CSS CYBER DEFENSE PROJECT

Hotspot Analysis:

Cyber disruption and cybercrime: Democratic People's Republic of Korea

Zürich, June 2018

Version 1

Risk and Resilience Team
Center for Security Studies (CSS), ETH Zürich

CSS
ETH Zurich

ETH zürich

Author: Marie Baezner

Contact:
Center for Security Studies
Haldeneggsteig 4
ETH Zürich
CH-8092 Zürich
Switzerland
Tel.: +41-44-632 40 25
css@sipo.gess.ethz.ch
www.css.ethz.ch

Analysis prepared by: Center for Security Studies (CSS), ETH Zürich

ETH-CSS project management: Tim Prior, Head of the Risk and Resilience Research Group, Myriam Dunn Cavelty, Deputy Head for Research and Teaching, Andreas Wenger, Director of the CSS

Please cite as: Baezner, Marie (2018): Hotspot Analysis: Cyber disruption and cybercrime: Democratic People's Republic of Korea, June 2018, Center for Security Studies (CSS), ETH Zürich.

Table of Contents

Executive Summary

Targets:	South Korean institutions and media; US military entities, government and businesses; financial institutions and cryptocurrency exchanges; and institutions of the Democratic People's Republic of Korea (DPRK)[1].
Tools:	Spear phishing, Distributed Denial of Service[2] (DDoS) attacks and malware (DDoS-KSig, Destover, Jokra, MYDOOM, Dozer, Hangman, DOGCALL, WannaCry, Android malware and others).
Effects:	Cyber capabilities used to spy on the DPRK's own citizens; economic losses for businesses targeted by DDoS attacks and hacked financial institutions; discovery of new malware families; cyber capabilities garnering the DPRK international attention without the inconvenience of economic sanctions; cyber capabilities fitting in with the DPRK's asymmetric strategy.
Timeframe:	2009 – still ongoing.

In 2014, a cyberattack targeted Sony Entertainment Pictures. The attack wiped the contents of Sony's computers and leaked sensitive information on the internet. In 2017, the US and other states attributed the ransomware WannaCry, which exploited unpatched Windows operating systems, to the DPRK. The US also attributed the Sony hack to the DPRK and revealed DPRK cyber capabilities to the world. However, the DPRK has been developing its cyber capabilities in parallel to its nuclear capabilities and has been attracting increasing attention throughout recent years.

This Hotspot Analysis studies cyber-activities related to the DPRK. It examines the impact of these cyber-activities on the DPRK's domestic society, the international economy, technological development and international relations.

The goal of this report is to better understand the mechanisms of the DPRK's cyber-activities and their role in the DPRK's strategy.

Description

States and cybersecurity companies regularly attribute cyberattacks to cyberactors with alleged links to the DPRK. However, these links cannot always be confirmed. This report examines these actors as well as the role of actors from other countries. The study looks at their various targets, techniques and tools deployed, such as spear phishing and malware.

Effects

The DPRK used its cyber capabilities at the domestic level to spy on its own citizens. DPRK leaders sought to maintain power by controlling their nation's information sphere.

Economically, cyberattacks attributed to the DPRK caused financial losses for the targeted institutions and businesses. DDoS and wiper malware damaged firms' websites and hardware, resulting in a need for costly cybersecurity intervention or hardware replacement.

The technological impact of DPRK cyber-activities was observed in the discovery of new malware families. Actors allegedly linked to the DPRK created specific malware to fit their targets' networks. These actors also appeared to follow technological advancements by targeting cryptocurrencies and adapting their malware to new vulnerabilities.

International effects observed in DPRK cyber-activities were marked by the country's use of cyber capabilities to complement its nuclear missile strategy. Cyber-activities gave the DPRK the opportunity to attract international attention without incurring economic sanctions such as those imposed for nuclear capabilities.

Consequences

The policy recommendations in this report are aimed at reducing states' risk of being impacted by DPRK cyber-activities. First, states should improve their cybersecurity by raising public awareness of spear phishing attacks and the need for keeping software updated. Second, states should encourage financial institutions and cryptocurrency exchanges to improve their own cybersecurity. Finally, states should closely monitor DPRK cyber-activities to be better prepared in the event of a DPRK cyberattack.

[1] Abbreviations are listed in section 9

[2] Technical terms are explained in a glossary in section 8.

1 Introduction

The attribution[3] of the Sony hack to the Democratic People's Republic of Korea (DPRK) [4] shed new light on DPRK cyber capabilities. Until then cyberattacks attributed to the DPRK had mostly been directed against South Korea, but since this event cybersecurity firms and states have attributed an increasing number of cyberattacks to the DPRK, revealing the DPRK's growing cyber capabilities. The unique aspect of DPRK cyberattacks resides in their motives, as the DPRK is the only state that allegedly conducts cyberattacks for both political motives and financial gain. DPRK cyber capabilities also appear to develop in parallel to its nuclear capabilities.

This Hotspot Analysis examines cyber-activities related to the DPRK. It looks at various cyberattacks that were attributed to the DPRK, but also at the role of other states in these activities.

The study of DPRK cyber-activities is relevant because of the DPRK's unique position in international politics and its growing cyber capabilities. The latter have attracted greater international attention in recent years and warrant more detailed examination.

The goal of this Hotspot Analysis is to better understand the mechanisms of DPRK cyber-activities and their role in DPRK strategy. This report will be updated as new cyberattacks or relevant elements related to the DPRK emerge. This Hotspot Analysis will also form part of a broader study that comprises the various Hotspot Analyses published during the year. This broader report will compare these Hotspot Analyses, study possible trends and propose recommendations to states wishing to improve their cybersecurity.

This Hotspot Analysis is organized as follows: Section 2 describes the historical context in which the DPRK developed its cyber capabilities to attract greater international attention alongside its nuclear missile program. A chronology helps to understand the sequence of international events that led to the DPRK developing nuclear missiles and cyber capabilities.

In Section 3, the report describes the various actors from the DPRK as well as actors allegedly linked to the DPRK and other countries. Next, the report details the nature of targets of DPRK cyberattacks as well as a selection of tools and techniques used in these cyberattacks. It shows that, while DPRK cybertools are not highly sophisticated and mostly exploit targets' vulnerabilities, they are sufficiently advanced to achieve the DPRK's strategic goals.

Section 4 analyzes the effects of DPRK cyber-activities at the domestic and international levels. At the domestic level, the report shows that the DPRK uses its cyber capabilities to spy on its own citizens to secure its information sphere and the continuity of the regime. Economically, DDoS attacks conducted by the DPRK on South Korean businesses caused economic losses, and other cyberattacks on financial institutions attributed to the DPRK also resulted in major economic losses. The technological effects of DPRK cyber-activities consisted of the discovery of new malware[5] families and the identification of the DPRK's growing interest in cryptocurrencies.

The examination of international effects addresses the role DPRK cyber-activities played beyond the Korean peninsula. It looks at how cyberattacks garnered the DPRK the same level of attention as its nuclear capabilities without the inconvenience of incurring international sanctions. This subsection explains how cyber capabilities fit into the DPRK's asymmetric strategy and complement its nuclear missile program. The WannaCry ransomware, for example, showed that DPRK cyber capabilities can be deployed to threaten individuals through indiscriminate cyberattacks.

In Section 5, this Hotspot Analysis suggests a series of policy recommendations that states may wish to implement in order to mitigate potential cyberattacks from the DPRK. States could improve their cybersecurity through awareness programs on spear phishing and by keeping their operating systems and software up to date. They could also encourage financial institutions, which are at a particularly high risk, to improve their cybersecurity. Finally, states should closely monitor the development of cyber capabilities to avoid being taken by surprise.

[3] The US intelligence attributed the hack to the DPRK, but some cybersecurity firms and experts claimed that the DPRK was not in fact the perpetrator. In this report, the DPRK is regarded as the attacker of Sony Entertainment Pictures in 2014. The general attribution problem is further discussed in section 3.1.

[4] Abbreviations are listed in section 9.

[5] Technical terms are explained in a glossary in section 8.

2 Background and chronology

Western states have focused on the DPRK's development of nuclear missiles and have mostly ignored its cyber capabilities. While the development of nuclear missiles gave DPRK international attention, it also attracted sanctions that damage the DPRK economy, whereas cyber-activities allow the DPRK to achieve its strategic goals with a low risk of retaliation or sanctions. Western states realized relatively late that the DPRK has successfully developed serious cyber capabilities despite its limited internet connectivity. In fact, the DPRK has been building its cyber capabilities for years. Kim Jong-un expanded these activities after his father's death and shifted their focus towards bolder and more visible targets such as the Bangladesh Central Bank and Sony Entertainment Pictures (Kim, 2018).

The DPRK's cyber-activities are interesting because this is the only state actor that uses cyber-activities for both political motivations and financial gains. The following chronology not only lists the main international developments relating to the DPRK, and its progress in its nuclear missile program, but also traces the main cyber-incidents attributed to the DPRK[6].

Rows with gray background refer to cyber-related incidents, while rows with light blue background list events related to DPRK nuclear missile development.

Date	Event
06.1950-07.1953	War on the Korean peninsula puts Western countries in opposition to the DPRK and its communist allies.
27.07.1953	The war ends with the signing of the Korean Armistice Agreement to stop the hostilities and establish the Korean Demilitarized Zone near the 38th parallel, separating North and South Korea.
1976	The DPRK starts the development of missiles using Soviet Scud-B missiles and a launch pad from Egypt.
1984	The DPRK conducts its first firing test of Scud-B missiles (Kim, 2017).
1990	The end of the USSR means reduced availability of material and economic support for the DPRK (Recorded Future, 2017).
10.1990	The DPRK conducts its first test of the Rodong-1 missile.
07.1994	DPRK leader Kim Il-sung dies and his son Kim Jong-il becomes the new leader of the DPRK (Kim, 2017).
31.08.1998	The DPRK conducts firing tests of the Taepodong-1 intermediate-range ballistic missile (N.K. News, 2017).
06.07.1999	The JML Virus, allegedly developed by the DPRK, is discovered in the wild.
2002	Win32/Weird.B, a version of the JML Virus, is discovered in South Korea (Jun et al., 2015).
29.01.2002	In his State of the Union address, US President George W. Bush places the DPRK in the "Axis of Evil" for its nuclear weapon program.
2003	The DPRK quits the Non-Proliferation Treaty.
20.03.2003	The US invades Iraq.
2004	South Korea establishes a National Cyber Security Center (NCSC) under its National Intelligence Service (NIS) (Park, 2016a).
04.2004	The DPRK hacks hundreds of computers and servers in South Korea (Mansourov, 2014).
2005	The DPRK announces that it possesses nuclear weapons.
05.07.2006	The DPRK tests the launch of its intermedium-range ballistic missile Taepodong-2.
09.10.2006	The DPRK announces it has conducted a successful nuclear test (Kim, 2017).
14.10.2006	The United Nations (UN) Security Council passes Resolution 1718 prohibiting exports of military supplies and luxury goods to the DPRK (United Nations Security Council, 2006).
03.2007	According to cybersecurity experts working on Operation Blockbuster, the Lazarus Group, a hacker group allegedly linked to the DPRK, starts to develop its first generation of malware (Novetta, 2016).
01.01.2008	The US National Security Agency (NSA) starts its operation Boxing Rumble to spy on the DPRK (Gallagher, 2015; Maness and Valeriano, 2017).
2009	The DPRK Korean Workers Party's Operations Department, responsible for clandestine operations during the Cold War, is restructured to become the Reconnaissance General Bureau (RGB), the DPRK's main intelligence

[6] A more detailed list of cyber-incidents attributed to the DPRK and cyberattacks that occurred in the DPRK can be found in Annex 1.

2009	agency (Jun et al., 2015; Recorded Future, 2017). The Lazarus Group starts its Operation Troy and its wiper malware (Novetta, 2016; Talmadge, 2017).
25.05.2009	The DPRK conducts a second nuclear test (Kim, 2017).
12.06.2009	The UN Security Council passes Resolution 1874 broadening the ban on exports of military supplies and luxury goods to the DPRK (United Nations Security Council, 2009).
04-07.07.2009	The Lazarus Group conducts Distributed Denial of Service (DDoS) attacks against 17 South Korean and US government websites (Chanlett-Avery et al., 2017).
2010	South Korea launches its military National Cyber Command (Park, 2016a).
26.03.2010	The DPRK torpedoes a South Korean Navy corvette.
07.07.2010	The DPRK conducts DDoS attacks on South Korean government and private websites (Jun et al., 2015).
19.07.2010	NSA's Operation Boxing Rumble ends (Gallagher, 2015; Maness and Valeriano, 2017).
23.11.2010	The DPRK fires artillery shells at the Yeonpyeong Island and jams South Korean radars to avoid direct retaliation (Jun et al., 2015).
04.03.2011	The Lazarus Group conducts a DDoS attack on 40 South Korean media outlets, critical infrastructures and financial websites, as well as on US military entities in South Korea, in an operation named Ten Days of Rain (Maness and Valeriano, 2017; Novetta, 2016).
12.04.2011	The Lazarus Group targets the South Korean Nonghyup Agriculture Cooperative Federation Bank with a DDoS attack (Chanlett-Avery et al., 2017).
17.12.2011	DPRK leader Kim Jong-il dies and his son Kim Jong-un becomes the new DPRK leader.
2012	Iran and the DPRK sign a treaty on sharing technologies, including cyber technologies (Novetta, 2016; Sin, 2016).
09.06.2012	A South Korean conservative newspaper stops a cyberattack by the Lazarus Group, but has its website defaced (Novetta, 2016).
22.01.2013	The UN Security Council passes Resolution 2087 tightening sanctions against the DPRK (United Nations Security Council, 2013a).
12.02.2013	The DPRK conducts its third nuclear test (Kim, 2017).
03.2013	The DPRK accuses the US and South Korea of having conducted cyberattacks on North Korean internet infrastructures (Center for Strategic and International Studies, 2018). A US strategic bomber plane, B-52, flies over South Korea (Meyers, 2017).
07.03.2013	The UN Security Council passes Resolution 2094 imposing sanctions on money transfers, thus isolating the DPRK from the global financial system (United Nations Security Council, 2013b).
20.03.2013	The Lazarus Group shuts down 32,000 computers in South Korean broadcast and financial companies (Jun et al., 2015; Novetta, 2016).
04.2013	Anonymous launches an operation against the DPRK causing numerous DDoS attacks and defacement on DPRK websites (Brodkin, 2013; Williams, 2013a).
25.06.2013	The DPRK launches a DDoS attack against 69 South Korean media outlets and government websites (Jun et al., 2015).
09.2013	Kaspersky Lab discovers a cyberespionage campaign named the Kimsuky campaign against South Korean think tanks and industries (Tarakanov, 2013).
2014	The DPRK compromises 140,000 South Korean government and business computers and tries to penetrate the control system for the South Korean transportation network (Tosi, 2017). The US starts a cyber program with the aim to stop the DPRK's nuclear missile program (Sanger and Broad, 2017). Scarcruft, a cyberactor associated with the DPRK government, targets South Korean media and websites on DPRK refugees with watering hole attacks (FireEye Inc., 2018).

08.2014	DPRK hackers attack the British TV broadcaster Channel 4. The channel had planned to release a TV show on a nuclear scientist being kidnapped by the DPRK. The TV show was cancelled after the cyberattack.
24.11.2014	The Lazarus Group targets Sony Entertainment Pictures with wiper malware. The group identifies itself as the Guardians of Peace and demands that a comedy movie about a plot to assassinate Kim Jong-un not be released. The group also steals information from Sony and leaks it on the internet (Chanlett-Avery et al., 2017; Maness and Valeriano, 2017).
19.12.2014	The US Federal Bureau of Investigation (FBI) publishes a report attributing the Sony cyberattack to the DPRK (Talmadge, 2017). However, cybersecurity experts are skeptical about this attribution and force the FBI to publish some of its evidence against the DPRK. US President Obama warns the DPRK of retaliation for the Sony cyberattack.
20.12.2014	The DPRK's intranet goes down for ten hours, possibly because of a cyberattack (Chanlett-Avery et al., 2017).
10.2015	The DPRK conducts cyberattacks against banks in the Philippines.
12.2015	The DPRK conducts cyberattacks against the Tien Phong Bank in Vietnam (Sanger et al., 2017).
06.01.2016	The DPRK conducts its fourth nuclear test (Kim, 2017).
02.2016	The Lazarus Group conducts a cyberattack on the Bangladesh Central Bank through the SWIFT messaging system and steals US$81 million (Chanlett-Avery et al., 2017).
02.03.2016	The UN Security Council passes Resolution 2270 imposing sanctions banning exports of gold, vanadium, titanium and rare earth materials to the DPRK (United Nations Security Council, 2016a).
04.2016	DPRK hackers penetrates the South Korean Defense Integrated Data Center and steal classified documents (Sanger et al., 2017).
08.2016	A Russian hacker group named Shadow Brokers steals a series of exploits and cybertools from the NSA and releases them on the internet (Solon, 2017).
11.2016	Scarcruft targets South Korean government and financial institutions as part of an cyberespionage campaign (FireEye Inc., 2018).
05.09.2016	The DPRK fires three ballistic missiles and at least one enters Japan's air defense zone.
09.09.2016	The DPRK conducts its fifth nuclear test.
30.11.2016	The UN Security Council passes Resolution 2321 imposing sanctions capping DPRK exports of coal (United Nations Security Council, 2016b).
2017	China stops importing coal from the DPRK (Sanger and Broad, 2017).
2017	The Lazarus Group infiltrates the website of the Polish financial regulator and infects visitors with malware (Sanger et al., 2017).
02.2017	DPRK hackers steal US$7 million worth of cryptocurrency from the South Korean cryptocurrency exchange Bithumb (Guerrero-Saade and Moriuchi, 2018).
03.2017	Microsoft patches some vulnerabilities identified by the NSA and leaked by the Shadow Brokers group in August 2016 (Nakashima, 2017).
03.2017	Scarcruft targets the South Korean government and military with spear phishing emails (FireEye Inc., 2018).
06.03.2017	The DPRK launches four ballistic missiles. Three of them land in Japan's exclusive economic zone (Kim, 2017).
04.2017	A series of spear phishing emails targeting US defense contractors is attributed to the Lazarus Group (Center for Strategic and International Studies, 2018).
05.2017	The DPRK starts to mine cryptocurrencies (Recorded Future, 2017).
05.2017	The DPRK tests the launch of several ballistic missiles, some of which hit the Sea of Japan.
05.2017	Scarcruft infects the network of a Middle Eastern firm through spear phishing (FireEye Inc., 2018).

12.05.2017	The ransomware WannaCry infects approximately 200,000 computers in over 150 countries (Kim, 2018).
15.05.2017	Cybersecurity companies Kaspersky Lab and Symantec affirm that the Lazarus Group is behind WannaCry (Solon, 2017).
06.06.2017	The NSA attributes the ransomware WannaCry to the DPRK (Nakashima, 2017).
05.08.2017	The UN Security Council passes Resolution 2371 imposing sanctions banning all exports of coal, iron, lead and seafood from the DPRK (United Nations Security Council, 2017a).
09.2017	A press report states that the US Cyber Command targeted the Reconnaissance General Bureau (RGB) with DDoS attacks (Center for Strategic and International Studies, 2018). The Lazarus Group targets users of the cryptocurrency exchange Coinlink with spear phishing emails (Guerrero-Saade and Moriuchi, 2018).
03.09.2017	The DPRK conducts its sixth nuclear test.
11.09.2017	The UN Security Council passes Resolution 2375 imposing sanctions limiting the DPRK's importation of crude oil and refined petroleum products (United Nations Security Council, 2017b).
10.2017	The DPRK acquires a new internet connection through Russia (Crowdstrike, 2018).
19.12.2017	The US publicly attributes WannaCry to the Lazarus Group (McAskill et al., 2017). Japan orders interceptor missiles from the US to counter North Korean's ballistic missiles (McCurry, 2017).
09.03.2018	The US President accepts to meet the DPRK leader in May 2018 to discuss nuclear missiles (BBC News, 2018).

3 Description

This section describes various actors involved in cyber-activities related to the DPRK, their targets and some of their cybertools. The aim of this section is to provide more information on and a deeper understanding of the relationships between these various actors and their techniques and cybertools.

3.1 Attribution and actors

A variety of actors were involved in cyber-activities related to the DPRK. It is worth mentioning that information coming out of and about the DPRK is scarce. Such information is mostly collected by South Korean and US intelligence and from North Korean defectors. The former have an interest in depicting the DPRK as an urgent, imminent threat, and their reports may be biased, while the reliability of the latter remains unclear, and knowledge of DPRK structures may also be outdated.

Attribution is a recurring point of contention in cybersecurity. It is usually based on the *cui bono* (to whose benefit) logic. However, cyber forensics cannot confirm with 100% certainty that an alleged perpetrator who is thought to benefit from a cyberattack is indeed the perpetrator. Due to language limitations, this Hotspot Analysis report is based on Western media, cybersecurity and think tank reports, and academic articles. In addition to the difficulty of gathering information on the DPRK, these sources represent specific points of view and agendas that are not neutral. It is important to bear in mind that, even though this Hotspot Analysis is intended to be objective, this choice of sources may entail a certain imbalance.

The report first examines several actors with direct links to the DPRK, and others with weaker associations with or alleged links to the DPRK. Second, the analysis looks at South Korean and US forces accused of targeting the DPRK. Third, the study analyzes China because of its role in the DPRK's cyber-activities. Finally, the report investigates the independent non-state actor Anonymous, who took part in confrontations in cyberspace with the DPRK.

DPRK actors

There are various actors from the DPRK, some of whom are directly linked to the state, while others are rather loose groups for which it remains difficult to prove effective links with the government.

Reconnaissance General Bureau

The RGB[7], the DPRK's main foreign intelligence agency and headquarter of special and cyber-operations, was created when the DPRK's intelligence institutions were restructured in 2009. It is under the administration of the Korean People's Army (KPA) General Staff Department (GSD) (Meyers, 2017). While the RGB is the country's main cyber-operations institution, the DPRK also has other organs that conduct such operations. The RGB is responsible for researching cyber solutions, gathering intelligence by cybermeans, and running cyber-operations. The RGB directly reports to the DPRK National Defense Commission, and there are rumors that the RGB is directly supervised by Kim Jong-un. The RGB is composed of seven Bureaus, each responsible for a different task, from operations to technical expertise. US reports also state that the RGB manages several trade companies that are currently under UN sanctions (Chanlett-Avery et al., 2017; Jun et al., 2014, 2015).

Bureau 121

Bureau 121[8] is the newest of the seven RGB Bureaus. It was created in 2013 and is the main cyberactor in the RGB (Chanlett-Avery et al., 2017; Recorded Future, 2017). Its tasks consist of offensive and defensive cyber-operations, cyberespionage, computer network exploitation and cybercrime to finance the regime (Jun et al., 2015). South Korean intelligence reports that Bureau 121 employs between 2,000 and 6,000 hackers who operate from both the DPRK and China (Libicki, 2017; Tosi, 2017).

Office 91

Reports claim that the RGB directly supervises Office 91, which employs approximately 80 staff and is dedicated to hacking activities and providing hardware to other hacker units (Kim, 2018). The staff allegedly travels regularly to Chinese cities hosting DPRK hackers, such as Shenyang and Dangong (Kim, 2011).

Other offices

Other offices in DPRK institutions are also involved in cyber-operations. The 414 Liaison Office and the 128 Liaison Office are subordinate to the RGB and are responsible for supporting cyber-operations in South Korea. They communicate with espionage networks in South Korea and conduct surveillance of South Korean law enforcement.

The Command Automation Bureau of the GSD is responsible for Computer Network Operations (CNO), i.e. the development of malware and research of exploits for the KPA. Within the Command Automation Bureau, Unit 31 develops malware, Unit 32 develops software for the KPA, and Unit 56 researches and develops command and control software.

The Enemy Collapse Sabotage Bureau's Unit 204 is not a cyber-operation unit per se, but is in charge of online information warfare and propaganda against South Korea (Jun et al., 2015).

There is also occasional mention of a Lab 110, which is said to be in charge of technical reconnaissance, infiltration, intelligence gathering through hacking and setting implants. However, it is unclear if Lab 110 is another name for an aforementioned unit or a separate one. It is also difficult to establish how this unit is positioned within the DPRK structure (Tosi, 2017).

Patriotic hackers

Reports state that DPRK patriotic hackers operate from China. Their role is mostly to post pro-DPRK and anti-South Korean propaganda on Western, Chinese and South Korean social media and forums. However, direct support and commands from the DPRK regime to these hackers is difficult to prove (Mansourov, 2014).

Lazarus Group

The Lazarus Group[9] is a hacker group, but many details about the group remain unclear. Experts from various cybersecurity firms have attributed several major cyberattacks to the Lazarus Group (e.g. WannaCry, the Bangladesh Central Bank heist, the Sony hack, cyberattacks on banks in Poland and South East Asia) (Guerrero-Saade and Moriuchi, 2018; Kaspersky Lab, 2017; Novetta, 2016). The group has been active at least since 2009, but a team of cybersecurity experts led by Novetta revealed the group to the public following its investigation of the Sony hack in 2014. This team of experts linked the Lazarus Group to approximately 48 malware families and several cyberattacks on South Korea (Novetta, 2016). Cybersecurity experts consider the Lazarus Group to be a highly skilled group that regularly changes the code of its malware to avoid detection. The group has allegedly employed its malware against financial institutions in at least 18 states since 2009 (Kaspersky Lab, 2017).

The structure of the group is uncertain, as are its potential links to the DPRK. This hacker group could:

[7] The RGB is also called Unit 586 (Recorded Future, 2017).

[8] Bureau 121 is also called Unit 121, Electronic Reconnaissance Bureau's Cyber Warfare Guidance Bureau (Jun et al., 2015).

[9] The Lazarus Group is also called DarkSeoul, WhoIS Hacking Team, NewRomanic Cyber Army Team, Guardian of Peace, Hidden Cobra, Chollima and Hermit.

- Be associated with the DPRK, possibly sponsored by the RGB (Nakashima, 2017)
- Conduct independent operations but have members associated with the DPRK
- Be a mercenary hacker group that sometimes works for the DPRK (Talmadge, 2017)
- Also sometimes be called Bureau 121 and might in fact be Bureau 121

There is no evidence to confirm whether the Lazarus Group is only a single group or a consortium of tightly connected hacker groups working together and sharing infrastructures. The group's finance also remains a mystery, but its sophistication makes it likely that it is well funded and organized. Cybersecurity experts have found Internet Protocol (IP) addresses from infrastructures in China, Malaysia and Indonesia in the Lazarus Group's cyberattacks. Therefore, experts assume that the group could be operating from these countries (Talmadge, 2017).

Bluenoroff

Cybersecurity experts assume that Bluenoroff is the cybercrime unit of the Lazarus Group, targeting financial institutions and cryptocurrency exchanges. It uses spear phishing emails and watering hole attacks to gain access to these institutions' networks. Bluenoroff allegedly has extensive reverse engineering skills to exploit network vulnerabilities. This subgroup pursues stealthy theft from financial institutions through long-term infiltration rather than simple hit-and-run operations. Cybersecurity experts have attributed the 2016 Bangladesh Central Bank heist and cyberattacks on financial institutions in Europe in 2016 to Bluenoroff (Kaspersky Lab, 2017; Meyers, 2017; Sheridan, 2018).

Scarcruft

Scarcruft[10] is a hacker group targeting mainly South Korean institutions and industries. Cybersecurity experts believe that the DPRK directly or indirectly supports Scarcruft. This assessment is based on four elements:

- The type of targets, which align with DPRK strategic interests
- The malware families deployed
- The belief that a DPRK individual was involved in the development of Scarcruft's malware
- The malware operating time, which matches working hours in the DPRK time zone

The group has supposedly been active since at least 2012. Up until 2017, Scarcruft focused its cyberattacks on South Korean targets, but since 2017 the group has expanded its range of targets by attacking organizations in the Middle East, Japan and Vietnam. Cybersecurity experts have identified that Scarcruft tends to use zero-day vulnerabilities in its spear phishing emails and watering hole attacks. The use of such vulnerabilities shows that the group is skilled, sophisticated and well-funded (FireEye Inc., 2018; Mercer and Rascagneres, 2018; Sheridan, 2018).

Other state actors

South Korea

South Korea is regarded as one of the best-connected countries in the world, but this connectivity constitutes a vulnerability in terms of cyberattacks. In South Korea, the military and national intelligence agencies are responsible for the state's cybersecurity. In 2011, South Korea established a National Cyber Command (NCC) under its Ministry of National Defense, which is tasked with defending government and military networks. The NCC employs approximately 1,000 staff (Abke, 2017; "South Korea to Launch Cyber Warfare Command," 2011). In 2014, the Ministry of National Defense announced a more offensive stance toward the DPRK in cyberspace, intending to give its cyber units the ability to identify DPRK cyber-activities and to use preemptive cyber strikes against such activities (Mansourov, 2014).

In 2004, the South Korean government created the National Cyber Security Center (NCSC) as part of the National Intelligence Service (NIS). This agency is responsible for overseeing South Korean cybersecurity and providing a discussion platform for the private sector, civilians and the military.

The NIS and South Korean military supported authoritarian regimes in the past. Therefore, both institutions are under strict governmental surveillance to avoid any abuse. The NIS and NCC came under criticism when agents were investigated for purchasing spying malware from the Italian firm Hacking Team. The NIS argued that the malware was intended for cyberespionage against the DPRK rather than South Korean citizens (Park, 2016a).

A 2014 report revealed that South Korea planned to build malware to stop or slow down the development of the DPRK's nuclear missiles (Kim, 2014). However, it is difficult to assess the South Korean cyber-operations against the DPRK because of the lack of reports from the North of the peninsula.

In January 2014, Kaspersky Lab discovered a cyberactor that targeted specific individuals through hotel networks. The campaign, named DarkHotel, was believed to be state-supported. The cybersecurity firm hypothesized that South Korea might have been behind these attacks (Zetter, 2014).

[10] The group is also called Reaper, APT37, Red Eyes and Group 123.

USA

In the US, the US Cyber Command, created in 2009, is in charge of cyber-operations and responsible for both defensive and offensive operations. The US Cyber Command is directed by the head of the NSA and forms part of the US Strategic Command. However, in August 2017, the US President announced that the US Cyber Command will be converted into an independent Unified Combatant Command in order to separate it from the NSA (Baldor, 2017).

The NSA is the US intelligence agency responsible for signal intelligence and the security of the US government's information systems. The NSA also has the capability to conduct CNO, and Edward Snowden revealed in 2013 that the NSA ran a mass internet surveillance program (Greenwald et al., 2013).

In relation to the DPRK, the US conducted cyberespionage campaigns against the DPRK and had implants in DPRK networks, but also tried to develop a malware similar to Stuxnet to stop or slow down the DPRK's nuclear missile program (Sanger and Broad, 2017). The DPRK repeatedly accused the US of having launched cyberattack on its internet infrastructures.

China

The direct role of the Chinese government in DPRK cyber-activities is difficult to evaluate. The DPRK used Chinese internet infrastructures to conduct cyberattacks, but it is difficult to verify whether the Chinese government is aware of or directly supports such activities. DPRK hackers operated from various cities in China such as Shenyang and Dangong. DPRK internet infrastructures are basic and limited, so by using Chinese facilities DPRK hackers gain access to better internet infrastructures and DPRK officials are able to deny any involvement in cyberattacks (Chanlett-Avery et al., 2017). The DPRK also sent hackers to Chinese universities to study computer science and hacking techniques (Kim, 2018; Libicki, 2017). The South Korean government reported that approximately 30 DPRK software and hardware companies were located in the Chinese city of Dalian. South Korean authorities warned that software and hardware coming from this region of China was probably compromised and implanted with built-in backdoors (Mansourov, 2014).

Other states

The cybersecurity firm Recorded Future (2017) observed that DPRK cyber-activities were often conducted from other countries' territories and reported that DPRK hackers had a strong physical presence in India. The DPRK and India have close diplomatic and trade relations, and India is the DPRK's main economic partner. The DPRK also sends students to universities in India. It is possible that the DPRK deployed hacker teams in India, as it did in China (Horwitz, 2017). Recorded Future noted that approximately 20% of the DPRK's malicious cyber-activities between April 1, 2017 and the July 1, 2017 transited or originated from India. However, India announced in April 2017 that it would suspend all trade with the DPRK except medicine and food (Horwitz, 2017).

Recorded Future (2017) claimed that the DPRK also had at least a virtual presence in Malaysia, New Zealand, Nepal, Kenya, Mozambique and Indonesia. Often, this merely involves activities routing through these states' internet infrastructures, and these states therefore may not be directly involved in the country's cyber-activities (Sanger et al., 2017).

Russia also played a supporting role in DPRK cyber-activities, sending computer science teachers to the DPRK to teach hacking techniques (Park, 2016b). Russia also provided the DPRK with a new internet connection, which may enable the DPRK to reduce its sole reliance on Chinese infrastructures and balance these with Russian infrastructures (Crowdstrike, 2018).

Iran signed a sharing agreement on nuclear and cyber technologies with the DPRK in 2012. Kaspersky Lab reported that some cyberattacks attributed to the Lazarus Group were technically similar to the cyberattack on the Saudi Arabian oil company Aramco attributed to Iran (Baumgartner, 2014). It is possible that Iran helped the DPRK to develop and improve its cyber capabilities (Sanger et al., 2017).

Non-state actor

Anonymous is the only non-state actor involved in cyber-activities with the DPRK. Anonymous is a decentralized cyberactivist group that supports internet freedom and freedom of speech. Anonymous launched an operation against the DPRK in 2013 that caused a series of DDoS and other cyberattacks on DPRK websites and networks. Members of Anonymous also hacked into the Twitter and Flickr accounts of a DPRK news agency and posted messages and pictures criticizing Kim Jong-un (Brodkin, 2013; Williams, 2013a, 2013b).

3.2 Targets

Targets of malicious cyber-activities in relation to the DPRK were numerous and diverse. This Hotspot Analysis report classifies these targets into four groups: targets in South Korea, which represent the majority of victims of cyberattacks; targets in other states, which mainly consist of the US; international financial targets, which, in contrast to the other targets, are targeted for financial rather than political motives; and targets in the DPRK.

Targets in South Korea

The main targets of DPRK cyber-activities were South Korean institutions. The DPRK targeted a wide range of South Korean victims: South Korean government officials and websites, businesses, media, financial institutions, critical infrastructures, defense industries, think tanks and cryptocurrency exchanges. DPRK motivations in targeting South Korea are mostly political and strategic. This broad spectrum of targets is consistent with the DPRK's asymmetric strategy and aligns with the country's strategic interests. The DPRK wants the unification of the Korean peninsula under North Korean leadership, and its strategy includes a rapid invasion of the southern part of the peninsula. The use of cybertools to compromise critical infrastructures, industries and government institutions therefore falls within this strategy (Libicki, 2017). Targeting industries, think tanks and government institutions could also serve the purpose of espionage, while targeting media and government websites serves to disrupt and erode citizens' morale (Sanger et al., 2017; Sin, 2016).

Targets in other states

While South Korea is clearly the main target, the DPRK started to target other states in 2014. The US was the most intensively targeted state, with DDoS attacks on US government websites and spear phishing on critical infrastructures operators and defense contractors. The most elaborate cyberattack from the DPRK on US soil was the Sony hack. The US represents a strategic target for the DPRK due to its status as a Great Power and its foreign military presence on the peninsula. However, the Sony hack served a different goal than the other politically and strategically motivated cyberattacks (Lewis, 2017), as its aim was to preserve the image of the DPRK leader by preventing the release of a movie showing the assassination of Kim Jong-un. The same motive was observed in the cyberattack on the British broadcaster Channel 4 (Sanger et al., 2017).

International financial targets

A unique aspect of DPRK cyber-activities is their targeting of financial institutions to generate revenue and circumvent economic sanctions. It is the only instance where a cyber state actor has been observed to employ cyberattacks for financial gains. DPRK hackers have launched cyberattacks against several banks in Asia (Bangladesh, Vietnam and Philippines) and also in Europe (Poland) since 2014 (McAskill et al., 2017; Sanger et al., 2017; Wilder, 2016). The most impressive cyberattack was the Bangladesh Central Bank heist, where DPRK hackers infected the Bangladesh Central Bank network with malware and used the SWIFT global messaging system to transfer US$81 million to an account in the Philippines (Chanlett-Avery et al., 2017).

The DPRK regime also used WannaCry, a ransomware that indiscriminately targeted unpatched Windows system users, in order to generate revenue. Hackers managed to raise approximately US$140,000 in Bitcoin, but did not collect it, probably because this would have been too easy to track (Nakashima, 2017).

DPRK cyber actors have shown an interest in cryptocurrencies since 2017, when the DPRK started to mine Bitcoins. DPRK-associated hackers have also sent spear phishing emails to cryptocurrency exchanges (Guerrero-Saade and Moriuchi, 2018; Recorded Future, 2017).

Targets in the DPRK

Motivated by a desire to maintain control over the population and perpetuate the regime, the DPRK regime also used cybertools to spy on its citizens (Mansourov, 2014).

However, the DPRK has also been a target of cyberattacks. It has been assumed that the US targeted the DPRK nuclear missile program, the DPRK intranet and the RGB with cyberattacks. However, the lack of information coming out of the DPRK renders the verification of such cyberattacks difficult. The US attacks could be in retaliation for DPRK cyberattacks on US targets, although the alleged cyberattacks on the DPRK nuclear missile program would have been aimed at stopping the program or slowing it down (Sanger and Broad, 2017).

3.3 Tools and techniques

Cyber-activities related to the DPRK have mainly consisted of spear phishing emails, DDoS and the use of malware. The first two techniques do not require extensive expertise in computer sciences. However, the latter requires greater knowledge and resources to develop custom-built malware.

Spear phishing

Spear phishing is a technique used to obtain login credentials from or infect the computer of a targeted victim. The attacker sends an email or message containing an attachment or a link, which appears to come from a trusted contact. When the target opens the attachment, this downloads malware without the user's knowledge. The malware then creates a backdoor in the user's system, allowing the perpetrator to access the user's computer. A link may also take the user to a website encouraging them to download content infected with malware. Or, a link may take the user to a webpage that looks like a trusted login page where the user would enter their login credentials. Once the

perpetrator has obtained the login information, they are able to login in the name of the target. The main goal of spear phishing attacks is therefore to gain access to a computer or an account.

Spear phishing has been frequently observed in the context of the DPRK's development of cyber capabilities, often as a first step in a cyberattack, as specifically targeted persons receive spear phishing emails and click on links or download attachments, inadvertently granting intruders network access. For example, the Lazarus Group has used spear phishing emails against US defense contractors, US electrical engineering companies and Bitcoin users (Auchard, 2017; Center for Strategic and International Studies, 2018).

Distributed Denial of Service

Prior to 2014, the DPRK mostly used Distributed Denial of Service (DDoS) attacks, where DPRK hackers would render websites inaccessible to users by overloading them with internet traffic. DPRK hackers and the Lazarus Group used this technique to shut down South Korean and US government and media websites. The goal of DDoS attacks is to disrupt and/or harass targets (Chanlett-Avery et al., 2017; Jun et al., 2015).

Malware

The DPRK developed and used various malware applications to further its strategic goals. The Lazarus Group is known to have reused some earlier malware code to build new malware. The following list describes a sample of malware attributed to the DPRK[11].

DDoS-KSig

The DDoS malware DDoS-KSig[12] is a Trojan used to perform DDoS attacks on specific websites. It also has the ability to download other files or malware, to modify files and to overwrite hard drives. This malware is attributed to the Lazarus Group and was used in the DDoS attack against South Korea in March 2011 (Lelli, 2011; Novetta, 2016).

Destover

Destover[13] is a Trojan used to open backdoors in infected computers, but can also overwrite hard disks. It shares technical similarities with Shamoon, the malware used in the cyberattack against Aramco in 2012. The malware was used in the Sony hack attributed to the Lazarus Group (Baumgartner, 2014; Hayashi, 2014; Novetta, 2016).

DOGCALL

DOGCALL[14] is a backdoor used by Scarcruft since September 2016. The malware is usually delivered through spear phishing emails using a vulnerability in the Hangul Word Processor, a Korean-language word processor widely used in South Korea. DOGCALL can take screenshots and register keystrokes of users without their knowledge. This malware communicates with attackers and receives commands through compromised cloud service providers. This backdoor was deployed against South Korean government and military networks in 2017, but also featured in other spear phishing campaigns (FireEye Inc., 2018; Mercer and Rascagneres, 2018).

Hangman

Hangman[15] is a backdoor Trojan that grants remote access to compromised computers. The Lazarus Group has been using the Hangman malware against South Korean targets since 2013. It is usually delivered through spear phishing emails, but can also be dropped in systems by other malware (US-CERT, 2017).

Jokra

Jokra[16] is a Trojan malware that wipes data from computer hard-disks. It was used in the DarkSeoul cyberattack in March 2013 and was attributed to the Lazarus Group (Constantin, 2013; Meyers, 2017; Novetta, 2016).

MYDOOM and Dozer

MYDOOM is a worm that is spread via email and peer-to-peer networks to drop other malware (Ballano Barcena and O Murchu, 2009). It was used in tandem with Dozer, a Trojan that performs DDoS attacks (Ballano Barcena et al., 2009). Both malware applications were used in the July 2009 cyberattacks on South Korean websites attributed to the Lazarus Group (Guerrero-Saade and Moriuchi, 2018; Novetta, 2016).

[11] A more detailed list is provided in Annex 2.

[12] DDoS-KSig is also called Fibedol (Windows Defender), QDDOS (Trend Micro) and Koredos (Symantec).

[13] Destover is also calledAgent.gqah (Kaspersky), and Escad (Windows Defender).

[14] DOGCALL is also called ROKRAT (Cisco Talos).

[15] Also named Volgmer and TEMP.Hermit.

[16] Jokra is also known as MBRKill (Sophos and Trend Micro).

WannaCry

WannaCry, the first ransomware paired with a worm, exploited a Windows vulnerability named EternalBlue. This vulnerability was discovered by the NSA but later stolen and leaked by the Shadow Brokers (Crowdstrike, 2018). A first version of WannaCry found in February 2017 shared some code with the Destover malware (Guerrero-Saade and Moriuchi, 2018). WannaCry spread to 200,000 computers in over 150 countries. This ransomware demanded US$300 worth of Bitcoin from each infected user in return for having their computers unlocked again. A British cybersecurity expert stopped the spread of this malware by incidentally discovering the WannaCry kill switch (Gibbs, 2017). The United Kingdom, the US, Kaspersky Lab and Symantec attributed the ransomware to the Lazarus Group (McAskill et al., 2017; Nakashima, 2017).

Android malware

Reports stated that the Lazarus Group also targeted smartphones. In 2017, McAfee reported that a fake Android Bible study app in Korean contained a backdoor. The fake app shared command and control infrastructures with malware of the Lazarus Group. This app is the first known activity of the Lazarus Group on Android smartphones (Han, 2017; Uchill, 2017).

4 Effects

This section examines the effects of cyber-activities in relation to the DPRK both at the domestic level of state actors and at the international level. At the domestic level, this report analyzes how the DPRK uses cyberspace to spy on its own citizens and examines the economic repercussions of cyberattacks conducted on financial institutions as well as resulting technological innovations.

At the international level, the analysis explains the role of cyber-activities in international relations and the DPRK's strategy regarding its nuclear missile program.

4.1 Social effects

At the domestic and social level, DPRK cyber-activities serve several purposes. It is difficult to obtain accurate information on DPRK actions against its own citizens; however, it can be assumed that cybertools would be used for international as well as domestic purposes. While it is difficult for outsiders to access information about DPRK domestic affairs, it is just as difficult for DPRK citizens to access international news, as the DPRK government tightly controls access to such information. In the DPRK, only the elites are able to connect to the worldwide internet. The domestic intranet, named Kwangmyong, is reserved for university students, scientists and selected government officials, but is not connected to the global internet. The DPRK government strictly controls the content of the intranet, which is only composed of a few websites on universities and government news. The DPRK dedicates extensive resources to ensuring that its population remain unable to access the global Internet and to maintaining its Intranet infrastructures (Chanlett-Avery et al., 2017; Mansourov, 2014; Recorded Future, 2017).

Reuters reported in 2017 that the DPRK developed tools to spy on its citizens using smartphones (Pearson, 2017). The DPRK government allowed the development of domestic smartphones with limited features, but while this gave DPRK citizens easier access to technology, it also made them more prone to surveillance (Chanlett-Avery et al., 2017; Recorded Future, 2017).

The DPRK is determined to maintain strict control over internet access and to spy on its citizens, aiming to assure the survival of the regime and to unify the peninsula under DPRK leadership. Controlling citizens' access to information is a way to ensure the perpetuation of the Kim dynasty, and withholding outside sources of information from DPRK citizens helps to prevent them from questioning the legitimacy of DPRK elites.

4.2 Economic effects

Economically, the DPRK is subject to tight international sanctions for developing nuclear weapons and therefore limited in the type of goods that it is able to export and import. Since the regime consequently needed to find new ways to generate revenue for its nuclear program and to ensure the perpetuity of the regime, it identified cyber-activities as a way to access funds and disrupt the world order with little risk of retaliation or sanctions (Kim, 2018; Sanger et al., 2017).

The economic effects of DPRK cyber-activities are mainly observed in the form of cybercrime actions. The DPRK is the first state actor known to use cybercrime to generate revenue for its regime and its nuclear program, as well as to circumvent international sanctions, and this aspect is therefore unique to the DPRK. Cybermeans constitute a relatively inexpensive option: since no costly equipment is required to be able to launch cyberattacks, significant revenue can be generated without incurring a substantial risk of retaliation (Libicki, 2017; Meyers, 2017).

The first stage of state-sponsored cybercrime targeted South Korean banks, but cybercrime attacks attributed to the DPRK have expanded to South East Asian banks since 2015 and to cryptocurrency exchanges since 2017 (Sanger et al., 2017; Sheridan, 2018; Wilder, 2016). According to a former British intelligence chief cited in Sanger et al (2017), annual revenue from DPRK cybercrime activities may be as high as US$1 billion.

Targeting cryptocurrency exchanges is a relatively new development for the DPRK, but in fact constitutes a natural progression. Since cryptocurrencies are not regulated by nation states and are therefore not affected by international sanctions, they are an easy way to generate revenue. In 2017, several cyberattacks targeted cryptocurrency exchanges in South Korea (Guerrero-Saade and Moriuchi, 2018), and the South Korean government considered closing some of these exchanges as a result. However, no reference was made to cyberattacks as a reason for the South Korean government discussing the closure of exchanges; rather the main reason given was that trading in cryptocurrencies had become too speculative and constituted a risk for the national economy (Song and Harris, 2018).

DPRK cyber- and crime-activities generated revenue for the regime and caused losses for the targeted firms and individuals. DPRK DDoS attacks targeted several South Korean firms and financial institutes, rendering websites unavailable and resulting in direct financial losses for the commercial firms concerned. These losses have been estimated to reach US$22,000 per minute of unavailability, with the average duration of unavailability calculated to be approximately 54 minutes. However, these costs are only the direct costs, and additional indirect costs, including damage to companies' reputation, also need to be taken into account (Kenig, 2013; NSFocus Inc., 2016). At the same time, DDoS attacks caused economic damage well beyond the context of DPRK cyber-activities. Criminal cyberattacks, such as the one on the Bangladesh Central Bank, showed that poor cybersecurity can have serious economic consequences.

Through its cyber-activities, the DPRK has found a way to circumvent sanctions and generate revenue. It is unlikely that the DPRK will abandon the use of cybercrime for financing its regime. Other states under international economic sanctions may also be tempted to follow the DPRK's approach and explore cybercrime for themselves.

4.3 Technological effects

Technological effects of DPRK cyber-activities consisted mostly in the discovery of new malware families. Most of the malware linked to DPRK cyberactors was custom-built. These groups developed malware families themselves and sometimes reused code from earlier malware in new applications. Novetta (2016) classified the Lazarus Group's malware families and identified which sections of code had previously been used in which cyberattacks.

The techniques observed in DPRK cyber-activities have shown that simple, relatively unsophisticated techniques can often do a great deal of damage. DPRK cyberattacks tended to be tailored to the targets and strategic goals they were intended to achieve (Lewis, 2017). DPRK cyberactors mostly relied on their targets' vulnerabilities rather than confront them with brute force, with the case of the Bangladesh Central Bank heist being a good example of this strategy. Reports stated that the Bangladesh Central Bank's information network was not protected by a firewall, and the perpetrators of the heist therefore simply exploited inadequate cybersecurity to their advantage (Chanlett-Avery et al., 2017).

Finally, DPRK cyberactors have shown growing interest in financial institutions and cryptocurrencies over the years. This interest could evolve into a serious risk to global finance as an increasing number of individuals and groups invest in such currencies, which have been found to be highly volatile. There have also been instances of cryptocurrency theft, including one in early 2017, when cyberactors associated with the DPRK stole US$7 million from a cryptocurrency exchange (Guerrero-Saade and Moriuchi, 2018). The DPRK's apparent interest in cryptocurrencies may also act as a driver to increase its future cybercrime activities.

4.4 International effects

Cyber-incidents attributed to the DPRK have had an extensive international impact, affecting not only

South Korea, but sometimes the entire world. Also, the DPRK's use of cyberattacks cannot be dissociated from its nuclear strategy and has even been found to risk angering some of its allies.

Cyberattacks attracting significant international attention

Cyberattacks attributed to the DPRK were often highly mediated and visible. The DPRK did not attempt to hide its cyber-activities (apart from cyberespionage campaigns) from its targets and the public; rather these cyberattacks were often extensively discussed in the media, although their attribution was not always unanimously accepted. With these highly visible cyberattacks, the DPRK endeavored to disrupt the peacetime status quo and to provoke South Korea and its allies (Park, 2016b). The goal of such behavior was to remind South Korea that the DPRK is still to be reckoned with and ready to fight, even though the DPRK leadership consistently denied any involvement. Furthermore, these cyberattacks served psychological warfare aims, with the idea being to intimidate the public and suggest that DPRK cyber capabilities are sufficiently well developed to affect critical infrastructures, the government or even individual citizens in South Korea (Talmadge, 2017).

Cyber-activities as a complement to nuclear strategy

The DPRK's cyber-activities can be seen to complement its nuclear program in an asymmetric strategy. The DPRK knows that, in a conventional war, it would not be able to win against South Korea and its allies and that the size of its army would not be sufficient to compensate for poorer technology. It is therefore logical for the DPRK to develop an asymmetric strategy, for which the development of nuclear weapons and cyber capabilities are perfectly suited (Park, 2016b; Tosi, 2017). While the DPRK's nuclear missile program offers the advantage of garnering international attention and attempts to create a strategic equilibrium with other nuclear powers, it has also brought disadvantages in the form of international economic sanctions. The DPRK's cyber-activities have attracted approximately the same level of international attention as its nuclear program, even with the country denying any involvement, but without the consequence of sanctions (Edwards, 2016; Park, 2016b).

The DPRK has therefore used its cyber capabilities with relative impunity, using a narrative of consistent denial of any involvement in cyberattacks. At the same time, the DPRK appears to be aware of its limits, as it directs its cyberattacks at relatively harmless targets to deliver high visibility at low intensity. This fits into its asymmetric strategy, as DPRK cyberattacks frequently remain at a low enough level not to trigger physical retaliation. In this type of situation, any physical retaliation to a cyberattack would seem disproportionate, a fact of which the DPRK is well aware. The DPRK is also aware that other states are anxious about potential retaliation using nuclear weapons. These two elements allow the DPRK to act with quasi-total impunity in cyberspace (Lewis, 2017; Libicki, 2017).

Yet, while the development of nuclear weapons and cyber capabilities brought the DPRK international attention, the risk of escalating tensions with South Korea and its main ally, the US, still exists, if a cyberattack on a critical US or South Korean infrastructures could be interpreted as an act of war. Such an incident could trigger retaliation by either conventional or unconventional means (Libicki, 2017; Lotrionte, 2013).

The US has tried to target the DPRK nuclear missile program with cybermeans. However, this choice of target could have unfortunate consequences, as it could threaten the balance of deterrence among other nuclear states. If the US was successful in its cyberattack on nuclear weapon facilities in the DPRK, Russia and China could decide to target US nuclear weapons facilities in return, launching either a preventive strike or a cyberattack to prevent the US from also targeting their own nuclear weapons arsenals with cybertools (Waddell, 2016).

Risks from indiscriminate cyberattacks for the DPRK

The DPRK has acted with impunity in cyberspace, but its boldness may pose a risk to its alliances and partnerships. WannaCry, the most recent significant cyberattack attributed to the DPRK, also badly affected China, which has been directly or indirectly supporting DPRK cyber-activities by turning a blind eye to DPRK hackers operating from its territory and by offering university courses to DPRK hackers. However, WannaCry severely impacted on Chinese individuals and the Chinese economy. Any repeat could make China change its mind on its support for DPRK cyber-activities and economic sanctions. China has already reduced its importation of coal from the DPRK, possibly as a sign of protest against DPRK cyber-activities (Bennett, 2017; Chanlett-Avery et al., 2017; Recorded Future, 2017).

China is not the only state that directly or indirectly supports DPRK cyberattacks, as both India and Russia also play a certain role in DPRK cyber-activities. However, indiscriminate cyberattacks such as WannaCry may also strain these alliances and partnerships and push these states away from the DPRK. While their assistance gives the DPRK the option of plausible deniability, but Western states could also pressure these states to force the DPRK into compliance. In 2017, India announced that would comply with international economic sanctions and limit its exports to the DPRK (Horwitz, 2017; Recorded Future, 2017).

5 Policy Consequences

This section sets out several recommendations focusing on general cybersecurity measures that states can take to reduce the risks of being impacted by cyber-activities from actors associated with the DPRK. Even though the DPRK is an untypical cyberthreat actor, the general cybersecurity measures that states can apply are the same as those applicable to other cyberthreat actors.

5.1 Improve cybersecurity

Malicious cyber-activities related to the DPRK compromised computers either through unpatched vulnerabilities or spear phishing. Therefore, it is essential to raise awareness of the need to regularly update software and operating systems. Users need to better understand the risks of running outdated software versions or operating systems. Increased awareness of the need for regular updates would reduce the risk of attacks such as WannaCry causing such widespread damage.

Awareness also needs to be raised regarding spear phishing. Users should be trained regularly concerning the risks and consequences of spear phishing emails as well as ways to recognize and flag malicious emails. Institutions could establish simple standard operating procedures for reporting such emails and enabling users to react quickly whenever malicious emails are identified. The implementation of certain technological solutions could also help users to identify fraudulent emails. The Sender Policy Framework is one example of such a technological solution, as it validates the sender's identity. Two-factor authentication systems also help to reduce the risk of damage when login credentials are stolen. This method of authentication asks for a second authentication, making it more difficult for malicious cyberactors to access full authentication details.

5.2 Encourage better cybersecurity in financial institutions

Cyber-activities associated with the DPRK have increasingly targeted financial institutions. Such institutions are therefore at a greater risk of cyberattacks from the DPRK than others. States should encourage these institutions and their own central banks to implement the best possible cybersecurity. The Bangladesh Central Bank heist showed that poor cybersecurity can have disastrous consequences. While the SWIFT messaging software was updated as a result, other vulnerabilities in networks connected to the SWIFT messaging system could still compromise the system.

Throughout the past year, actors associated with the DPRK have also targeted cryptocurrency exchanges and users. States could seek to regulate cryptocurrency exchanges through cybersecurity standards to limit the risk of theft.

5.3 Monitor the situation

Cyberattacks attributed to DPRK actors have so far mostly targeted South Korean and financial targets or specific targets that presented the DPRK regime in a negative light. It has not been possible to establish clearly whether there has been any relationship between the number of cyberattacks attributed to the DPRK and DPRK missile test launches. Cyberattacks do not appear to have increased either before or after DPRK missile test launches, though (Recorded Future, 2017), and states, apart from South Korea, are therefore not directly affected by DPRK cyber-activities. However, states should remain aware of the evolution of the DPRK's nuclear and cyber capabilities. WannaCry spread indiscriminately across the globe, and new, similar ransomware may reoccur in the future. Nuclear missiles also have wider geopolitical consequences for states other than the US and South Korea, and monitoring the evolution of these activities would therefore enable states to stay ahead and avoid surprises.

6 Annex 1

Non-exhaustive list of cyber-incidents related to the DPRK.

B = Business, CI = Critical Infrastructures, F = Financial institutions, G = Government, M = Media, MIL = Military institutions, O = Others				
Date	**Victim(s)**	**Type of victim(s)**	**Alleged perpetrator**	**Technique/Tool/Name of operation**
04.2004	Approximately 300 computers and 200 servers of South Korean institutions	G/O	DPRK	Used proxy computers in China to hack South Korean institutions (Mansourov, 2014).
2008	South Korean military officers	MIL	DPRK	Spear phishing emails containing an attachment infected with malware (Cluley, 2008).
01.01.2008 – 19.07.2010	DPRK	G	NSA	Operation Boxing Rumble was a cyberespionage campaign that hacked into South Korean exploits that were already installed on DPRK computers (Gallagher, 2015).
2009	South Korean institutions		Lazarus Group	Operation Troy (Novetta, 2016).
04-07.07.2009	17 South Korean and US government websites	G	Lazarus Group	DDoS with the malware Dozer and MYDOOM malware (Chanlett-Avery et al., 2017).
03.2010	DPRK nuclear missile program	G/MIL	USA	Failed attempt to target a DPRK nuclear missile with Stuxnet-like malware (Waddell, 2016; Zetter, 2015).
07.07.2010	South Korean government and firms websites	B/G	DPRK	DDoS (Jun et al., 2015).
08-09.01.2011	DPRK news website Uriminzokkiri	M	South Korea	Hack (Mansourov, 2014).
17.01.2011	Free North Korea Radio	M	DPRK	DDoS (Mansourov, 2014).
04.03.2011	40 South Korean media outlets, financial institutions, critical infrastructures and US military entities	CI/F/G/ M/MIL	Lazarus Group	The operation was named Ten Days of Rain and comprised DDoS attacks (Maness and Valeriano, 2017; Novetta, 2016).
12.04.2011	South Korean Nonghyup National Agriculture Cooperative Bank	F	Lazarus Group	DDoS (Chanlett-Avery et al., 2017; Jun et al., 2015).
09.06.2012	South Korean conservative newspaper	M	Lazarus Group	The wiper malware attack was stopped before doing any damage, but the website was defaced (Novetta, 2016).
03.2013	DPRK internet access	O	USA and South Korea (accused by DPRK)	(Center for Strategic and International Studies, 2018).

Date	Victim(s)	Type of victim(s)	Alleged perpetrator	Technique/Tool/Name of operation
20.03.2013	3 South Korean broadcast companies, financial institutions and one internet service provider	F/M/O	Lazarus Group	Jokra wiper - 32,000 computers shut down by implants – Cyberattack named DarkSeoul (Chanlett-Avery et al., 2017).
25.03.2013	4 South Korean media outlets websites	M	DPRK	DDoS (Jun et al., 2015).
03-04.2013	DPRK websites and Twitter and Flickr accounts	G/M	Anonymous	DDoS and website defacement (Brodkin, 2013; Williams, 2013a).
05.2013	South Korean banks and their users	F	Lazarus Group	Use of the Castov malware to steal credentials and install other malware (Security Response, 2017)
25.06.2013	DPRK military	G/MIL	Anonymous	Theft and release of documents (Keck, 2013).
25.06.2013	DPRK websites	M/O	Anonymous	DDoS (Williams, 2013b).
25.06.2013	69 South Korean media outlets and government websites	G/M	DPRK	DDoS ("South Korea Blames North Korea for Cyberattack," 2013).
09.2013	South Korean think tanks, Ministry of Defense, and defense industries	G/MIL/O	Unknown (actor with probable links to DPRK)	Cyberespionage (Center for Strategic and International Studies, 2018; Tarakanov, 2013).
2014	140,000 South Korean government and businesses computers	B/G	DPRK	Hack (Tosi, 2017).
2014	South Korean media and websites on DPRK refugees	M/O	Scarcruft	Infected through watering hole websites containing the POORAIM malware (FireEye Inc., 2018).
2014	South Korean transportation network control system	CI	DPRK	Failed attempt to penetrate the network (Tosi, 2017).
19.05.2014 – 16.09.2014	Smartphones in South Korea	O	DPRK	Use of malicious gaming application to spy on smartphone users in South Korea (Mansourov, 2014).
08.2014	British Channel 4	M	Lazarus Group	Data theft (Center for Strategic and International Studies, 2018; Sanger et al., 2017).
24.11.2014	Sony Entertainment Pictures	O	Lazarus Group	Data theft and Destover wiper (Chanlett-Avery et al., 2017; Maness and Valeriano, 2017; Novetta, 2016).
20.12.2014	DPRK intranet	G	USA	Intranet shut-down possibly due to a cyberattack (Tosi, 2017).
24.12.2014	South Korean Hydro and Nuclear Power	CI/G	DPRK	Data theft (Chanlett-Avery et al., 2017; Maness and Valeriano, 2017).
08.2015	South Korean	O	Lazarus Group	Spear phishing campaign with a lure document containing the Hawup RAT (Crowdstrike, 2018, 2016).

Date	Victim(s)	Type of victim(s)	Alleged perpetrator	Technique/Tool/Name of operation
10.2015	South Korean government officials	G	Lazarus Group	Spear phishing emails (Novetta, 2016).
10.2015	Bank in Philippines	F	DPRK	Hack (Sanger et al., 2017; Wilder, 2016).
10.2015	South Korean National Assembly, Ministry of Unification and the Blue House	G	RGB	Hack (Center for Strategic and International Studies, 2018).
12.2015	Tien Phong Bank in Vietnam	F	DPRK	Hack (Sanger et al., 2017; Wilder, 2016).
2016	2 South Korean defense contractors and South Korean national security officials	G/MIL	DPRK	Cyberespionage (Sin, 2016).
02.2016	Bangladesh Central Bank	F	Lazarus Group	Hack (Chanlett-Avery et al., 2017).
03.2016	Smartphones of dozen of South Korean government officials	G	DPRK	Hack (Center for Strategic and International Studies, 2018).
03.2016	Users of Korean-language torrent file-sharing websites	O	Scarcruft	Users who downloaded infected torrent files were infected by the malware KARAE, possibly to create a botnet (FireEye Inc., 2018).
04.2016	South Korean Defense Integrated Data Center	MIL	DPRK	Data theft of South Korean and US classified documents (Center for Strategic and International Studies, 2018; Sanger et al., 2017).
13.06.2016	160 South Korean firms and government agencies	B/G	DPRK	Cyberespionage (Wilder, 2016).
11.2016	South Korean government and financial institutions	F/G	Scarcruft	Cyberespionage with the malware HAPPYWORK (FireEye Inc., 2018).
02.2017-ongoing	Bitcoin insiders	F	Lazarus Group	Spear phishing (Auchard, 2017).
02.2017	Polish financial regulator website	F	Lazarus Group	Hack (Sanger et al., 2017).
02.2017	South Korean cryptocurrency exchange Bithumb	F	DPRK	Hack (Guerrero-Saade and Moriuchi, 2018).
03.2017	South Korean government and military	G/MIL	Scarcruft	Infection through spear phishing emails delivering the DOGCALL backdoor (FireEye Inc., 2018).
04.2017	US defense contractors	MIL	Lazarus Group	Spear phishing (Center for Strategic and International Studies, 2018).
05.2017	Middle East Company	B	Scarcruft	Spear phishing email that delivered the SHUTTERSPEED backdoor (FireEye Inc., 2018).
12.05.2017	Individuals	O	DPRK	WannaCry ransomware (Chanlett-Avery et al., 2017).
09.2017	RGB	G	US Cyber Command	DDoS (Center for Strategic and International Studies, 2018).

Date	Victim(s)	Type of victim(s)	Alleged perpetrator	Technique/Tool/Name of operation
09.2017	Coinlink cryptocurrency exchange	F	Lazarus Group	Spear phishing (Auchard, 2017).
10.2017	US electrical companies	CI	DPRK	Spear phishing (Center for Strategic and International Studies, 2018; Crowdstrike, 2018).

7 Annex 2

Non-exhaustive list of malware associated with the DPRK

Malware name	Other names	Type of malware	Group using this malware	Cyberattack in which this malware was used	Comments and reference
Android/ Backdoor	-	Android spying malware	Lazarus Group[17]	-	(Han, 2017; Uchill, 2017)
Brambul	Mal/Brambul-A	Worm	DPRK actor	Cyberattack on South Korea in October 2015	Associated with Duuzer and Joanap (Symantec Security Response, 2015)
Castov	Castdos	Downloader and credentials stealer	Lazarus Group	Cyberattacks against South Korean banks in 2013	(Security Response, 2017)
CORALDECK	-	Exfiltration tool	Scarcruft	-	(FireEye Inc., 2018)
DarkSeoul	Mal/EncPk-ACE	DDoS malware	Lazarus Group	DarkSeoul	(Cluley, 2013)
DDoS-Ksig	DeltaAlfa, Fibedol, QDDOS and Koredos	DDoS trojan	Lazarus Group	Ten Days of Rain, Operation Troy	(Lelli, 2011; Novetta, 2016)
Destover	Agent.gqah, Escad, Wiper, WhiskeyAlfa	Wiper trojan	Lazarus Group	Sony hack	Shared some similarities with Shamoon[18] and DarkSeoul malware (Baumgartner, 2014)
DOGCALL	ROKRAT	Backdoor	Scarcruft	Used in attack against South Korean government and military in 2017	Often seen with the wiper RUHAPPY (FireEye Inc., 2018)
DoublePulsar	-	Backdoor	Lazarus Group	WannaCry	Developed by the NSA and then stolen by the Shadow Brokers. It was used with the Eternal Blue vulnerability (Crowdstrike, 2018)
Dozer	-	DDoS trojan	Lazarus Group	DDoS against South Korean and US targets in July 2009	(Ballano Barcena et al., 2009)

[17] More than 45 malware families have been linked to the Lazarus Group. Not all of them are in this list. For more information see: https://www.operationblockbuster.com/wp-content/uploads/2016/02/Operation-Blockbuster-Report.pdf

[18] Shamoon was a wiper malware used in y cyberattacks against the Saudi Arabian oil company Aramco in 2012. The Shamoon cyberattack was attributed to Iran.

Malware name	Other names	Type of malware	Group using this malware	Cyberattack in which this malware was used	Comments and reference
Duuzer	Wildpositron	Backdoor	DPRK actor	Cyberattack on South Korea in October 2015	Associated with Brambul and Joanap (Kaspersky Lab, 2017; Symantec Security Response, 2015)
GELCAPSULE	-	Downloader	Scarcruft	-	Used to download the malware SLOWDRIFT (FireEye Inc., 2018)
Hangman	Volgmer, TEMP.Hermit	Trojan	Lazarus Group	-	(US-CERT, 2017)
HAPPYWORK	-	Downloader	Scarcruft	Used in attack against South Korean government and financial institutions in 2016	(FireEye Inc., 2018)
Hawup RAT	-	RAT	Lazarus Group	Used in a spear phishing campaign against South Korean	(Crowdstrike, 2018, 2016)
JML Virus	Win32/Weird, Win32/JML	Virus	DPRK	Used in cyberattacks around 2000	(Jun et al., 2015)
Joanap	-	Trojan	DPRK actor	Cyberattack on South Korea in October 2015	Associated with Duuzer and Brambul (Symantec Security Response, 2015)
Jokra	MBRKill	Wiper trojan	Lazarus Group	DarkSeoul	(Constantin, 2013; Meyers, 2017; Novetta, 2016)
KARAE	-	Backdoor	Scarcruft	-	Delivered through South Korean torrent file-sharing websites (FireEye Inc., 2018)
Kimsuky	-	Spying malware family	Unknown (actor with probable links to DPRK)	Used in a cyberespionage campaign against South Korean think tanks and industries in 2013	Malware family composed of single malware for each spying activity (Tarakanov, 2013).
MILKDROP	PoohMilk	Launcher for backdoor	Scarcruft	-	(FireEye Inc., 2018; Mercer and Rascagneres, 2018)
MYDOOM	-	Worm	-	-	(Ballano Barcena and O Murchu, 2009)
POORAIM	-	Backdoor	Scarcruft	Used against South Korean media and websites on DPRK refugees since 2014	Delivered through watering hole attacks (FireEye Inc., 2018)

Malware name	Other names	Type of malware	Group using this malware	Cyberattack in which this malware was used	Comments and reference
RICECURRY	-	Profiler	Scarcruft	-	Used to identify a victim's web browser (FireEye Inc., 2018)
RUHAPPY	ERSP.enc	Wiper	Scarcruft	-	Delivered on a computer through the DOGCALL malware and developed by the same developer as DOGCALL and HAPPYWORK, may be linked to the cyberattack on a South Korean power plant in December 2014 (FireEye Inc., 2018; Mercer and Rascagneres, 2018)
SHUTTERSPEED	Freenki, FreeMilk	Backdoor	Scarcruft	-	Delivered through spear phishing emails (FireEye Inc., 2018; Mercer and Rascagneres, 2018)
SLOWDRIFT	-	Launcher	Scarcruft	Used in a cyberattack targeting South Korean academics	Delivered through spear phishing emails, downloads other malware (FireEye Inc., 2018)
SOUNDWAVE	-	Recorder	Scarcruft	-	Enables microphones and registers audio files (FireEye Inc., 2018)
SpaSpe	-	-	Lazarus Group	-	(Guerrero-Saade and Moriuchi, 2018)
Trojan.Banker. Win32.Alreay	-		Lazarus Group/ Bluenoroff	Bangladesh Central Bank	Banks in South East Asia and banks in Poland (related to the Romeo malware family identified by Novetta) (Kaspersky Lab, 2017)
WannaCry	-	Ransomware paired with a worm	Lazarus Group	WannaCry	Shared some code with Destover and Hawup RAT (Crowdstrike, 2018; Guerrero-Saade and Moriuchi, 2018)
WINERACK	-	Backdoor	Scarcruft	-	(FireEye Inc., 2018)
ZUMKONG	-	Credential stealer	Scarcruft	-	(FireEye Inc., 2018)

8 Glossary

Backdoor: Part of a software code allowing hackers to remotely access a computer without the user's knowledge (Ghernaouti-Hélie, 2013, p. 426).

Bitcoin mining: Process of verifying and adding Bitcoin transactions to the blockchain, and of creating new Bitcoins (Investopedia, 2018).

Botnet or bot: Network of infected computers which can be accessed remotely and controlled centrally in order to launch coordinated attacks (Ghernaouti-Hélie, 2013, p. 427).

Command and Control infrastructure (C&C): A server through which the person controlling malware communicates with it in order to send commands and retrieve data (QinetiQ Ltd, 2014, p. 2).

Computer Network Exploitation (CNE): A form of Computer Network Operation (CNO) consisting of espionage and reconnaissance of a network architecture through cybermeans (Zetter, 2016).

Distributed Denial of Service (DDoS): Act of overwhelming a system with a large number of packets through the simultaneous use of infected computers (Ghernaouti-Hélie, 2013, p. 431).

Exploit: An attack on a computer operating system using a vulnerability of the system or software (Rouse, 2017).

Hack: Act of entering a system without authorization (Ghernaouti-Hélie, 2013, p. 433).

Malware: Malicious software that can take the form of a virus, a worm or a Trojan horse (Collins and McCombie, 2012, p. 81).

Patch: Software update that repairs one or several identified vulnerabilities (Ghernaouti-Hélie, 2013, p. 437).

Ransomware: Malware that locks the user's computer system and only unlocks it when a ransom is paid (TrendMicro, 2017).

Remote Administration or Access Tool (RAT): Software granting remote access and control to a computer without having physical access to it. RAT can be legitimate software, but also malicious (Siciliano, 2015).

Sender Policy Framework (SPF): Technical system validating email senders as coming from an authenticated connection in order to prevent email spoofing (Openspf, 2010).

Spear phishing: A sophisticated phishing technique that not only imitates legitimate webpages, but also selects potential targets and adapts malicious emails to them. Emails often look like they come from a colleague or a legitimate company (Ghernaouti-Hélie, 2013, p. 440).

SWIFT messaging system: A messaging platform used internationally in financial transactions. It connects more than 11,000 banking institutions in over 200 countries (SWIFT, 2018).

Torrent file: Any type of file that is shared via the BitTorrent protocol, a peer-to-peer (P2P) sharing protocol (TechTerms, 2007a, 2007b).

Trojan horse: Malware hidden in a legitimate program in order to infect and hijack a system (Ghernaouti-Hélie, 2013, p. 441).

Two-factor authentication: A login procedure that involves two out of the following three elements: something the user knows (e.g. password), something the user has (e.g. card), and something the user is (e.g. biometric) (Rosenblatt and Cipriani, 2015).

Virus: Malicious program with the capacity to multiply itself and to impair an infected system. Its purpose is also to spread to other networks (Ghernaouti-Hélie, 2013, p. 442).

Watering hole attack: Attack where a legitimate website is injected with malicious code that redirects users to a compromised website which infects users accessing it (TechTarget, 2015).

Wiper: Feature that completely erases data from a hard disk (Novetta, 2016, p. 57).

Zero-day exploit / vulnerabilities: Security vulnerabilities of which software developers are not aware and which can be used to hack a system (Karnouskos, 2011, p. 2).

9 Abbreviations

CNO	Computer Network Operation
DDoS	Distributed Denial of Service
DPRK	Democratic People's Republic of Korea
FBI	Federal Bureau of Investigation - USA
GSD	General Staff Department - DPRK
KPA	Korea People's Army - DPRK
NCC	National Cyber Command – South Korea
NCSC	National Cyber Security Center – South Korea
NIS	National Intelligence Service – South Korea
NSA	National Security Agency - USA
RAT	Remote Access Tool
RGB	Reconnaissance General Bureau - DPRK
UN	United Nations

10 Bibliography

Abke, T., 2017. Cyber security a high priority issue for South Korea [WWW Document]. Indo-Asia-Pac. Def. Forum. URL http://apdf-magazine.com/cyber-security-a-high-priority-issue-for-south-korea/ (accessed 20.02.18).

Auchard, E., 2017. Suspected North Korean cyber group seeks to woo bitcoin job seekers [WWW Document]. Reuters. URL https://www.reuters.com/article/us-markets-bitcoin-northkorea/suspected-north-korean-cyber-group-seeks-to-woo-bitcoin-job-seekers-idUSKBN1E91ZW (accessed 15.02.18).

Baldor, L.C., 2017. US to create independent military cyber command [WWW Document]. ABC News. URL http://abcnews.go.com/Technology/wireStory/us-create-independent-military-cyber-command-48675223 (accessed 19.07.17).

Ballano Barcena, M., O Murchu, L., 2009. W32.Dozer [WWW Document]. Symantec Secur. Response. URL https://www.symantec.com/security_response/writeup.jsp?docid=2009-070816-5318-99 (accessed 21.02.18).

Ballano Barcena, M., O Murchu, L., Itabashi, K., Ciubotariu, M., 2009. Trojan.Dozer [WWW Document]. Symantec Secur. Response. URL https://www.symantec.com/security_response/writeup.jsp?docid=2009-070814-5311-99 (accessed 21.02.18).

Baumgartner, K., 2014. Sony/Destover: mystery North Korean actor's destructive and past network activity [WWW Document]. Securelist. URL https://securelist.com/destover/67985/ (accessed 21.02.18).

BBC News, 2018. Trump and North Korea's Kim Jong-un to hold "milestone" meeting [WWW Document]. BBC News. URL http://www.bbc.com/news/world-us-canada-43339901 (accessed 12.03.18).

Bennett, C., 2017. North Korean hackers test China's patience [WWW Document]. POLITICO. URL https://www.politico.com/story/2017/05/16/north-korean-hackers-test-china-patience-238473 (accessed 15.02.18).

Brodkin, J., 2013. Anonymous hackers take control of North Korean propaganda accounts [WWW Document]. Ars Tech. URL https://arstechnica.com/information-technology/2013/04/anonymous-hackers-take-control-of-north-korean-propaganda-sites/ (accessed 20.02.18).

Center for Strategic and International Studies, 2018. Significant Cyber Incidents [WWW Document]. Cent. Strateg. Int. Stud. URL

https://www.csis.org/programs/cybersecurity-and-warfare/technology-policy-program/other-projects-cybersecurity (accessed 25.01.18).

Chanlett-Avery, E., Rosen, L.W., Rollins, J.W., Theohary, C.A., 2017. North Korean Cyber Capabilities: In Brief (No. R44912). Congressional Research Service.

Cluley, G., 2013. DarkSeoul: SophosLabs identifies malware used in South Korean internet attack [WWW Document]. Nakedsecurity Sophos. URL https://nakedsecurity.sophos.com/2013/03/20/south-korea-cyber-attack/ (accessed 06.03.18).

Cluley, G., 2008. Sex, spyware and North and South Korea [WWW Document]. Nakedsecurity Sophos. URL https://nakedsecurity.sophos.com/2008/09/02/sex-spyware-and-north-and-south-korea/ (accessed 08.03.18).

Collins, S., McCombie, S., 2012. Stuxnet: the emergence of a new cyber weapon and its implications. J. Polic. Intell. Count. Terror. 7, 80–91. https://doi.org/10.1080/18335330.2012.653198

Constantin, L., 2013. New disk wiper malware linked to attacks in South Korea [WWW Document]. PCWorld.com. URL https://www.pcworld.com/article/2043241/new-disk-wiper-malware-linked-to-attacks-in-south-korea-researchers-say.html (accessed 21.02.18).

Crowdstrike, 2018. 2018 Global Threat Report: Blurring the lines between statecraft and tradecraft. CrowdStrike.

Crowdstrike, 2016. 2015 Global Threat Report. CrowdStrike.

Edwards, W., 2016. North Korea as a cyber threat [WWW Document]. Cipher Brief. URL https://www.thecipherbrief.com/north-korea-as-a-cyber-threat (accessed 15.02.18).

FireEye Inc., 2018. APT37 (Reaper) The overlooked North Korean Actor (Special Report). FireEye Inc., Milpitas, CA.

Gallagher, S., 2015. NSA secretly hijacked existing malware to spy on N. Korea, others [WWW Document]. Ars Tech. URL https://arstechnica.com/information-technology/2015/01/nsa-secretly-hijacked-existing-malware-to-spy-on-n-korea-others/ (accessed 21.02.18).

Ghernaouti-Hélie, S., 2013. Cyberpower: crime, conflict and security in cyberspace, 1. ed. ed, Forensic sciences. EPFL Press, Lausanne.

Gibbs, S., 2017. WannaCry hackers still trying to revive attack says accidental hero [WWW Document]. The Guardian. URL https://www.theguardian.com/technology/2017/may/22/wannacry-hackers-ransomware-attack-kill-switch-windows-xp-7-nhs-accidental-hero-marcus-hutchins (accessed 22.02.18).

Greenwald, G., MacAskill, E., Poitras, L., 2013. Edward Snowden: the whistleblower behind the NSA surveillance revelations [WWW Document]. The Guardian. URL https://www.theguardian.com/world/2013/jun/09/edward-snowden-nsa-whistleblower-surveillance (accessed 13.11.17).

Guerrero-Saade, J.A., Moriuchi, P., 2018. North Korea Targeted South Korean Cryptocurrency Users and Exchange in Late 2017 Campaign (No. CTA-2018-0116), Cyber Threat Analysis. Recorded Future.

Han, I., 2017. Android Malware Appears Linked to Lazarus Cybercrime Group [WWW Document]. McAfee. URL https://securingtomorrow.mcafee.com/mcafee-labs/android-malware-appears-linked-to-lazarus-cybercrime-group./ (accessed 12.02.18).

Hayashi, K., 2014. Backdoor.Destover [WWW Document]. Symantec. URL https://www.symantec.com/security_response/writeup.jsp?docid=2014-120209-5631-99 (accessed 21.02.18).

Horwitz, J., 2017. India is an unexpected axis of North Korea's suspect cyber activity. Quartz.

Investopedia, 2018. Bitcoin Mining [WWW Document]. Investopedia. URL https://www.investopedia.com/terms/b/bitcoin-mining.asp (accessed 21.02.18).

Jun, J., LaFoy, S., Sohn, E., 2015. North Korea's cyber operations: strategy and responses.

Jun, J., LaFoy, S., Sohn, E., 2014. What Do We Know About Past North Korean Cyber Attacks and Their Capabilities?

Karnouskos, S., 2011. Stuxnet worm impact on industrial cyber-physical system security. IEEE, pp. 4490–4494. https://doi.org/10.1109/IECON.2011.6120048

Kaspersky Lab, 2017. Lazarus Under The Hood. Kaspersky Lab HQ.

Keck, Z., 2013. Anonymous: We Have Stolen North Korean Military Documents [WWW Document]. The Diplomat. URL https://thediplomat.com/2013/06/anonymous-we-have-stolen-north-korean-military-documents/ (accessed 06.03.18).

Kenig, R., 2013. How Much Can a DDoS Attack Cost Your Business? [WWW Document]. Radware Blog. URL https://blog.radware.com/security/2013/05/how-much-can-a-ddos-attack-cost-your-business/ (accessed 23.01.17).

Kim, E., 2014. S. Korea pushes to develop offensive cyberwarfare tools [WWW Document]. Yonhap News Agency. URL http://english.yonhapnews.co.kr/search1/2603000000.html?cid=AEN20140219003100315 (accessed 20.02.18).

Kim, S., 2018. Inside North Korea's Hacker Army [WWW Document]. Bloomberg. URL https://www.bloomberg.com/news/features/2018-02-07/inside-kim-jong-un-s-hacker-army (accessed 13.02.18).

Kim, S., 2017. A Timeline of North Korea's Missile Launches and Nuclear Detonations [WWW Document]. Bloomberg. URL https://www.bloomberg.com/news/articles/2017-04-16/north-korea-missile-launches-nuclear-detonations-timeline (accessed 25.01.18).

Kim, S.Y., 2011. No. 91 "Hackers HQ" Revealed [WWW Document]. DailyNK. URL http://www.dailynk.com/english/read.php?cataId=nk00100&num=7772 (accessed 20.02.18).

Lelli, A., 2011. Trojan.Koredos [WWW Document]. Symantec. URL https://www.symantec.com/security_response/writeup.jsp?docid=2011-030417-4602-99 (accessed 21.02.18).

Lewis, J.A., 2017. The Likelihood of North Korean Cyber Attacks [WWW Document]. Cent. Strateg. Int. Stud. URL https://www.csis.org/analysis/likelihood-north-korean-cyber-attacks (accessed 1502.18).

Libicki, M.C., 2017. North Korean cyber operations: active, noisy, and lacking strategy [WWW Document]. Cipher Brief. URL https://www.thecipherbrief.com/north-korean-cyber-operations-active-noisy-lacking-strategy (accessed 12.02.18).

Lotrionte, C., 2013. State Sovereignty and Self-Defense in Cyberspace: A Normative Framework for Balancing Legal Rights. Emory Int. Law Rev. 26, 825–919.

Maness, R.C., Valeriano, B., 2017. The Dyadic Cyber Incident and Dispute Data, Versions 1.5 Incidents only 20 jan.

Mansourov, A., 2014. North Korea's Cyber Warfare and Challenges for the U.S.-ROK Alliance.

McAskill, E., Hern, A., McCurry, J., 2017. Facebook action hints at western retaliation over WannaCry attack [WWW Document]. The Guardian. URL https://www.theguardian.com/technology/2017/dec/19/wannacry-cyberattack-us-says-it-has-evidence-north-korea-was-directly-responsible (accessed 15.02.18).

McCurry, J., 2017. Japan buys US missile defence system to counter North Korean threat [WWW Document]. The Guardian. URL https://www.theguardian.com/world/2017/dec/19/japan-buys-us-missile-defence-system-to-counter-north-korean-threat (accessed 15.02.18).

Mercer, W., Rascagneres, P., 2018. Korea In The Crosshairs [WWW Document]. Talos. URL http://blog.talosintelligence.com/2018/01/korea-in-crosshairs.html (accessed 08.03.18).

Meyers, A., 2017. North Korean Cyber Operations: Weapons of Mass Disruption [WWW Document]. 38North. URL https://www.38north.org/2017/11/ameyers111317/ (accessed 12.02.18).

Nakashima, E., 2017. The NSA has linked the WannaCry computer worm to North Korea [WWW Document]. Wash. Post. URL https://www.washingtonpost.com/world/national-security/the-nsa-has-linked-the-wannacry-computer-worm-to-north-korea/2017/06/14/101395a2-508e-11e7-be25-3a519335381c_story.html?utm_term=.e986139b2a8c (accessed 15.02.18).

N.K. News, 2017. Chronology of North Korea's missile, rocket launches [WWW Document]. Yonhap News Agency. URL http://english.yonhapnews.co.kr/northkorea/2017/04/05/0401000000AEN20170405007000315.html (accessed 09.02.18).

Novetta, 2016. Operation Blockbuster: Unraveling the long thread of the Sony attack. Novetta, McLean,Virginia, USA.

NSFocus Inc., 2016. Distributed Denial-of-Service (DDoS) Attacks: An Economic Perspective (Whitepaper). NSFocus Inc., Santa Clara, CA.

Openspf, 2010. Sender Policy Framework [WWW Document]. Send. Policy Framew. URL http://www.openspf.org/Introduction (accessed 03.01.17).

Park, D., 2016a. Cybersecurity Spotlight: South Korea [WWW Document]. Henry M Jackson Sch. Int. Stud. URL https://jsis.washington.edu/news/cybersecurity-spotlight-south-korea/ (accessed 06.03.18).

Park, D., 2016b. North Korea Cyber Attacks: A New Asymmetrical Military Strategy [WWW Document]. Henry M Jackson Sch. Int. Stud. URL https://jsis.washington.edu/news/north-korea-cyber-attacks-new-asymmetrical-military-strategy/ (accessed 16.02.18).

Pearson, J., 2017. North Korea uses sophisticated tools to spy on citizens digitally - report [WWW Document]. Reuters. URL https://www.reuters.com/article/us-northkorea-surveillance/north-korea-uses-

sophisticated-tools-to-spy-on-citizens-digitally-report-idUSKBN1690DZ (accessed 22.02.18).
QinetiQ Ltd, 2014. Command & Control: Understanding, denying, detecting. QinetiQ Ltd.
Recorded Future, 2017. North Korea Cyber Activity. Recorded Future.
Rosenblatt, S., Cipriani, J., 2015. Two-factor authentication: What you need to know (FAQ) [WWW Document]. CNet. URL https://www.cnet.com/news/two-factor-authentication-what-you-need-to-know-faq/ (accessed 14.12.16).
Rouse, M., 2017. computer exploit [WWW Document]. TechTarget. URL http://searchsecurity.techtarget.com/definition/exploit (accessed 20.02.18).
Sanger, D.E., Broad, W.J., 2017. Trump Inherits a Secret Cyberwar Against North Korean Missiles. N. Y. Times.
Sanger, D.E., Kirkpatrick, D.D., Perlroth, N., 2017. The World Once Laughed at North Korean Cyberpower. No More. [WWW Document]. N. Y. Times. URL https://www.nytimes.com/2017/10/15/world/asia/north-korea-hacking-cyber-sony.html (accessed 16.02.18).
Security Response, 2017. Lazarus: History of mysterious group behind infamous cyber attacks [WWW Document]. Symantec Secur. Response. URL https://medium.com/threat-intel/lazarus-attacks-wannacry-5fdeddee476c (accessed 06.03.18).
Sheridan, K., 2018. 8 Nation-State Hacking Groups to Watch in 2018 [WWW Document]. DarkReading. URL https://www.darkreading.com/attacks-breaches/8-nation-state-hacking-groups-to-watch-in-2018/d/d-id/1331009?image_number=3 (accessed 14.02.18).
Siciliano, R., 2015. What is a Remote Administration Tool (RAT)? [WWW Document]. McAfee Blog. URL https://securingtomorrow.mcafee.com/consumer/identity-protection/what-is-rat/ (accessed 04.11.16).
Sin, S., 2016. Another Tool in the Arsenal [WWW Document]. Cipher Brief. URL https://www.thecipherbrief.com/article/asia/another-tool-in-the-arsenal (accessed 15.02.18).
Solon, O., 2017. WannaCry ransomware has links to North Korea, cybersecurity experts say [WWW Document]. The Guardian. URL https://www.theguardian.com/technology/2017/may/15/wannacry-ransomware-north-korea-lazarus-group (accessed 13.02.18).
Song, J., Harris, B., 2018. Bitcoin tumbles as South Korea plans trading ban [WWW Document]. Financ. Times. URL https://www.ft.com/content/0d5ff7d4-f67d-11e7-88f7-5465a6ce1a00 (accessed 22.02.18).
South Korea Blames North Korea for Cyberattack [WWW Document], 2013. . Hamedia. URL http://hamodia.com/2013/07/17/south-korea-blames-north-korea-for-cyberattack/ (accessed 14.02.18).
South Korea to Launch Cyber Warfare Command [WWW Document], 2011. . Army Technol. URL http://www.army-technology.com/news/news74048-html/ (accessed 20.02.18).
SWIFT, 2018. Discover SWIFT [WWW Document]. SWIFT. URL https://www.swift.com/about-us/discover-swift (accessed 19.02.18).
Symantec Security Response, 2015. Duuzer back door Trojan targets South Korea to take over computers [WWW Document]. Symantec Secur. Response. URL https://www.symantec.com/connect/blogs/duuzer-back-door-trojan-targets-south-korea-take-over-computers (accessed 06.03.18).
Talmadge, E., 2017. North Korea, cyberattacks and "Lazarus": What we really know [WWW Document]. Phys.org. URL https://phys.org/news/2017-06-north-korea-cyberattacks-lazarus.html (accessed 13.02.18).
Tarakanov, D., 2013. The "Kimsuky" Operation: A North Korean APT? [WWW Document]. Securelist. URL https://securelist.com/the-kimsuky-operation-a-north-korean-apt/57915/ (accessed 05.03.18).
TechTarget, 2015. watering hole attack [WWW Document]. TechTarget. URL http://searchsecurity.techtarget.com/definition/watering-hole-attack (accessed 29.11.16).
TechTerms, 2007a. Torrent [WWW Document]. TechTerms. URL https://techterms.com/definition/torrent (accessed 05.03.18).
TechTerms, 2007b. BitTorrent [WWW Document]. TechTerms. URL https://techterms.com/definition/bittorrent (accessed 05.03.18).
Tosi, S.J., 2017. North Korean Cyber Support to Combat Operations. Mil. Rev. 43–51.
Trend Micro, 2017. Ransomware [WWW Document]. Trend Micro. URL https://www.trendmicro.com/vinfo/us/security/definition/ransomware (accessed 19.02.18).
Uchill, J., 2017. North Korea-aligned hackers branching out into mobile phones: report [WWW Document]. The Hill. URL http://thehill.com/policy/cybersecurity/361166-north-korea-aligned-hackers-branching-out-

into-mobile-phones-report (accessed 13.02.18).
United Nations Security Council, 2017a. Resolution 2371, S /RES/2371.
United Nations Security Council, 2017b. Resolution 2375, S /RES/2375.
United Nations Security Council, 2016a. Resolution 2270, S /RES/2270.
United Nations Security Council, 2016b. Resolution 2321, S /RES/2321.
United Nations Security Council, 2013a. Resolution 2087, S /RES/2087.
United Nations Security Council, 2013b. Resolution 2094, S /RES/2094.
United Nations Security Council, 2009. Resolution 1874, S /RES/1874.
United Nations Security Council, 2006. Resolution 1718, S /RES/1718.
US-CERT, 2017. Alert (TA17-318B) HIDDEN COBRA – North Korean Trojan: Volgmer [WWW Document]. US-CERT. URL https://www.us-cert.gov/ncas/alerts/TA17-318B (accessed 21.02.18).
Waddell, K., 2016. Is It Wise to Foil North Korea's Nuclear Tests With Cyberattacks? [WWW Document]. The Atlantic. URL https://www.theatlantic.com/technology/archive/2017/03/north-korea-cyberattack-nuclear-program/518634/ (accessed 20.02.18).
Wilder, D., 2016. The Cyber Bandit State [WWW Document]. Cipher Brief. URL https://www.thecipherbrief.com/article/asia/the-cyber-bandit-state (accessed 15.02.18).
Williams, M., 2013a. #OpNorthKorea brings more attacks on DPRK websites [WWW Document]. North Korea Tech. URL https://www.northkoreatech.org/2013/03/30/tango-down-more-attacks-on-dprk-websites/ (accessed 06.03.18).
Williams, M., 2013b. Analyzing the June 25 DDoS attacks [WWW Document]. North Korea Tech. URL https://www.northkoreatech.org/2013/06/27/analyzing-the-june-25-ddos-attacks/ (accessed 06.03.18).
Zetter, K., 2016. Hacker Lexicon: What Are CNE and CNA? [WWW Document]. WIRED. URL https://www.wired.com/2016/07/hacker-lexicon-cne-cna/ (accessed 20.02.18).
Zetter, K., 2015. The US Tried to Stuxnet North Korea's Nuclear Program [WWW Document]. WIRED. URL https://www.wired.com/2015/05/us-tried-stuxnet-north-koreas-nuclear-program/ (accessed 28.02.18).
Zetter, K., 2014. DarkHotel: A Sophisticated New Hacking Attack Targets High-Profile Hotel Guests [WWW Document]. WIRED. URL https://www.wired.com/2014/11/darkhotel-malware,/ (accessed 28.02.18).

CSS
ETH Zurich

The **Center for Security Studies (CSS) at ETH Zurich** is a center of competence for Swiss and international security policy. It offers security policy expertise in research, teaching and consulting. The CSS promotes understanding of security policy challenges as a contribution to a more peaceful world. Its work is independent, practice-relevant, and based on a sound academic footing.