chemical, energy, and information technology companies, as well as targeting the healthcare and public health sector with ransomware.

- (U) Moreover, DPRK cyber actors have deployed spearphishing campaigns against dozens of foreign government officials, including their representatives to the UN.

- (U) In large part, the DPRK engages in illicit cyber activity because it is low in cost, there are a wide range of targets available, it is easy for Pyongyang to deny its involvement in an operation, and there is low risk of reprisal.

- (U) This illicit activity is ongoing – the DPRK continues to develop advanced tradecraft, deploy new malware, and engage in increasingly sophisticated social engineering campaigns to steal funds and engage in ransomware campaigns.

- (U) We must all work together to regularly ensure our cyber defenses, detection, and response options are as up-to-date and effective as possible. When we all harden our defenses and share information, we not only protect ourselves but also deny the DPRK the illicit funds it uses to develop its unlawful WMD and ballistic missile programs.

- (U) It is vital for governments, network defenders, and the public to stay vigilant and to work together to mitigate the cyber threat posed by the DPRK. Given the DPRK's targeting of the private sector for many of its illicit cyber activities, the private sector has a vital role to play in ensuring that we are all better protected against this threat.

- (U) We urge all countries to engage with their private sectors, especially financial, cryptocurrency, blockchain companies, and relevant industry associations to ensure industry is aware of the severity of the DPRK cyber threat and takes steps to better defend against Pyongyang's malicious cyber activities.

- (U) We also encourage countries to review the relevant POE recommendations to Member States and to ensure your government has appropriate regulations and policies in place to counter this threat. We would like to provide you with a copy of some of these recommendations.

- (U) The U.S. government also releases technical advisories and information on DPRK cyber threats to help other governments, industry, and the public better protect themselves. This information is released via a website, https://www.cisa.gov/uscert/northkorea. We encourage relevant officials in your government to sign up to receive an alert whenever we post new information on this site.

- (U) In addition, your government and private sector may find an April 2020 U.S. Government DPRK Threat Advisory helpful.

- (U) The U.S. Department of the Treasury has also issued Sanctions Compliance Guidance for the Virtual Currency Industry which highlights important characteristics of an anti-money laundering (AML), counter terrorism finance (CFT) and sanctions compliance program for the digital assets industry which may be helpful as you engage with your private sector about the North Korean threat.

- (U) We may be able to offer your government and private sector stakeholders assistance in hardening your defenses against DPRK cyber threats. If you are interested in such assistance, please let us know.