North Korea's Ruling Elite Are Not Isolated

In-depth analysis of North Korean internet activity reveals an informed, modern, and technologically savvy ruling elite.

by Insikt Group

Recorded Future

Executive Summary

This is part two of our series on North Korea. In part one entitled "North Korea Is Not Crazy," we revealed that North Korean cyber actors are not crazy or irrational: they just have a wider operational scope than most other intelligence services.

Here we enrich our analysis via our intelligence partner, Team Cymru, and conduct a comprehensive study revealing unique insights into how North Korean leadership and ruling elite use the internet and what that can tell us about their plans and intentions.

Our analysis demonstrates that the limited number of North Korean leaders and ruling elite with access to the internet are actively engaged in Western and popular social media, regularly read international news, use many of the same services such as video streaming and online gaming, and above all, are not disconnected from the world at large or the impact North Korea's actions have on the community of nations. Further, we have concluded that:

› Attempts to isolate North Korean elite and leadership from the international community are failing. In fact, their internet activity is in many ways not that different from most Westerners.

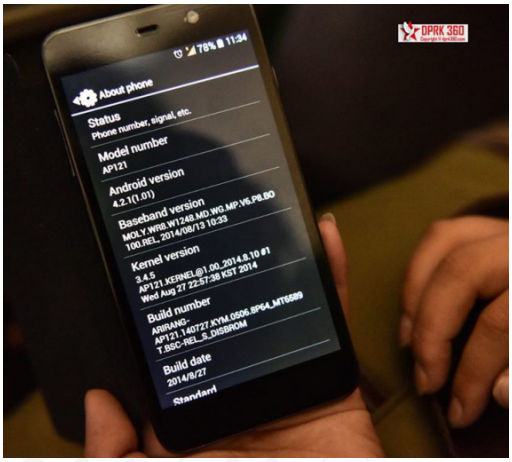
› The data set reviewed suggests that general internet activity in North Korea may not provide early warning of a strategic military action, contrary to conventional hypotheses. If there is a correlation between North Korean activity and missile tests, it is not telegraphed by leadership and ruling elite internet behavior.

› North Korea is not using territorial resources to conduct cyber operations and most North Korean state-sponsored activity is likely perpetrated from abroad, which presents an opportunity to apply asymmetric pressure on the Kim regime.

This analysis, together with part one of our blog series, demonstrates that there are likely other regime pressure points, and as a result, other tools, techniques, and partners that could be explored toward a path for North Korean denuclearization.

Background

South Korean media assesses that there may be as many as 4 million mobile devices in North Korea. So while mobile devices are widespread in North Korea, the vast majority of North Koreans do not have access to the internet. Mobile devices (see image of a North Korea-made device below) sold to ordinary North Koreans are enabled with minimal 3G services, including voice, text messaging, and picture/video messaging, and are restricted to operating only on North Korea's domestic provider network, Koryolink.



A small minority of users, such as university students, scientists, and select government officials, are allowed access to North Korea's domestic, state-run intranet via common-use computers at universities and internet cafes. *Slate* described the domestic intranet this way:

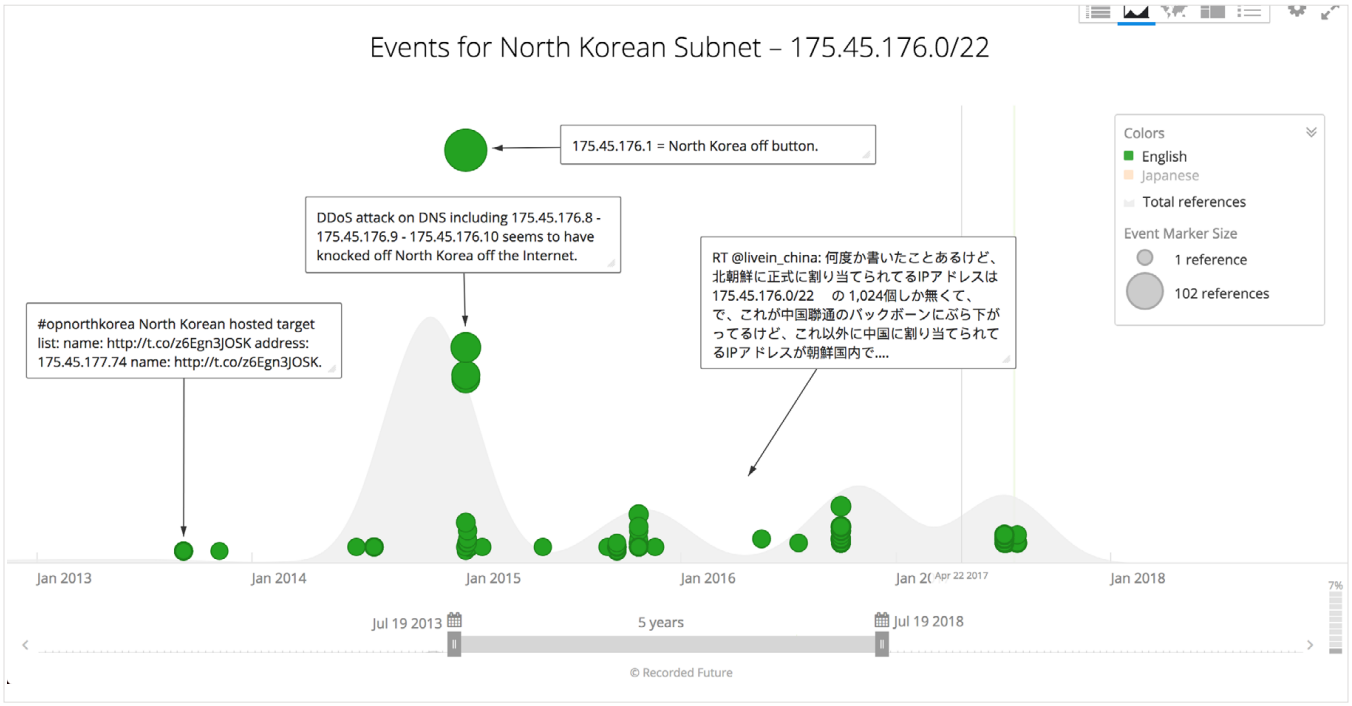
"The network, called Kwangmyong, currently connects libraries, universities, and government departments and is slowly making its way into homes of better-off citizens. It houses a number of domestic websites, an online learning system, and email. The sites themselves aren't much to get excited about: They belong to the national news service, universities, government IT service centers, and a handful of other official organizations. There's also apparently a cooking site with recipes for Korean dishes."

Computer lab at Kim Il Sung University.
Source: Sophie Schmidt, https://sites.google.com/site/sophieinnorthkorea/

Among the select few with permission to use the country's intranet are an even slimmer group of the most senior leaders and ruling elite who are granted access to the worldwide internet directly. While there are no reliable numbers of North Korean internet users, reporters estimate anywhere from "only a very small number" to "the inner circle of North Korean leadership" to "just a few dozen families." Regardless of the exact number, the profile of a North Korean internet user is clear; trusted member or family member of the ruling class.

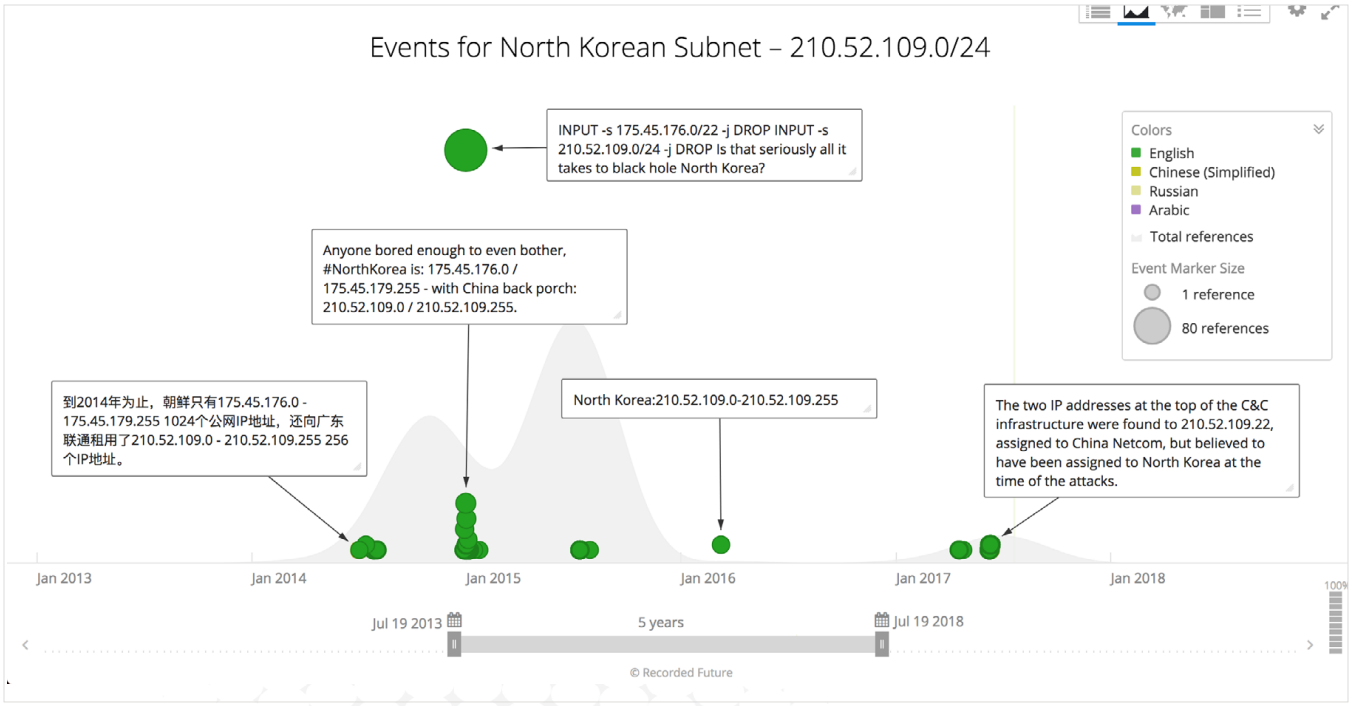
There are three primary ways North Korean elites access the internet.

› First is via their allocated .kp range, 175.45.176.0/22, which also hosts the nation's only internet-accessible websites. These include nine top-level domains (such as co.kp, gov.kp, and edu.kp) and approximately 25 subdomains for various North Korean state-run media, travel, and education-related sites (these sites do not always resolve).



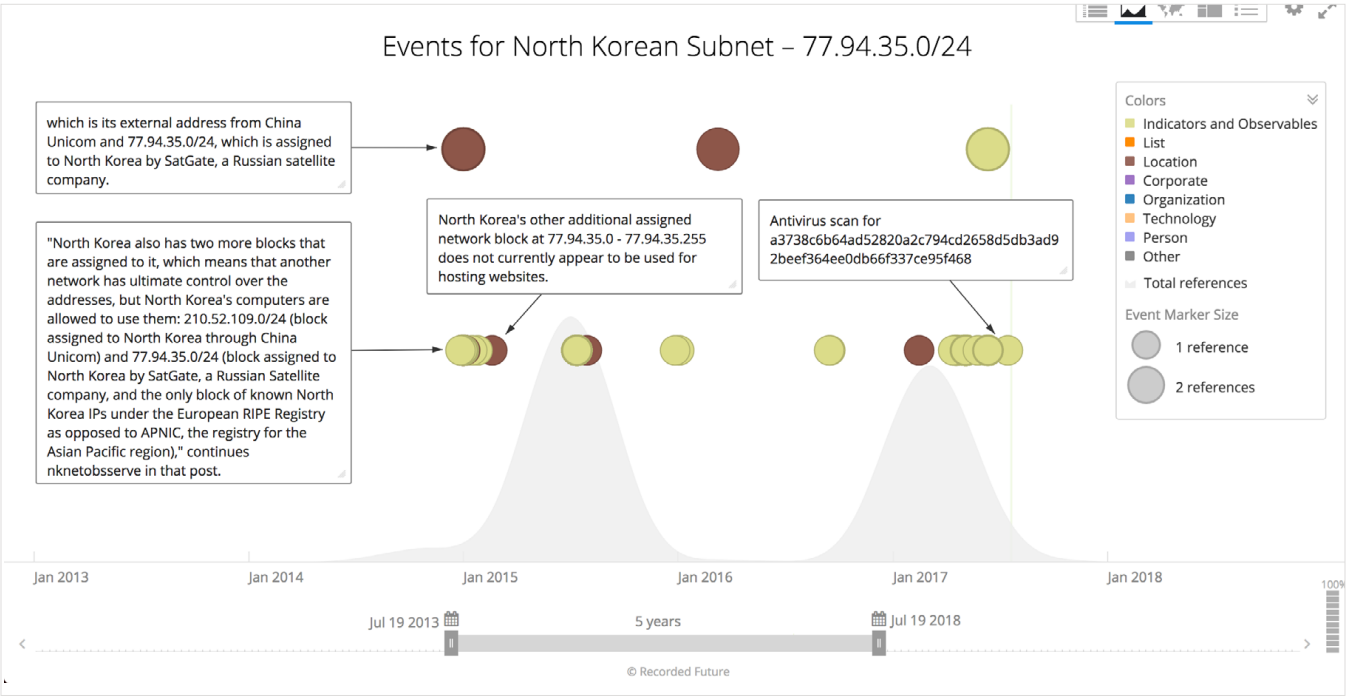
Source: https://app.recordedfuture.com/live/sc/3mj7WHQSPPvU

› The second method is via a range assigned by China Netcom, 210.52.109.0/24. The netname "KPTC" is the abbreviation for Korea Posts and Telecommunications, Co, the state-run telecommunications company.



Source: https://app.recordedfuture.com/live/sc/5NjGxYtQWgiL

› The third method is through an assigned range, 77.94.35.0/24, provided by a Russian satellite company, which currently resolves to SatGate in Lebanon.



Source: https://app.recordedfuture.com/live/sc/4Rx8tsaRgYp3

Two important notes: One, from this point on when we refer to "North Korean internet activity" or "behavior," we are referring to use of the internet (not the North Korean domestic intranet Kwangmyong) by the select few leaders and ruling elite that are permitted access. This data does not give us any insight into intranet activity or behavior by the larger group of privileged North Koreans permitted access to Kwangmyong or diplomatic and foreign establishments that are located in North Korea.

Two, we chose this date range, April 1 through July 6, 2017, because it represented one of the periods of highest missile launching and testing activity, and also because it was the period of time during which the data had the greatest depth and fidelity. While we have data stretching back to January 1, 2017, that dataset (January 1 to March 31) is much less robust.

Analysis

In the early hours of April 1, 2017, as many in the West were just waking up, checking email and social media, a small group of North Korean elites began the day in much the same manner. Some checked the news on Xinhua or the People's Daily, others logged into their 163.com email accounts, while still others streamed Chinese-language videos on Youku and searched Baidu and Amazon.

Recorded Future's analysis of this limited-duration data set has given us new insight into this isolated country and ruling regime. Our analysis demonstrates that the limited number of North Korean leaders and ruling elite with access to the internet are much more active and engaged in the world, popular culture, international news, and with contemporary services and technologies than many outside North Korea had previously thought. North Korean leaders are not disconnected from the world and the consequences of their actions.

While this data source is not absolute, it gives us a detailed picture of North Korean internet use and activity during the April – July 2017 timeframe, and as a result, we are able to reach a number of unique new insights.

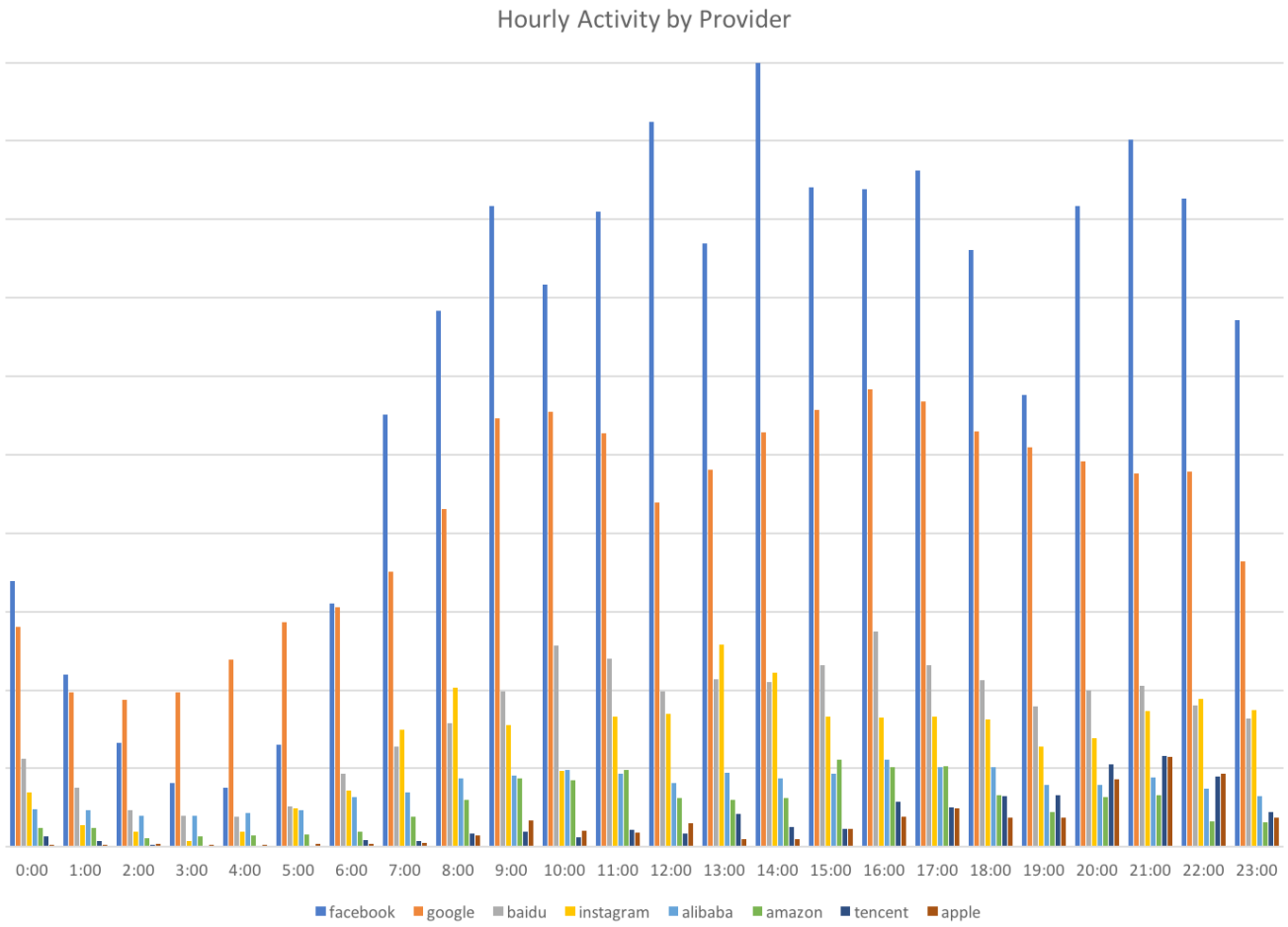
The data reveals that North Korea's leadership and ruling elite are plugged into modern internet society and are likely aware of the impact that their decisions regarding missile tests, suppression of their population, criminal activities, and more have on the international community. These decisions are not made in isolation nor are they ill-informed as many would believe.

Patterns of Use Mirror Western Users

North Korean elite and leadership internet activity is in many ways not that different from most Westerners, despite the extremely limited number of people who can access the internet; the relatively few numbers of both computers and IP space from which to reach it; the linguistic, cultural, social, and legal barriers; and sheer hostility to the rest of the world.

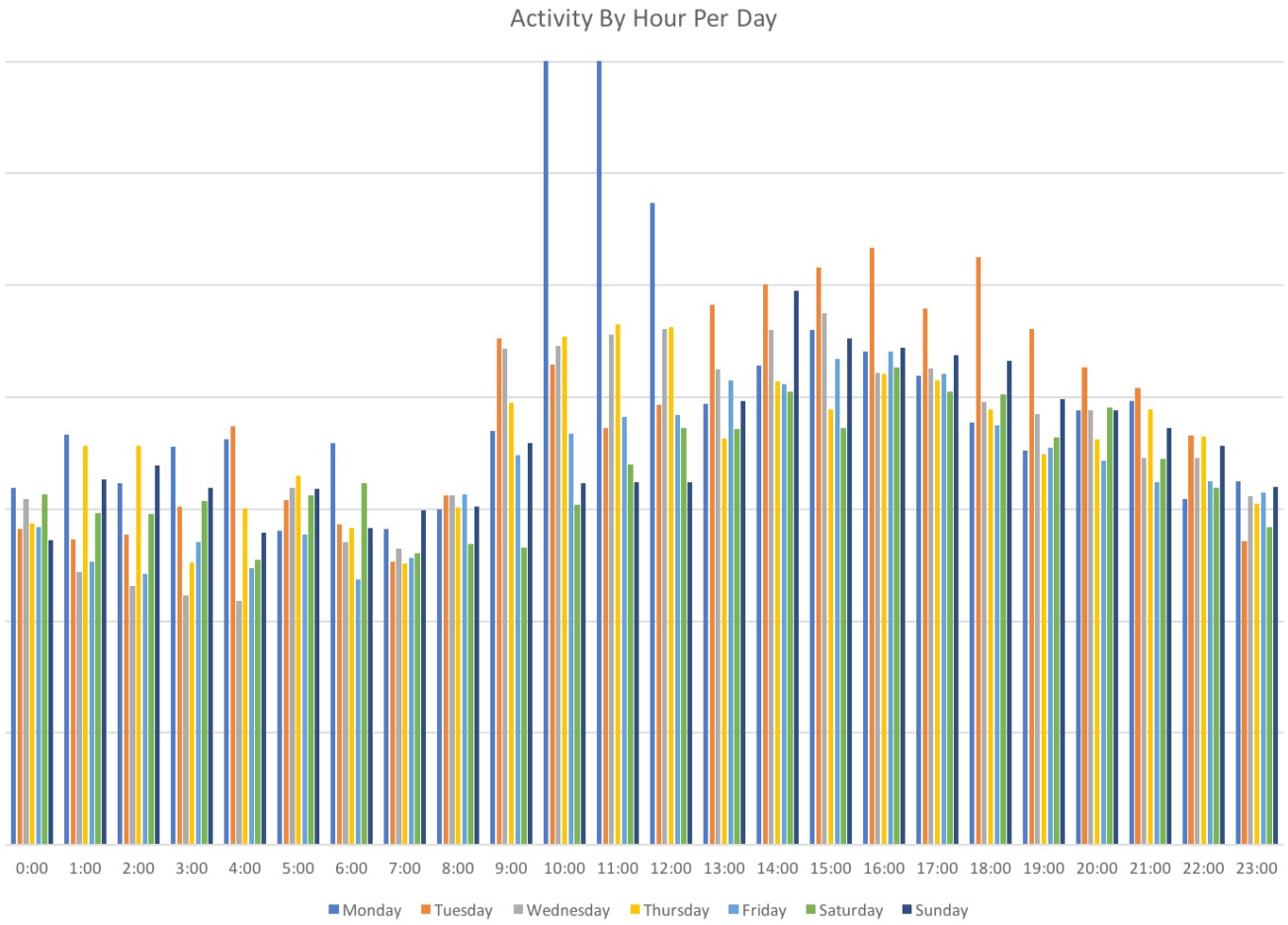
For example, similar to users in the developed world, North Koreans spend much of their time online checking social media accounts, searching the web, and browsing Amazon and Alibaba.

Facebook is the most widely used social networking site for North Koreans, despite reports that it, Twitter, YouTube, and a number of others were blocked by North Korean censors in April 2016.



Hourly activity on eight social networking, shopping, and search sites for April1 through July 6, 2017 (actual). Providers are listed by popularity, from Facebook (highest) to Apple (lowest).

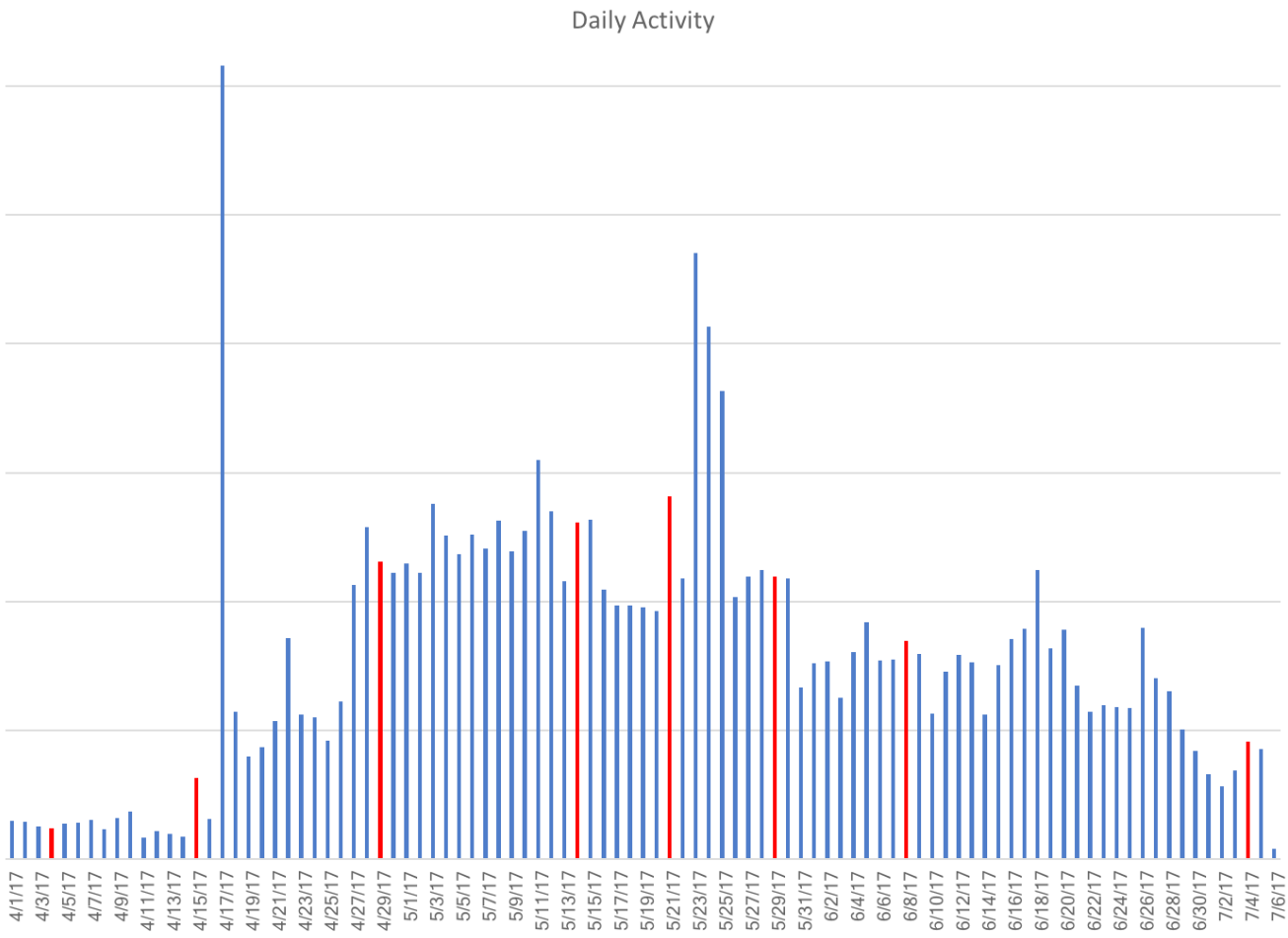
Additionally, North Koreans have distinct patterns of daily usage over this period as well. On weekdays, times of highest activity are from approximately 9:00 AM through 8:00 or 9:00 PM, with Mondays and Tuesdays being the days of consistently highest activity.



Daily internet usage by hour (not an average).

Not an Early Warning for Missile Activity

Many researchers and scholars have hypothesized that there may be a connection between North Korean cyber activity and missile launches or tests. In particular, that we may be able to forecast or anticipate a missile test based on North Korean cyber or internet activity. While we were not able to examine levels of North Korean malicious cyber activity, for this limited time period using this data set, there does not appear to be a correlation between North Korean internet activity at large and missile tests or launches.



Caption: Daily actual internet activity for April 1 through July 6, 2017. Red bars are dates of North Korean missile tests or launches.

This current data set is too short a duration of time to apply any long-term conclusions about the utility of internet activity as a warning device for missile tests. However, our analysis does suggest that if there is a correlation between North Korean activity and missile tests, it is not telegraphed by leadership and ruling elite internet behavior.

Presence in Foreign Countries

The near absence of malicious cyber activity from the North Korean mainland from April to July 2017 likely indicates that, for the most part, they are not using territorial resources to conduct cyber operations and that most state-sponsored activity is perpetrated from abroad. This is a significant operational weakness which could be exploited to apply asymmetric pressure on the Kim regime, limit current North Korean cyber operational freedom and flexibility, and reduce the degree at which they are able to operate with impunity.

This data and analysis demonstrate that there are significant physical and virtual North Korean presences in several nations around the world — nations where North Koreans are possibly engaging in malicious cyber and criminal activities (as demonstrated in part one). These nations include India, Malaysia, New Zealand, Nepal, Kenya, Mozambique, and Indonesia.

Based on our analysis, we were able to determine the following:

› It is clear that North Korea has a broad physical and virtual presence in India. Characterized by the Indian Ministry of External Affairs as a relationship of "friendship, cooperation, and understanding," the data we analyzed supports the reports of increasingly close diplomatic and trade relationship between India and North Korea.

› Patterns of activity suggest that North Korea may have students at least seven universities around the country and may be working with several research institutes and government departments.

› Nearly one-fifth of all activity observed during this time period involved India.

North Korean embassy in India.
Source: https://www.quora.com/How-are-the-relations-between-India-North-Korea

North Korea also has substantial and active presences in New Zealand, Malaysia, Nepal, Kenya, Mozambique, and Indonesia. Our source revealed not only above-average levels of activity to and from these nations, but to many local resources, news outlets, and governments, which was uncharacteristic of North Korean activity in other nations.

It has been widely reported that North Korea has a physical presence to conduct cyber operations in China, including co-owning a hotel in Shenyang with the Chinese from which North Korea conducted malicious cyber activity. Nearly ten percent of all activity observed during this timeframe involved China, not including the internet access points provided by Chinese telecommunications companies.

Our analysis finds that the profile of activity for China was different than the seven nations identified above, mainly because North Korean leadership users utilized so many Chinese services, such as Taobao, Aliyun, and Youku, which skewed the data. After accounting for use of Chinese internet services, which of course do not signify either physical or virtual presence in China, the pattern of activity to local Chinese resources, news outlets, and government departments mirrored the seven previously identified nations.

This Chinese example, where the distinct pattern of activity we discovered combined with the already known facilities for cyber operations, provides us with a model we can apply to the other seven nations.

Together with the fact that North Korea has a meaningful physical and virtual presence in several nations around the world, and our previous research in part one, it is highly likely that North Korea is conducting cyber operations from third-party countries. Therefore, an alternative avenue to explore would be whether malicious cyber activity from these nations correlates with missile launches or tests, as opposed to activity from territorial North Korea.

Note: We are not implying that the governments of these seven nations identified above (excluding China) are complicit with, supportive, or even knowledgeable of the North Korean presence in their country.

Poor Security Leads to New Intelligence

Less than one percent of North Korean internet activity during this period was obfuscated or protected in any way. Among the activity that met this criteria, tradecraft varied broadly from incorrect implementation of TLS/SSL, to utilizing nearly untraceable chains of multiple virtual private networks (VPN) and virtual private servers (VPS) to transfer large amounts of data.

As an example of incorrect implementation, one North Korean user went to the trouble of using Tor (The Onion Router) to obfuscate their activity but then proceeded to use torrent file sharing and exited the Tor network from the same node every day for over three months.

Of the users that employed obfuscation technologies, a wide range of VPN and VPS services and providers were utilized. Almost all VPN and VPS consumed by North Koreans are monthly subscriptions, likely managed by an individual or government department.

It is not clear how these services are purchased and many of the providers are large and well-known Western companies. These include Sharktech, iWeb, Digital Ocean, Linode, Leaseweb USA, Telemax, Touch VPN, and others.

Many VPN and VPS were used to obfuscate or facilitate browsing, either from passive internet monitoring or domestic censors.

One U.S. VPN was used by an iPad to check a Gmail account, access Google Cloud, check Facebook and MSN accounts, and view adult content. Other VPN and VPS were used to run Metasploit, make purchases using bitcoin, check Twitter, play video games, stream videos, post documents to Dropbox, and browse Amazon.

As a result of this generally poor obfuscation, this data afforded us insight into North Korean leadership and elite interests that we have never had before. For example, many users utilized VoIP services to talk and message others overseas; others still had AOL accounts and checked them regularly; some users frequented beauty and health sites; others purchased expensive sneakers online; many users investigated industrial hardware and technology optimization services; others used iPhones, iPads, and Blackberries to communicate.

Other users spent time every day researching cybersecurity companies and their research, including Kaspersky, McAfee, Qihoo360, and Symantec; and DDoS prevention companies and technologies such as DoSarrest and Sharktech. One user received training on the use of THURAYA and satellite communications equipment and others researched the physics and engineering departments at several Malaysian, U.S., and Canadian universities.

Gaming and content streaming accounted for sixty-five percent of all internet activity in North Korea. Broadly, users consume content mostly from the Chinese video hosting service Youku, iTunes, and various BitTorrent and peer-to-peer streaming services. For games, North Korean users seem to prefer games hosted by Valve and a massively multiplayer online game called World of Tanks.

Suspect Activity

While the majority of activity from North Korea during this timeframe was not malicious, there was a smaller, but significant, amount of activity that was highly suspect. One instance was the start of Bitcoin mining by users in North Korea on May 17.

According to the Bitcoin wiki, bitcoin mining is "the process of adding transaction records to Bitcoin's public ledger of past transactions (or block chain)." Bitcoin mining is difficult because it is a computationally complex task and can require up to 90% of a machine's power.

The benefit to using all of this energy and adding the transaction records to the blockchain is that each miner is awarded not only the fees paid by the users sending the transaction, but 25 bitcoins once they discover a new block.

Before that day, there had been virtually no activity to Bitcoin-related sites or nodes, or utilizing Bitcoin-specific ports or protocols. Beginning on May 17, that activity increased exponentially, from nothing to hundreds per day. The timing of this mining is important because it began very soon after the May WannaCry ransomware attacks, which the NSA has attributed to North Korea's intelligence service, the Reconnaissance General Bureau (RGB), as an attempt to raise funds for the Kim regime.

By this point (May 17) actors within the government would have realized that moving the bitcoin from the three WannaCry ransom accounts would be easy to track and ill-advised if they wished to retain deniability for the attack.

It is not clear who is running the North Korean bitcoin mining operations; however, given the relatively small number of computers in North Korea coupled with the limited IP space, it is not likely this computationally intensive activity is occurring outside of state control.

Additionally, during this time frame it appeared that some North Korean users were conducting research, or possibly even network reconnaissance, on a number of foreign laboratories and research centers.

In particular, activity targeting the Indian Space Research Organization's National Remote Sensing Centre, the Indian National Metallurgical Laboratory, and the Philippines Department of Science and Technology Advanced Science and Technology Research Institutes raised flags of suspicion, but we could not confirm malicious behavior.

Impact

The international policy and engagement strategy toward North Korea has struggled to be impactful for decades because it has relied on the same set of tools (sanctions, increasing international isolation) and engaged the same nations (China, Russia, UN Security Council Permanent Five) as partners. This two-part series demonstrates that there are likely other pressure points on the regime and as a result, other tools, techniques, and partners that should be explored.

Team Cymru's intelligence and Recorded Future's analysis have revealed two separate realities.

First, in spite of the sanctions and massive international pressure, North Korea's leaders are not isolated from the outside world. They are active and engaged participants in the contemporary internet society and economy; meaning that attempts to shut North Korean leadership off from the global economy have largely failed.

Second, new tools that do not focus on Pyongyang and territorial North Korea are needed to achieve a lasting negative impact on the current Kim regime. We have identified other nations with which the West could partner and alternate tools and techniques that could be utilized to apply asymmetric pressure on North Korea. Partnering with nations such as India, Malaysia, Indonesia, or others identified above, would enable the U.S. and other Western nations to circumvent uncooperative partners in China and Russia and exert pressure on the broad North Korean operational diaspora, which, because of the regime's dependency, would likely impose larger real costs on leadership.

For cybersecurity professionals and network defenders, this two-part series reveals just how complex defending from North Korean malicious cyber activity can be. We continue to recommend that financial services firms and those supporting U.S. and South Korean military THAAD deployment as well as on-penninsula operations maintain the highest vigilance and awareness of the heightened threat environment to their networks and operations on the Korean peninsula.

Similarly, energy and media companies, particularly those located in or that support these sectors in South Korea, should be alert to a wide range of cyber activity from North Korea, including DDoS, destructive malware, and ransomware attacks. Broadly, organizations in all sectors should continue to be aware of the adaptability of ransomware and modify their cyber security strategies as the threat evolves.

About Recorded Future

Recorded Future delivers threat intelligence powered by machine learning, arming you to significantly lower risk. We enable you to connect the dots to rapidly reveal unknown threats before they impact your business, and empower you to respond to security alerts 10 times faster. Our patented technology automatically collects and analyzes intelligence from technical, open, and dark web sources to deliver radically more context than ever before, updates in real time so intelligence stays relevant, and packages information ready for human analysis or instant integration with your existing security systems.