Boym Institute

INTERNET, CRYPTOCURRENCIES & BLOCKCHAINS IN NORTH KOREA

Nicolas Levi

[Boym Institute]

INTERNET, CRYPTOCURRENCIES & BLOCKCHAINS IN NORTH KOREA

Nicolas Levi

INTRODUCTION

North Korea is considered as a secretive state. Paradoxically, the country is developing last trend technologies.

The scope of this work is related to the development of cryptocurrencies in the context of the DPRK. The report starts with a presentation of the IT sector in North Korea. The second chapter is focused on the development of Internet in North Korea. The two last chapters are dealing with North Korean's IT attacks and the key organizations driving these issues.

The objectives of this study are to address key issues and critical paths for dangers associated to the bitcoins industry form the perspective of the DPRK. This report can be considered as crucial, as The IT sector in North Korea is a sub-cell of the North Korean economy which was analyzed only by a few western analysts.

1. THE IT SECTOR IN NORTH KOREA

In spite of its secretive nature, the North Korean state proved its interests in ICT already in the 80's[1]. The first public institution responsible for the development of the access to IT products was the KCC (조선컴퓨터위원회 – Chosŏnk'ŏmp'yut'ŏwiwŏnhoe). One of its director was Kim Jong Nam (1971-2017), the eldest son of Kim Jong Il. He was appointed over there in the early 90's. The latest known director is Han U-chol. The most famous North Korea IT product is probably the Operating System Red Star (붉은별; – Pulgŭnbyŏl), based on Linux and with a first development stage initiated in 1998 at the previously mentioned North Korean Computer Committee is a North Korean Linux distribution, with development first starting in 1998 at the KCC. Version 3.0 was released in the summer of 2013, but as of 2014, version 1.0 continues to be more widely used.

To attract foreigners and IT specialists, North Korean authorities organized on a regular basis technological exhibition. The first one took place in 1999. During this event, the main North Korean universities (such as the Kim Il-sung University and the Kim Chaek University of Technology[2]) and public institutions (Pyongyang Information Technology Bureau) are promoting their knowledge and its latest softwares including linguistic translation tools, anti-virus programs and the organization of computer-based painting exhibitions. There are several other institutions which train North Korean hackers such as the University Mirim, the Computer Tech-

nology University of Hamheung[3], the Computer Technology University of Pyongyang[4], the Kim Il Sung Military Academy, and the Moranbong University[5].

2. INTERNET IN NORTH KOREA

As of 2019, North Korea is known as being the only one in the world that does not grant an open access to its citizens[6]. However, there is an internal Internet in North Korea known as Kwangmyong (광명) providing e-shops, dating websites, news, and a content taken from Internet after the censorship[7]. The Kwangmyong network began to be developed in 1995, and was opened nationwide in 1998. The Kwangmyong network is only available within North Korea.

As stipulated before, there is no private Internet service provider in North Korea. However, some government elites are accessing the Internet via a Chine provider based in China. Thousands of companies and state organizations have intranet addresses. During the three years from 2004 to 2007, North Korea has connected optical cables for intranets to major cities and towns. The data transmission speed in Pyongyang is 70 ~ 80Mbps and the local speed is 10Mbps, which is the level of South Korea in 2000. In 2006 all intranet access at home were blocked and all PC rooms in Pyongyang were closed till 2015[8]. Foreigners have an access to Internet through special devices and the North Korean company Koryolink, however at a prohibitive rate (EUR 0,15 per Mb). This allow foreign reporters based in Pyongyang to wrote tweets in Pyongyang.

In 2010, Korean state organizations registered Twitter, YouTube and Facebook accounts. The majority of them were blocked by the previously mentioned western firms.

Table 2. Number of IP addresses in North Korea

Type (year between brackets)	Number of registered IP adresses
Maximum (2013)	*26100*
Minimum (2008)	*2800*

Last data (2015)	*13000*
Previous data (2014	*7700*

Source: Trading Economics Korea. Data are provided for the period 2008-2015

The number of IP address assigned to North Korea consists of an important source of information as these IP addresses are more noteworthy. For instance, according to the AT&T Consulting company[9], some North Korean IP address are notorious as they were used to control compromised web-servers in a set of 2014/2015 attacks linked to North Korea known as BlackMine[10]. However, it does not mean that we deal with the same people involved in the 2014/2015 attacks.

The access to e-mails is also prohibited to a large extent. It's impossible from abroad to send an email to North Korea if the receiver didn't confirm your e-mail address to North Korean authorities. Furthermore, any answers are usually sent within a few days, which is an improvement as a few years ago, foreigner used to wait several weeks before getting any answer. North Korean diplomats have also only a group e-mail. In other words, diplomats attached to an embassy have only one e-mail for all diplomats.

3. NORTH KOREAN IT ATTACKS

The continuing round of sanctions imposed on North Korea by the UN aims to target some of the country's main external revenue streams. With prohibitions restricting the flow of money, the country is turning to bitcoin and other cryptocurrencies to finance their programs, instead of coming under new pressure. Moreover, it has been reported that Kim Jong-un's regime targets cryptocurrency trading in South Korea, with at least three confirmed successful attacks. When attacking bitcoins platforms in South Korea, the Lazarus Group The first cryptocurrency-focused lure appears designed to obtain the emails and passwords of users of South Korean cryptocurrency exchange platforms (for instance from the platform Coinlink).

The most famous attack took place in 2014 and was related to Sony Picture's hijacking and due to the movie "The Interview"[11]. One year later,

the account of the Central Bank of Bangladesh at the Federal Reserve Bank in New York was robbered with USD 80 million. Hackers tried to transfer financial assets to some accounts localized in Sri Lanka and the Philippines. Unfortunately for them, on the 5th transaction, a mistake was done. Hackers wrote fandation instead of foundation, when they wanted to transfer some funds to an organization called Shalika Foundation. In 2017 due to the spread of the WannaCry virus, european institutions (and especially the Polish Financial Supervision Authority[12]) was hacked. On the same year, in October the Taiwan Far Eastern International Bank was also robbered[13]. During the following years, attacks were more focused on financial institutions in African countries, South Korea, or Vietnam. In march 2019, an Israeli institution was also attacked[14].

On the other side, North Korean authorities decided to participate to the cryptocurrencies market, considering it as a source of foreign currency. The first transactions of bitcoins in North Korea were realized in 2014[15]. In order to improve its image, North Korean authorities organized one Blockchain and Cryptocurrencies conference. The first one was supposed to be held in 2018. This event called the “Korean International Blockchain Conference,” would take place in Pyongyang from September 27 to October 4. However, it was cancelled. Therefore a new edition was set up for 2019. This 7-days event held from April 18th till the 25th of 2019 was organized by the Korean Friendship Association and the consulting firm TokenKey led by the 30 years old Christopher Emms[16]. Emms originally reached out to KFA to help bring the conference to North Korea, following his experience speaking at similar events in other countries in recent years. The seminar attended by more than 100 people from North Korea and abroad took place at the Pyongyang University of Science and Technology[17]. Foreign experts were invited and provided lectures on protocols related to crypto-currencies such as “mining” or blockchain. The panels related to block-chains were screened on the 22&23 April. Other sessions were done under the form of field trip at the Kim Il-sung University, Panmunjom, and at the Daedong River Beer Factory. Participants to the conference visited the War Memorial, the Pyongyang Foreign Language University, the Juche Idea Tower, the city of Kaesong and Panmunjom[18].

According to a report prepared by the UN Security Council, North Korea has managed to extort more than $ 670 million in cryptocurrencies since the beginning of its activities in 2015. 571 million dollars were allegedly stolen directly from Asian cryptocurrency trading platforms during various

hacks, such as the Japanese platform Coincheck in January 2018 where 532 million dollars were stolen of the platform Zaïf for $ 60 million. The South Korean e-commerce platform Interpark was also hacked. 10 million personal data were stolen in 2016[19].

4. THE LAZARUS ORGANIZATION

North Korean authorities set up a militia dedicated to cyber-attacks to ensure cash flow while circumventing international sanctions. For several years, cyber security experts have identified this group of hackers as Lazarus[20]. The leader of the Lazarus group[21] is supposed to be Park Jin-hyok[22]. Born on the 15 August 1994, he completed his education at the Kim Chaek University of Technology, one of the top IT University of North Korea[23] where he acquired skills in Visual C++. He's supposed to be an employee of Chosun Expo[24], a North Korean company based in northeastern China, in Dalian, a port city overlooking the gulf of Korea. He was working there between 2010 and 2014. During his malwares operations, he was also known as Kim Hyon-woo.

Sources indicate that he participated to the biggest North Korean hacks such as the WannaCry virus, which has infected hundreds of thousands of computers around the world such as the hacking of the Central Bank of Bangladesh with a $ 81 million diversion[25]. He's considered as the leader of the group of hackers Lazarus, responsible for the infiltration of the servers of the Sony Group. He also speaks English and Chinese. The Lazarus Kaspersky Lab estimates that Lazarus[26]has been active since at least 2009 utilizing the MYDOOM worm or and malicious .hwp extension files[27]. "Hwp files" are word processor file written in Hangul, the Korean writing system, used in both Koreas.

It must be also taken in consideration that even if the group of hackers are based in North Korea or at the Kim Il Sung University[28], it does not mean that they are North Korean, as North Korean education structures welcome also foreigner student, especially from China, Russia, and Vietnam.

Table 3. Structure of the Lazarus Group

Groups considered as substructures of the Lazarus entity	Specialization	Targets

Bluenoroff	Attacks of foreign financial institutions	Bangladeshi bank, Polish financial supervisory authority, South Korea Bitcoin companies, , South Korean Ministry of Defense, SWIFT banking attacks
Andariel	Attacks of private and public organizations	South Korean companies, South Korean ATMs

Source: own research

North Korea specifically targets Southeast Asia, especially since the lifting of sanctions against the country, following the meeting in Hanoi last February between Kim Jong Un and US President Donald Trump, did not work out. Cryptocurrencies stolen by North Korea, such as Bitcoin, Ethereum or XRP, would be used to:

- Fundraising: To meet its cash requirements, North Korea can obtain cryptocurrencies for the purpose of converting them into short-term currency.
- Storing funds: North Korea could accumulate cryptocurrency reserves for the purpose of spending them or converting them into currency at a given time.
- Bypass sanctions: North Korea could use cryptocurrencies to pay for goods, services and resources explicitly prohibited by international sanctions.

In December 2018, IssueMakersLab, a cybersecurity blockchain startup, explained that North Korean hackers had changed their strategy and were attacking crypto-investors directly rather than attacking crypto-exchanges.

The key-market for North Korean hackers remain South Korea as this country hosts some of the world's largest and richest bitcoin exchange platforms. North Korean hackers try to obtain an access to less-know cryptocurrencies such as Monero, the 14th largest cryptocurrency by value as of 2018. Some studies demonstrated that North Korean hackers in-

fected IT devices to mine Monero owners and send their cryptocurrencies back to North Korea[29]. It's also possible to use bitcoins in North Korea but to an extent limited to 4 restaurants in Pyongyang[30]. In any case, It is very difficult for North Korea to expand its activities related to virtual currency due to lack of electricity, lack of high-performance computer, and lack of internet infrastructure.

There is a dedicated team of South Korean specialists dedicated to domestic attacks of Lazarus[31].

Unfortunately, according to Jay Rosenberg, a senior security researcher based in North America, who belongs to Kaspersky Lab's Global Research Analyst Team (GReAT) "North Korea's cyber capabilities are improving. They will continue to attack in the future using evolved attack techniques."[32]

5. FINDINGS

The findings can be summarized as follows.

- To meet its cash requirements, North Korea can obtain cryptocurrencies for the purpose of converting them into real currencies. North Korean authorities use cryptocurrencies to have a viable source of income. Later North Korean authorities may use these cryptocurrencies for trading activities. As of 2019, North Korea has managed to extort more than $ 670 million in cryptocurrencies since the beginning of its activities in 2015.
- Previously, most of this type of attack appeared destined to cause social disruption or covert data, and the targets were usually computer networks of government agencies or media companies in countries considered hostile. In recent years, North Korean pirates seem to be more interested in stealing money. ". Therefore, The strategy of North Korean specialists changed over the year, looking for the weak link. North Korean hackers are attacking crypto-investors instead of attacking crypto-exchanges or platforms.
- We recommend to less advanced countries, which are more vulnerable to North Korean attacks, to regulate cryptocurrency platforms, and imposing anti-money laundering and anti-terrorist financing standards.
- Although, according to the document, cryptocurrencies are likely to play only a peripheral role in general fundraising and tax evasion

activities in North Korea, the authors indicate, however, that better coordination between the different countries in the region would make them less vulnerable to attacks by Kim Jong Un. It's especially important in the context of South-East Asia, where the cryptocurrency sector is booming. Fortunately, Singapore is the most advanced country in regulating and regulating cryptocurrency platforms and shall play a role of mentor for less advanced countries such as Malaysia, the Philippines and Thailand, which are vulnerable to North Korean attacks.

- Westerners who participate to the development of the bitcoin/blockchain industry in North Korean are young ventures people. We can't blame them of the development of hacking industry in North Korea.
- We have no information whether the Lazarus group consists only of North Korean workers.

DEFINITIONS

Blockchain: technology of storage and transmission of information, which functions without a central control body. By extension, a blockchain is a database that contains the history of all the exchanges made between its users since its creation. This database is secure and distributed: it is shared by its different users, without intermediaries, which allows everyone to check the validity of the chain.

Cryptocurrency or cryptographic currency is a 100% electronic and magnetic currency. Its value is the same as the currencies we use on a daily basis but it is virtual. The cryptocurrency was created based on the computer technology called blockchain.

ABOUT THE AUTHOR

Nicolas Levi (nicolas_levi@yahoo.fr) is an associate professor at the Institute of Mediterranean and Oriental Cultures of the Polish Academy of Sciences. He recently published *A statistical analysis of the North Korean overseas laborers in Poland during the period 2000-2017: Current Status and Prospects* (Asian Century, 2018). and coauthored (with prof. Kyungyon Moon) a research paper entitled *Historical Relations between Poland and North Korea from 1948 to 1980* (vol. 27, nr 1,

2018 - International Journal of Korean Unification Studies, pp. 29-71,). Holding a PhD regarding the North-Korean leadership, his personal website (nkreports.wordpress.com) focuses on North Korea issues.

BIBLIOGRAPHY

[1] Computers were also considered as gifts from Kim Jon gil for Senior Elites, especially in the early 2000's. 북한 주요인사 –인물정보, 2017, 통일부, p. 692.

[2] The latest known head of the computer faculty of the Kim Chaek University of Technology is Rim Won-gi.

[3] The latest known head of this University is Ri Hak-sun.

[4] The latest known head of this University is Jeon Ja-hyok.

[5] Jang Sae-yul, 북, 정찰총국 해커부대 다시 중국에 진출, http://www.lkp.news/news/article.html?no=4961 (accessed: 14.06.2019)

[6] Internet is blocked to a lower extent in Erythrea.

[7] Tudor, D., & Pearson, J. (2015). *North Korea confidential: private markets, fashion trends, prison camps, dissenters and defectors*. Tuttle Publishing, p. 62.

[8] Ju Song-ha, '지구촌 인터넷 혁명, 北 파고들 가능성은…' 美방송위 토론회, http://www.donga.com/news/Inter/New/article/all/20110216/34887225/1, (accessed: 2 April 2019).

[9] AT&T is a is a developer of commercial and open source solutions to manage cyber attacks.

[10] https://www.alienvault.com/blogs/labs-research/a-north-korean-monero-cryptocurrency-miner (accessed: 12.06.2019)

[11] Sun Heidi Saebo, Kim Dzong Un – Szkic Portretu Dyktatora, wyd. Czarne, Wołowiec 2019, p. 297.

[12] *Komisja Nadzoru Finansowego* (https://www.knf.gov.pl) in Polish.

[13] Sun Heidi Saebo, Kim Dzong Un – Szkic Portretu Dyktatora, wyd. Czarne, Wołowiec 2019, p. 299.

[14] Oded Yaron, *North Korean Hackers Cited in Rare Attack in Israel*, https://www.haaretz.com/israel-news/business/.premium-north-korean-hackers-cited-in-rare-attack-in-israel-1.7059457, „Haaretz.com", 26 March 2019 (accessed 10.06.2019).

[15]가상화폐 비트코인 북한서 '첫 거래', https://m.yna.co.kr/view/MY-H20140109011300038, 9 January 2014 (accessed: 21.04.2019))

[16] "평양서 첫 블록체인 국제대회…*100*여명 참가", https://www.rfa.org/korean/in_focus/food_international_org/blockchain-04192019143335.html, „Rfa.org" (accessed 14.5.2019)

[17] "북한 블록체인 행사에서 동아시아 블록체인 프로젝트 소개", http://www.nkeconomy.com/news/articleView.html?idxno=1378. 2 May 2019 (accessed: 20.5.2019).

[18] About 50-60 people were supposed to participate to this event. Due to security reasons, the list of participants was undisclosed. 북한 블록체인 컨퍼런스 '또' 열린다…AI도 추가. http://www.thebchain.co.kr/news/articleView.html?idxno=4225 (accessed: 10.4.2019).

[19]경찰은 인터파크 해킹을 '북한' 소행으로 판단했다, https://www.huffingtonpost.kr/2016/07/28/story_n_11234790.html (accessed: 20.03.2019).

[20] The first group of North Korean hackers was settled in a North Korean Hotel in Shenyang (aka the Chilbosan hotel) where North Koreanhackers used to live in the early 2000's. The hotel was shut down in January 2018.

[21]라자루스 그룹 in Korean.

[22] A.k.a Pak Jin-hek.

[23] A team of students of the KimChaek University of Technology obtained the 8th position in the International Collegiate Programming Contest

[24] A.k.a. Korea Expo Joint Venture. Interestinly Chosun Expo was originally a joint venture between North Korea and South Korea established to be a Korean e-commerce and lottery website. The South Korean partners retired a few years ago from this venture. Chosun Expo i san entity working under the auspices of the room 110 (aka Lab 110) of the WPK. The company is a.k.a. Korea Expo Joint venture Corporation. Sanctions against this company were applied in October 2018.

[25] Sun Heidi Saebo, *Kim Dzong Un – Szkic Portretu Dyktatora*, wyd. Czarne, Wołowiec 2019, p. 299.

[26] The Lazarus Group is also known as APT 38, HIDDEN COBRA, Guardians of Peace, Whois Team and Zinc. The most common name is the Lazarus Group.

[27] Lee Yu-ji, "북한 해킹그룹 '라자루스'의 공격은 멈추지 않았다", 23 May 2019, https://byline.network/2019/05/23-43/ (Accessed: 20.06.2019); Guerrero-Saade, J. A., & Moriuchi, P. (2018). North Korea targeted South

Korean cryptocurrency users and exchange in late 2017 campaign. Recorded Future, 16, p. 3.

[28] In the mid 80's, it was already possible to study Computer Science at the Kim Il Sung University. The majority of the equipment were donations from other communist countries such Bulgaria and Poland, but also bought from Japan, or Singapore. There was also a computer laboratory at the Kim Chaek University of Technology. Martin, Bradley K. *Under the loving care of the fatherly leader: North Korea and the Kim dynasty*. Macmillan, 2004., p. 347; p. 610.

[29]김일성종합대학, 모네로 채굴기 전파하고 있다, https://www.boannews.com/media/view.asp?idx=65981 (Accessed: 10.5.2019).

[30] 북한의 가상통화 이용 현황, 김민관, *KDB* 산업은행 미래전략연구소, http://www.spnews.co.kr/news/articleView.html?idxno=12630 (Accessed: 22.06.2019)

[31] One of these IT specialists is identified as being Park Seong-su.

[32] Lee Yu-ji, "북한 해킹그룹 '라자루스'의 공격은 멈추지 않았다", 23 May 2019, https://byline.network/2019/05/23-43/ (accessed: 0.06.2019)