Recorded Future

CYBER THREAT ANALYSIS

North Korea Relies on American Technology for Internet Operations

By Priscilla Moriuchi and Fred Wolens
Recorded Future

CTA-2018-0606

Scope Note: Insikt Group examined North Korea's technology architecture by analyzing third-party data, IP geolocation, Shodan port scans, user agents, and open source intelligence (OSINT) using a number of tools. This is a follow up to our April 2018 analysis on the North Korean elites' internet behavior. The data analyzed for this report spans from December 1, 2017 through April 15, 2018.

Executive Summary

In April 2018, Recorded Future published research on the internet browsing behavior of North Korea's most senior leaders and revealed stark changes in how North Korea's ruling elite utilize the internet from our original analysis in July 2017. Utilizing a data set spanning from December to mid-April, we compiled a significant amount of information on North Korea's technology architecture, including which types, manufacturers, and models of hardware and software North Korean leaders used to access the internet.

Our analysis reveals the overwhelming presence of American hardware and software on North Korean networks and in daily use by senior North Korean leaders. We also examined the broad legal regime that restricts U.S. trade with North Korea and discovered that it is insufficient to prevent U.S. electronics, hardware, and software from reaching North Korea.

Key Judgments

- This failure to keep American technology from reaching North Korea has enabled North Korea's destabilizing, disruptive, and destructive cyber operations as well as its internet-enabled circumvention of international sanctions.
- International inconsistency in the definition of the term "luxury goods" has also facilitated the Kim regime's acquisition of American technology.
- For seven years, between 2002 and 2017, the United States allowed the exportation of "computer and electronic products" to North Korea, totaling more than $430,000. Our analysis demonstrates that many of the electronic devices North Korean elite utilize are older models or are running older software, and that at least some of those devices could have been legally acquired from the U.S. during these seven years.
- All U.S. exporters are liable for any violation of the sanctions regime, but beyond the implementation of a robust compliance program, there's relatively little that can be done to actually stop prohibited goods from reaching sanctioned countries. This is especially true for North Korea, as they have proven to be sophisticated at utilizing intermediaries or spoofing identities.

History of Export Controls Against North Korea

Since the split of North and South Korea following World War II, the United States has regarded the Democratic People's Republic of Korea (DPRK or North Korea) as an adversary. Despite the lack of open hostilities for nearly 65 years, the U.S. has never normalized diplomatic relations with the "Hermit Kingdom." From the 1950s to 1980s, North Korea's status as a Communist government, and sponsorship of international terrorism, ensured that the two countries remained enemies. Then, in 1988, after the bombing of Korean Air Flight 858, North Korea was officially designated as a state sponsor of terrorism by the Reagan administration, inaugurating the modern export control regime against North Korea.

Separately, export control as a response to North Korea's nuclear proliferation efforts dates back to 1992 when the U.S. imposed sanctions on two North Korean companies due to their missile proliferation activities. Between June 1992 and June 2000, some restrictions were lifted as a result of the U.S.-North Korea bilateral missile talks, but the respite was short lived and the U.S. ratcheted up sanctions from January 2001 through to 2006. This period included the notorious labeling of North Korea as part of the "Axis of Evil" in President Bush's 2002 State of the Union Address.

In 2006, the first widespread international sanctions began after North Korea carried out its initial nuclear weapons test. This test prompted the UN Security Council (UNSC) to pass two resolutions imposing sanctions on North Korea — first Resolution 1695, and then Resolution 1718. These resolutions together banned a broad range of both imports and exports to North Korea by any UN member states.

While these resolutions initially focused on military materiel, they were supplemented by broader sanctions from the U.S., Australia, and Japan. After North Korea conducted its second underground nuclear test in May 2009, the UNSC adopted Resolution 1874, which further expanded the arms embargo and sought to target Pyongyang's financial apparata. From 2009 to the present day, both the U.S. and UNSC have progressively strengthened and expanded earlier sanctions with Resolution 2087, 2094, 2270, 2371, 2375, and 2397, which covered everything from missile materiel to textiles and caps on oil trading.

Despite a perceived thaw in diplomatic relations beginning earlier this year, U.S. officials have re-emphasized numerous times that "all sanctions and maximum pressure must remain," while denuclearization of the Korean peninsula is negotiated.

State of Current U.S. Sanctions Against North Korea

Current United States sanctions against North Korea can be split into two categories:

1. Sanctions that specifically target North Korea.
2. Sanctions related to "Weapons of Mass Destruction Proliferators."

Until 2008, the bulk of U.S. sanctions specific to North Korea were implemented via the Trading With the Enemy Act (1917), which empowers the federal government to prohibit any and all trade with designated countries. On June 26, 2008, the Bush administration issued Executive Order (E.O.) 13466 under the authority of the International Emergency Economic Powers Act. That same year, the National Emergencies Act. E.O. 13466 was supplemented by Executive Orders 13551, 13570, 13687, 13722, and the North Korea Sanctions Regulations (31 C.F.R. part 510). These measures extended a variety of trade restrictions and blocking of interests belonging to various figures in North Korea.

Pre-dating these sanctions, E.O. 13382 was issued in 2005 targeting various entities engaged in WMD proliferation. Three North Korean entities and numerous North Korean persons were listed as blocked entities.

Today, these regulations have culminated in six prohibited categories of transactions involving North Korea:

1. Blocked property belonging to the state of North Korea and certain North Korean nationals (E.O. 13466, 13551, 13687, 13722, and 13382).
2. U.S. persons are prohibited from registering vessels in North Korea, flying the DPRK flag, or operating any vessel flagged by North Korea (E.O. 13466).
3. Goods, services, and technology from North Korea may not be imported into the U.S. (E.O. 13570).
4. No new investment in North Korea by U.S. persons is allowed (E.O. 13722).
5. No financing by a U.S. person involving North Korea is allowed (E.O. 13722).
6. And most importantly for our purposes, goods, services, and technology may not be exported to North Korea from the U.S., or by a U.S. person wherever located, without a license (E.O. 13722).

U.S. export enforcement responsibility falls under three executive branch agencies: the Office of Foreign Asset Control within the Department of Treasury, the Office of Export Enforcement within the Department of Commerce's Bureau of Industry and Security, and Homeland Security Investigations within the Department of Homeland Security. These three agencies enforce the Executive Orders, U.S. sanctions, International Trafficking in Arms Regulation, Export Administration Regulation, and other laws which make up the

body of export control laws in the United States. In 2010, Executive Order 13558 created the Export Enforcement Coordination Center to further strengthen the partnership between these independent agencies.

The United States is one of the only countries which enforces its export laws outside of its national boundaries. Federal agents located in foreign countries work in conjunction with local authorities to conduct end use license checks, knocking on doors to see whether the parties are still upholding their stated exporting intentions.

Currently, civil penalties of up to the greater of $284,582, or twice the amount of the transaction, can be imposed against any party that violates these sanctions. Similarly, upon conviction, criminal penalties of up to $1 million, imprisonment for up to 20 years, or both, may be imposed on any person that willfully violates the sanctions.

North Korea Leverages a Breadth of U.S. Technology Despite Export Controls

North Korea's Technology Architecture

Numerous third-party data sources used for this analysis gave Recorded Future visibility into what types of devices North Korea's most senior leadership use to access the global internet. As has been widely publicized over the past several years, Kim Jong Un has been photographed on several occasions with Apple devices, and North Korean-made mobile phones have been assessed as mimicking Apple technology.

While we cannot confirm the actual users behind the activity we see, our analysis indicates that numerous American and Western-manufactured devices are being used by North Korean elite to access the global internet. Several reports and accounts have documented how few North Koreans are granted access to the global internet. At most, only the inner circle of North Korea's leadership, such as party, military, and intelligence leaders and their families, are allowed to own computers and independently utilize the global internet. This is one of the data points we use to determine with such certainty that North Korea's ruling elite are the users of this hardware and software.

North Korea's use of proxies and load balancers limited our ability to identify exactly how many of each device was present, but we can determine some models and versions:

- Windows 7
- Windows 8.1
- Windows 2000
- Windows XP
- Windows 10

- Microsoft Terminal Server
- Samsung Galaxy S5
- Samsung Galaxy J5
- Samsung Galaxy S7
- Samsung Galaxy S8 Plus
- Huawei Mate 95c 6 v6
- Apple iPhone 4S
- Apple iPhone 5
- Apple iPhone 5S
- Apple iPhone 6
- Apple iPhone 6S Plus
- Apple iPhone 7 Plus
- Apple iPhone 8 Plus
- Apple iPhone X
- Apple MacBook
- IBM Tivoli Storage Manager server
- Conexant Hasbani web servers
- Ascend Communications[1] switches
- F5 BIG-IP load balancer

While the majority of North Korean cyber operations are likely conducted from abroad, a small minority historically have been conducted from territorial North Korea. These operations have been conducted utilizing this very same hardware and software. This means that minimally, U.S. technology has enabled North Korea's destabilizing, disruptive, and destructive cyber operations as well as its internet-enabled circumvention of international sanctions.

Where Technology Export Control Fails

According to a Congressional Research Service study conducted in 2016, U.S. trade restrictions with North Korea are extensive, but do not amount to a comprehensive embargo.

> *The United States curtails trade with North Korea for reasons of regional stability, that country's support for acts of international terrorism, lack of cooperation with U.S. antiterrorism efforts, proliferation, and its status as a Communist country and a nonmarket economy. The United States also prohibits transactions relating to trade with certain North Korean entities identified as those who procure luxury goods, launder*

[1] Ascend Communications was acquired by Lucent Technologies in 1999, which was then acquired by Nokia in 2016.

> *money, smuggle bulk cash, engage in counterfeiting goods and currency, and traffic in illicit narcotics.*

Further, "a U.S. company may apply for a license to export to North Korea, but for nearly all items other than food and medicine, there is a presumption of denial."

This is despite the fact that North Korea has been on and off the State Sponsors of Terrorism list twice in the last 10 years (President Bush rescinded the declaration in 2008 and President Trump re-applied it in November 2017). In terms of exportation of technology to North Korea, the State Sponsors of Terrorism designation has relatively little impact in and of itself because the sanctions resulting from that designation govern primarily U.S. foreign aid, defense exports, and dual-use items. There is a provision for sanctions on "miscellaneous financial and other restrictions," however, it is not clear whether that provision goes above and beyond the existing prohibitions on technology exports to North Korea.

Most electronics, including laptop computers, digital music players, large flat-screen televisions, and "electronic entertainment software" are considered "luxury goods" and fall under the broad trade Export Administration Restrictions (EAR) for North Korea administered by the Department of Commerce.

While the United Nations (UN) clarified its definition of "luxury goods" in Resolution 2321 as not including electronics, each UN member state is allowed to interpret the "luxury goods" term as including different products, "creat[ing] a situation of uneven practice" in the application of export controls. For instance:

- The European Union bans "electrical/electronic items and appliances for domestic use of a value exceeding EUR 50 each."
- Australia bans all "consumer electronics."
- Japan prohibits "portable computing devices consisting of at least a central processing unit (CPU), a keyboard, and a display."
- South Korea broadly restricts and governs trade with the North including "electronic goods" as a luxury item.
- China has not made a distinction on embargoed luxury goods and does not "honor the luxury goods lists of other countries when it exports to" North Korea.

The Saga of ZTE

In March 2016, Zhongxing Telecommunications Equipment (ZTE), a Chinese cellular device and hardware manufacturer, was added to the Export Administration Regulations (EAR) Entities List. The EAR "imposes additional licensing requirements on and limits the availability of most license exceptions for, exports, reexports, and transfers (in-country) to those listed" on the Entities List. ZTE was initially placed on the Entities List for violating U.S. sanctions by selling American-made goods to Iran and North Korea. Placement on the Entities List prohibited U.S. companies from selling goods to ZTE without a license, and because nearly all ZTE-manufactured products contained U.S. goods, essentially crippled the company.

For more than two years, ZTE and the U.S. government went back and forth attempting to reach an agreement over penalties and validate that ZTE was no longer violating U.S. sanctions. In April 2018, the Department of Commerce (DOC) ended the negotiations by imposing a denial order, prohibiting American companies from selling to ZTE for seven years.

The denial order was the end of a lengthy export control enforcement process which would have bankrupted ZTE. Instead, in late May, the DOC negotiated an agreement which lifted the denial order and re-opened ZTE to U.S. exports.

The case of ZTE, a company which was placed on the Entities List and under a denial order for violating U.S. sanctions against North Korea, is a useful example of how impactful successful export control can be — if allowed to be. Had ZTE been allowed to fail, it would have sent a powerful message to companies around the world indicating how seriously the U.S. considers these violations. Instead, the message is that a company can violate U.S export controls and sanctions if it is large enough and aligned with an economically powerful nation.

Technology Exports to North Korea Were Not Always Prohibited

The question of how U.S. technology gets to North Korea is not entirely a story of failed export control or inconsistent application. According to Department of Commerce data, the U.S. has actually exported over $176 million of goods to North Korea since 2002. While this number pales in comparison to export volume with nations such as China or Canada, it is important to note that the export of "computers and electronic products" to North Korea has occurred.

At its peak in 2014, the U.S. exported $215,862 worth of computers and electronic products to North Korea. We do not know exactly which products or how many were exported to North Korea that year. However, based on the Department of Commerce definition of "computers and electronic products," we have an idea of what kind of electronics these exports might have included. This category includes "computers, computer peripherals (including items like printers, monitors, and storage devices), communications equipment (such as wired and wireless telephones), and similar electronic products (including audio and video equipment and semiconductors)," as well as components for these products.

Again, while we do not know exactly which computer and electronic products were exported to North Korea over the past 15 years, that data can be useful in an exercise to demonstrate exactly how much value North Korea could have derived from that amount of money.

For example, in 2014, a decent desktop could cost around $500, while a similarly specified laptop would cost $700. Hypothetically, if North Koreans were paying the average prices for computers, they could have purchased over 350 computers from U.S. suppliers in 2014 alone. In total, since 2002, the U.S. has legally exported $483,543 worth of computers and electronics to North Korea — a sum that could have legally supplied some of the ruling elites' electronics needs.

Our analysis demonstrates that many of the electronic devices North Korean elite utilize are older models or are running older software. These legal exports certainly do not account for all of the devices we have observed on North Korean networks, nor is $483,543 sufficient to completely build a moderately sized and proxied network. However, it presents an interesting part of the answer to the question of exactly how North Korea could have acquired all of their Western hardware and software. At least some of the computers and software we observed being used in North Korean networks today was probably acquired during these past 15 years.

Outlook

It is the responsibility of any U.S. exporters to be familiar and compliant with federal export controls, as penalties can include fines, civil or criminal charges, imprisonment, negative publicity, revocation of exporting privileges, or debarment from U.S. government contracting. As explained by the Massachusetts Export Center, "[Even if the exporter is selling only] *innocuous products or selling only to 'friendly' countries … the exporter is ultimately responsible to have a thorough understanding of export regulations and to establish operating procedures aimed at preventing violations.*"

For U.S. companies and persons to avoid the risk of being found guilty of violating sanctions, it is expected that an effective export compliance program is implemented. The U.S. Department of Commerce's Bureau of Industry and Security suggest eight elements for an effective program:

1. Statements and commitments from management
2. Risk assessment of potential export violations
3. Export authorization
4. Effective record keeping
5. Instituting training programs for employees
6. Auditing records
7. Detecting and correcting export violations
8. Maintaining an export compliance manual

Generally, all U.S. business are not expected to perfect all eight elements, but any deviation from a robust compliance program poses a risk that an entity could be found in violation of the U.S. export regime. However, while a U.S. company may have a robust program, sanctioned states often use false flags or non-national facilitators to skirt even the most advanced programs. As a recent report from Arms Control Wonk and Reuters pointed out, the North Koreans are adept at falsifying addresses and names to circumvent sanctions programs. This flow of technology is not one way, either — recent reports point out that North Korea has used shell companies and various aliases to export various technologies, including facial recognition software to U.S. allies and encryption software in Asia.

One transaction involving the DPRK shell company Glocom that was widely reported last year demonstrates the ease with which North Korea is able to avoid technology control sanctions. Glocom used a network of Asian-based front companies to purchase components from electronic resellers, and the payment was even cleared through a U.S. bank account. Glocom, the company at the center of these transactions, was tied to Pan Systems Pyongyang via invoices uncovered by the UN and International Global System via WHOIS website registration data. Ryang Su Nyo is listed as a director of Pan Systems Pyongyang and a shareholder of International Global System, and Reuters has reported that Ryang reports to "Liaison Office 519," a department within the North Korean Reconnaissance General Bureau.

Today, the varied interpretation of the term "luxury goods," a sophisticated sanctions evasion operation, and lax enforcement of technology and electronics as a subcategory has created a situation where the Kim regime can acquire U.S. electronics, software, and hardware virtually at will. Technology resellers, North Koreans abroad, and the Kim regime's extensive criminal networks all facilitate the transfer of American technology for daily use by one of the world's most repressive governments. Unless there's a globally unified effort to impose comprehensive sanctions on the DPRK, and multilateral cooperation to ensure that these sanctions cannot be thwarted by a web of shell companies, North Korea will be able to continue its cyberwarfare operations unabated with the aid of Western technology.