

Companion report



HP Security Briefing

Episode 16, August 2014

Profiling an enigma: The mystery of North Korea's cyber threat landscape

HP Security Research

Table of Contents

Introduction.....	3
Research roadblocks.....	4
Ideological and political context.....	5
Juche and Songun.....	5
Tension and change on the Korean Peninsula.....	8
North Korean cyber capabilities and limitations.....	10
North Korean infrastructure.....	10
An analysis of developments in North Korean cyberspace since 2010.....	14
North Korean cyber war and intelligence structure.....	21
North Korean cyber and intelligence organizational chart.....	26
North Korea's cyber doctrine, strategies and goals.....	26
Cyber warfare operations.....	27
Gaming for profit and pwnage.....	29
Intelligence and counterintelligence.....	29
Psychological operations.....	32
Electronic warfare.....	38
Training cyber warriors.....	39
Important political and military ties.....	42
China.....	42

Russia	43
Iran.....	43
Syria.....	44
Cuba.....	44
Timeline of significant North Korean cyber activity	45
Patterns in the noise: cyber incidents attributed to North Korean actors	47
DarkSeoul	50
Whols Team.....	52
IsOne.....	55
Kimsukyang.....	57
New Romantic Cyber Army Team / Hastati	57
Malware summary.....	58
Analysis	60
Summary	61
HP Security Research recommendations.....	62
Appendix A – WHOIS records.....	64
Appendix B – Sites found on North Korean IP space.....	72
Appendix C – Analysis of DarkSeoul Dropper	74
Learn more at	75

Episode 16

Thank you for subscribing to Episode 16 of the HP Security Briefing. In this edition we discuss the cyber landscape within the Democratic People's Republic of Korea.

Introduction

The Democratic People's Republic of Korea (DPRK), known in the West as North Korea, is a unique country with a military-focused society and an unconventional technology infrastructure. While North Korea was formerly on the U.S. list of state sponsors of terrorism, it was removed in 2008.¹ However, due to North Korea's hostility toward other nations, its pursuit of nuclear weapons, and human rights violations against its own citizens, the United Nations and many Western entities have placed sanctions and embargoes against North Korea.^{2 3} For example, U.S. export laws forbid the sale of dual-use technologies, or those that can be used or repurposed for both civilian and military use, to North Korea.^{4 5} Additionally, the U.S. has a military alliance with the Republic of Korea (ROK), known in the West as South Korea, North Korea's primary target of conflict.⁶

Due to North Korea's global interactions, its cyber warfare capabilities are of particular interest to the U.S. According to a 2009 report by Major Steve Sin, an intelligence analyst at U.S. Forces Korea, North Korean hackers have successfully penetrated U.S. defense networks more frequently than any other country that has targeted U.S. defense assets.⁷ While Major Sin may have been overly optimistic about North Korea's abilities, it is clear that they should not be underestimated. Frank Cilluffo, co-director of the Cyber Center for National and Economic Security at George Washington University, testified before Congress that North Korea's cyber capability "poses an important 'wild card' threat, not only to the United States but also to the region and broader international stability..."⁸ In an April 2014 testimony given to the House Armed Services Committee, General Curtis M. Scaparrotti noted that "North Korea remains a significant threat to United States' interests, the security of South Korea, and the international community due to its willingness to use force, its continued development and proliferation of nuclear weapon and long-range ballistic missile programs, and its abuse of its citizens' human rights, as well as the legitimate interests of its neighbors and the international community." Scaparrotti stressed that "While North Korea's massive conventional forces have been declining due to aging and lack of resources...North Korea is emphasizing the development of its asymmetric capabilities. North

¹ http://thecable.foreignpolicy.com/posts/2010/05/25/why_the_state_department_wont_put_north_korea_back_on_the_terror_list

² http://www.sanctionswiki.org/North_Korea

³ <https://www.fas.org/irp/offdocs/eo/eo-13551.pdf>

⁴ <http://www.foxnews.com/world/2012/04/17/un-computer-shipment-to-north-korean-regime-violates-us-manufacturers-ban/>

⁵ <http://www.state.gov/strategictrade/overview/>

⁶ <http://docs.house.gov/meetings/AS/AS00/20140402/101985/HHRG-113-AS00-Wstate-ScaparrottiUSAC-20140402.pdf>

⁷ <http://www.nextgov.com/defense/whats-brewin/2009/07/north-koreas-hackers-in-a-luxury-hotel/51330/>

⁸ [http://www.csmonitor.com/World/Security-Watch/2013/1019/In-cyberarms-race-North-Korea-emerging-as-a-power-not-a-pushover/\(page\)/3](http://www.csmonitor.com/World/Security-Watch/2013/1019/In-cyberarms-race-North-Korea-emerging-as-a-power-not-a-pushover/(page)/3)

Korea's asymmetric arsenal includes...an active cyber warfare capability."⁹ While one would expect the regime's digital infrastructure to also suffer from aging or lack of resources, these factors do not take away from their technical abilities to wage cyber warfare.

While the U.S. views North Korea's cyber warfare program as the regime's foray into modern asymmetrical warfare, South Korea views the regime's cyber capabilities as a terroristic threat, -a build-up for an impending multifaceted attack. It is important to note that, to date, no such attack has occurred. According to a report written by Captain Duk-Ki Kim, Republic of Korea Navy officer and Ph.D. "...the North Korean regime will first conduct a simultaneous and multifarious cyber offensive on the Republic of Korea's society and basic infrastructure, government agencies, and major military command centers while at the same time suppressing the ROK government and its domestic allies and supporters with nuclear weapons."¹⁰ South Korea's view of North Korea as a terroristic threat may be an attempt to downgrade North Korea politically, since South Korea does not recognize the regime as a legitimate state.¹¹ South Korean reports also claim that North Korea's premier hacking unit, Unit 121, trails Russia and the U.S. as the world's third largest cyber unit.¹² While this claim may be exaggerated, in 2012, South Korean reports estimated North Korea's hacker forces at around 3000 personnel. In a July 2014 report from South Korea's Yonhap News Agency, that figure was upgraded to 5900 hacker elite.¹³ We must stress that although these claims have not been corroborated, South Korea has taken the regime's cyber threats very seriously and is reportedly training 5000 personnel to defend against North Korean cyber attacks.¹⁴

Obtaining details on North Korea's cyber warfare capabilities is not an easy task. This paper will examine the known cyber capabilities of North Korea's regime and how the country maintains secrecy in these matters. Through information obtained via open source intelligence (OSINT), we will present what is known about North Korea's cyber warfare and supporting intelligence and psychological operations capabilities.

Research roadblocks

The following conditions proved to be research roadblocks when gathering intelligence regarding North Korea's cyber warfare capabilities:

- Much of the intelligence available on North Korea is dated and may not accurately reflect the regime's current capabilities.
- Much of the intelligence available on North Korea comes from U.S. or South Korean military or agency reports. These reports omit details that are likely classified, such as specific IP addresses and individual actor information.
- While South Korea is an ally of the United States, its reports on North Korean cyber activity potentially contain incomplete or biased information. Cultural factors that stem

⁹ <http://docs.house.gov/meetings/AS/AS00/20140402/101985/HHRG-113-AS00-Wstate-ScaparrottiUSAC-20140402.pdf>

¹⁰ <https://www.usnwc.edu/getattachment/8e487165-a3ef-4ebc-83ce-0ddd7898e16a/The-Republic-of-Korea-s-Counter-asymmetric-Strateg>

¹¹ <http://www.atimes.com/atimes/Korea/GA04Dg01.html>

¹² <http://www.koreaherald.com/view.php?ud=20130321000980>

¹³ http://www.theregister.co.uk/2014/07/07/north_korea_employs_6000_leet_hackers_source_claims/

¹⁴ http://www.theregister.co.uk/2014/07/07/north_korea_employs_6000_leet_hackers_source_claims/

from a history of tension and conflict between the two nations may skew perception and make objectivity difficult.^{15 16}

- North Korea's Internet infrastructure and the regime's strict control over its use ensures that there are no rogue actors and that all officially sanctioned actors exercise careful OPSEC and PERSEC practices in order to prevent inadvertent information leaks. In other words, there was no significant identifying information in the form of an OSINT trail left behind by the actors. This hinders collection of original, actionable threat intelligence and individual actor attribution.
- North Korea is well-isolated from the outside world, and its strong intelligence and psychological operations presence effectively creates confusion via counterintelligence and disinformation about the regime's capabilities.¹⁷ For this reason, any "official" reports emanating from North Korea must be taken with a grain of salt. This also hinders attempts to obtain original, actionable threat intelligence.

Ideological and political context

In order for Westerners to understand the North Korean mindset, it is necessary to examine the key components of North Korean political and ideological thought. It is also necessary to provide a brief explanation of how North Korea and South Korea view one another, in order to understand the basis for conflict between the two.

Juche and Songun

North Korea has two primary ideologies that provide context for the regime's motivations and activities: *juche* (*ju-cheh*) and *songun* (*sun-goon*). *Juche* is the official political ideology of North Korea. It was instituted in 1972 and is based on the ideologies of Kim Il-Sung, the founder of the DPRK. *Juche* emphasizes self-reliance, mastering revolution and reconstruction in one's own country, being independent of others, displaying one's strengths, defending oneself, and taking responsibility for solving one's own problems. North Korea's air-gapped intranet, described below, exemplifies this philosophy in the country's cyber infrastructure. The *juche* philosophy explains North Korea's disdain for outside cultural and political influence. *Juche* challenges North Koreans to contribute to the regime's *chaju* (*ja-ju*), a concept of national sovereignty and independence.¹⁸ The regime's greatest fear is internal dissent and resulting destabilization.^{19 20} In a June 2014 Reddit AMA session, Dr. Andrei Lankov, an expert on North Korean culture and society, noted "there are also serious signs of public alienation and discontent. And I cannot rule out a public outbreak of such discontent in the near future. Of course, if it happens, it will have a serious impact on the government."²¹ Despite North Korea's strong conviction in *juche*, the regime collaborates with and receives support from other nations. However, due to this deep-seated

¹⁵ <http://www.businessinsider.com/did-kim-jong-un-execute-his-ex-girlfriend-2013-8>

¹⁶ <http://www.telegraph.co.uk/news/worldnews/asia/northkorea/10554198/North-Koreas-invisible-phone-killer-dogs-and-other-such-stories-why-the-world-is-transfixed.html>

¹⁷ http://edition.cnn.com/2014/04/01/world/north-korea-provocation/index.html?iid=article_sidebar

¹⁸ <http://www.stanford.edu/group/sjeaa/journal3/korea1.pdf>

¹⁹ http://belfercenter.ksg.harvard.edu/publication/20269/keeping_kim.html

²⁰ <http://www.buzzfeed.com/miriamberger/the-world-as-viewed-by-north-koreas-propaganda-machine>

²¹ http://www.reddit.com/r/NorthKoreaNews/comments/296ryd/i_am_dr_andrei_lankov_i_studied_in_north_korea/

ideology, it is doubtful that North Korea fully trusts these apparent allies.²² Later in this document, we will show that North Korea relies heavily on China for Internet access. North Korea also collaborates with China and Russia to train its cyber warriors and has longstanding political and military relationships with several nations.

Songun is North Korea's "military first" doctrine. *Songun* emphasizes the priority of the military in resource allocation and political and economic affairs.²³ This doctrine stems from the belief that the military is vital for preservation of *chaju*.²⁴ Understanding *songun* mindset gives context for this potential threat actor's motivations. According to a 2013 Congressional report, the strategy established under former leader Kim Jong-Il focused on "internal security, coercive diplomacy to compel acceptance of its diplomatic, economic and security interests, development of strategic military capabilities to deter external attack, and challenging South Korea and the U.S.-South Korean alliance."²⁵

North Korea's *songun* permeates the lives of all North Korean citizens. Article 58 of the North Korean Constitution states that the nation should base itself on a nationwide defense system that includes all people.²⁶ North Korea, with a population of 25 million, has an active duty force of 1.19 million personnel, the fourth largest in the world. The country's reserve and paramilitary units comprise 7.7 million additional personnel.²⁷ In other words, over a third of the country's population serves in a military or paramilitary capacity.

Songun is North Korea's "military first" doctrine. *Songun* emphasizes the priority of the military in resource allocation and political and economic affairs. Understanding this mindset gives context for a potential threat actor's motivations.

Some North Korean youth aged 7-13 are inducted into the Korean Children's Union. The Korean Children's Union is responsible for indoctrinating youths who pledge to build up their strength to later defend the regime.²⁸

²² <http://www.defense.gov/pubs/ReporttoCongressonMilitaryandSecurityDevelopmentsInvolvingtheDPRK.pdf>

²³ <http://www.strategicstudiesinstitute.army.mil/pdffiles/pub728.pdf>

²⁴ http://www.iar-gwu.org/sites/default/files/articlepdfs/DeRochie_-_The_Driving_Factor.pdf

²⁵ <http://www.defense.gov/news/newsarticle.aspx?id=119924>

²⁶ <http://asiamatters.blogspot.co.uk/2009/10/north-korean-constitution-april-2009.html>

²⁷ <http://edition.cnn.com/video/data/2.0/video/international/2014/04/29/north-korea-military-numbers.cnn.html>

²⁸ http://www.dailymail.co.uk/news/article-2307937/North-Korea-Haunting-images-indoctrination-ceremony-communist-cult-leaders-threatening-nuclear-war-poisoning-generation.html?ITO=1490&ns_mchannel=rss&ns_campaign=1490



Figure 1 A group of North Korean children being inducted into the Korean Children's Union.²⁹



Figure 2 Members of the Korean Children's Union with the regime's leader Kim Jong Un.³⁰

²⁹ http://www.dailymail.co.uk/news/article-2307937/North-Korea-Haunting-images-indoctrination-ceremony-communist-cult-leaders-threatening-nuclear-war-poisoning-generation.html?ITO=1490&ns_mchannel=rss&ns_campaign=1490

Children aged 14-16 can begin military training as members of the Young Red Guards, a paramilitary unit. Beginning at age 17, North Koreans are eligible to join the Reserve Military Training Unit.³¹ The Reserve Military Training Unit forms the core of North Korea's reserves and is typically assigned to the front or regional defense in wartime.³² The youngest age at which a citizen can be conscripted for active duty is unclear; reported ages range from 18-20. Youths can volunteer for active duty service at age 16 or 17.³³ The Worker-Peasant Militia, or Red Guards, includes males ages 17-60 and unmarried females ages 17-30 who are not part of active duty units or the Reserve Military Training Unit.³⁴

The regime has an impressive number of conventional weapons, considering the nation's small land area and population size.³⁵ According to statistics released by CNN in 2014, North Korea's ground arsenal includes 4100 tanks, 2100 armored vehicles, and 8500 pieces of field artillery. The regime's sea weaponry includes 70 submarines, 420 patrol combatants, and 260 amphibious landing craft. Their airpower includes 730 combat aircraft, 300 helicopters, and 290 transport aircraft. While the limits of the regime's ballistic missile program are unknown, North Korea is thought to have fewer than 100 short-range missiles and fewer than 100 medium to long-range missiles.³⁶ However, in recent years, North Korea has suffered oil,³⁷ fuel,³⁸ electricity,³⁹ and food⁴⁰ shortages. Without aid from another entity, the regime does not have sufficient resources to maintain and sustain the majority of its weapons and associated personnel for rapid deployment or prolonged combat.

Tension and change on the Korean Peninsula

Tension between North and South Korea has continued well past the armistice meant to end the Korean War. Neither nation recognizes the other as a legitimate state. South Korea's constitution legally defines South Korean territory as the entire Korean peninsula and its adjacent islands, with "North Korea" being a part of South Korea.⁴¹ North Korea also claims to be the sole government of the Korean Peninsula.⁴² Each country's claim of sovereignty and refusal to acknowledge the other as a legitimate state creates the condition for perpetual conflict. North Korea's negative sentiment towards the U.S. stems from two major factors: the U.S. – South Korea military alliance and North Korea's perception that the U.S. is imperialistic and prone to exploitative capitalism.⁴³

³⁰ http://www.dailymail.co.uk/news/article-2307937/North-Korea-Haunting-images-indoctrination-ceremony-communist-cult-leaders-threatening-nuclear-war-poisoning-generation.html?ITO=1490&ns_mchannel=rss&ns_campaign=1490

³¹ <http://www.globalsecurity.org/military/world/dprk/army.htm>

³² <http://www.globalsecurity.org/military/world/dprk/army.htm>

³³ https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=6&ved=0CFkQFjAF&url=http%3A%2F%2Fwww.child-soldiers.org%2Fuser_uploads%2Fpdf%2Fkoreademocraticpeoplesrepublicof2639438.pdf&ei=fcylU_uqCMas0QXUk4DoCw&usq=AFQjCNG0nKQt5ZStqxfc tKrUY-5IWYSH0A&sig2=ivQLF6lHKS08Yx9O9VlO4g&bvm=bv.67720277,d.d2k&cad=rja

³⁴ <http://www.globalsecurity.org/military/world/dprk/army.htm>

³⁵ <http://www.globalfirepower.com/>

³⁶ <http://edition.cnn.com/video/data/2.0/video/international/2014/04/29/north-korea-military-numbers.cnn.html>

³⁷ <http://www.presstv.com/detail/2013/04/23/299897/facing-food-and-oil-shortages-north-korea-turns-to-iran/>

³⁸ http://english.chosun.com/site/data/html_dir/2014/07/02/2014070201995.html

³⁹ <http://www.rfa.org/english/news/korea/electricity-10212013160033.html>

⁴⁰ <http://edition.cnn.com/2013/04/09/business/north-korea-economy-explainer/>

⁴¹ <http://www.atimes.com/atimes/Korea/GA04Dg01.html>

⁴² http://teacher.scholastic.com/scholasticnews/indepth/north_korea/north-south/index.asp?article=north_korea

⁴³ http://cns.miis.edu/other/pinkston_strategic_insights_sep06.pdf

In recent years, two primary factors have heavily influenced the current state of North Korea's relations with South Korea and her allies: the rise of the regime's leader Kim Jong Un and the inauguration of South Korean president Park Geun-hye. Kim Jong Un officially rose to power in April 2012, following the death of his father Kim Jong Il in December 2011. While his age remained a mystery for quite some time, it was later revealed that he was born in January 1983, making him age 31 at present. This makes Kim Jong Un the world's youngest leader of an established nation.⁴⁴ The young leader's rise to power brought about several changes in North Korea. First, Kim Jong Un's personal life is more public and more extravagant than that of his father. Unlike his father, the young Kim is often accompanied by his wife when making public appearances.⁴⁵ Second, the young Kim, who is more high-tech than his predecessor, is reported to have an affinity for luxury items⁴⁶ and is an avid gamer and basketball fan.⁴⁷ Third, Kim Jong Un is more totalitarian than his father. Following his rise to power, the regime reportedly expanded its labor camps, and more military resources were allocated to target those attempting to defect. Kim also executed his own uncle, a high-ranking official who did not share his ideals. These moves indicate the regime's priority to deter internal destabilization and dissent, which is perceived to be a greater threat than outside adversity. According to Phil Robertson, deputy Asia director at Human Rights Watch, "The government now recognizes that the accounts of escaping North Koreans reveal Pyongyang's crimes – so it is doing what it can to stop people from fleeing."⁴⁸ Under Kim Jong Un's rule, the regime has stepped up its nuclear materials production, and the propaganda distributed by state media has become more menacing.⁴⁹

The regime's response to perceived threats has also become more volatile. Christian Whiton, a former deputy envoy to North Korea, noted that following Kim Jong Un's rise to power, "the regime still acts in a very belligerent manner, but it seems less predictable, and more random." Ellen Kim, assistant director of the Korea Chair at the Center for Strategic and International Studies, assessed the situation thusly: "Since [Kim Jong Un] took power he has purged almost all of his elder guardians ... and filled his surroundings with new faces. We are in a situation where we are learning about him a little bit every day through his unpredictable behavior and actions, which is why the current situation with North Korea is a lot more dangerous than before."⁵⁰ The regime's recent reaction to an upcoming film supports these statements. The plot for the comedy film "The Interview" follows two talk show hosts who are asked to assassinate Kim Jong Un. The regime even sent a complaint about the movie to the UN.⁵¹ In response to the film, a North Korean official stated, "The enemies have gone beyond the tolerance limit in their despicable moves to dare hurt the dignity of the supreme leadership." The official referred to the movie as "the most undisguised terrorism and a war action to deprive the service personnel and people of the DPRK of their mental mainstay and bring down its social system." The official also issued a threat: "If the U.S. administration connives at and patronizes the screening of the film, it will invite a strong and merciless countermeasure."⁵² This reaction demonstrates North Korea's priority of preserving the

⁴⁴ <http://www.theatlantic.com/international/archive/2012/12/kim-jong-uns-age-is-no-longer-a-mystery/265983/>

⁴⁵ <http://www.telegraph.co.uk/news/worldnews/asia/northkorea/10522136/Kim-Jong-un-10-ways-North-Koreas-Dear-Leader-is-different.html>

⁴⁶ http://www.huffingtonpost.com/2014/02/18/north-korea-luxury-goods_n_4808823.html

⁴⁷ <http://nypost.com/2011/12/20/kims-007-nut-kid-in-charge/>

⁴⁸ <http://www.hrw.org/news/2014/01/21/north-korea-kim-jong-un-deepens-abusive-rule>

⁴⁹ <http://www.telegraph.co.uk/news/worldnews/asia/northkorea/10522136/Kim-Jong-un-10-ways-North-Koreas-Dear-Leader-is-different.html>

⁵⁰ http://edition.cnn.com/2014/04/01/world/north-korea-provocation/index.html?iid=article_sidebar

⁵¹ <http://www.northkoreatech.org/2014/07/10/dprk-takes-the-interview-movie-complaint-to-the-un/>

⁵² http://edition.cnn.com/2014/06/25/world/asia/north-korea-the-interview-reaction/index.html?iid=article_sidebar

regime's self-perceived dignity in the global arena and its intolerance of any disrespect directed at the Kim family.

While tensions between North and South Korea have persisted since the Korean War, these tensions escalated following the 2013 inauguration of South Korea's current president, Park Geun Hye. Her platform, in her words, is as follows: "North Korea must keep its agreements made with South Korea and the international community to establish a minimum level of trust, and second there must be assured consequences for actions that breach the peace. To ensure stability, *trustpolitik* should be applied consistently from issue to issue based on verifiable actions, and steps should not be taken for mere political expediency."⁵³ Shortly after Park's inauguration, North Korea denounced UN Security Council Resolution 2094, which is "a resolution strengthening and expanding the scope of United Nations sanctions against the Democratic People's Republic of Korea by targeting the illicit activities of diplomatic personnel, transfers of bulk cash, and the country's banking relationships, in response to that country's third nuclear test on 12 February [2013]."⁵⁴ North Korea also responded strongly to joint U.S.-South Korea military exercises in March 2013, as is noted later in this paper.⁵⁵

North Korean cyber capabilities and limitations

North Korean infrastructure

North Korea's cyber infrastructure is divided into two major parts: an outward-facing Internet connection and a regime-controlled intranet. North Korea's outward-facing Internet connection is only available to select individuals and is closely monitored for any activity that is deemed anti-regime. Individuals using the outward-facing Internet connection must be authorized. In 2013, Jean H. Lee, the Associated Press bureau chief in Pyongyang, stated that foreigners visiting North Korea are allowed Internet access with no firewalls.⁵⁶ Common citizens are limited to using the Kwangmyong (*gwang me-young*), a nationwide intranet with no access to the world outside North Korea.⁵⁷ According to Lee, Kwangmyong allows citizens "access to the state media, information sources that are vetted by the government, and picked and pulled from the Internet and posted to their intranet site."⁵⁸ As of May 2013, North Korea had only one "Internet café."⁵⁹ A 2003 report from the Office of the National Counterintelligence Executive stated that North Korea's "Internet café" was "the only place in North Korea for the public to access the Internet" and that foreigners were allowed to access the Internet from this café.⁶⁰ Whether citizens are allowed to access the Internet from this location is unknown.

Star Joint Venture Co. is responsible for providing North Korea's Internet access. Star Joint Venture Co. was established by the Post and Telecommunications Corporation in cooperation with Loxley

⁵³ <http://www.ncnk.org/resources/briefing-papers/all-briefing-papers/an-overview-of-south-korea2019s-dprk-policy>

⁵⁴ <http://www.un.org/News/Press/docs/2013/sc10934.doc.htm>

⁵⁵ <http://www.ncnk.org/resources/briefing-papers/all-briefing-papers/an-overview-of-south-korea2019s-dprk-policy>

⁵⁶ <http://www.austinchronicle.com/daily/sxsw/2013-03-11/social-media-in-north-korea/>

⁵⁷ http://www.computerworld.com/s/article/9177968/North_Korea_moves_quietly_onto_the_Internet?taxonomyId=18&pageNumber=2

⁵⁸ <http://www.austinchronicle.com/daily/sxsw/2013-03-11/social-media-in-north-korea/>

⁵⁹ <http://www.washingtonpost.com/blogs/worldviews/wp/2013/01/29/north-koreans-shouldnt-count-on-using-the-new-google-maps/>

⁶⁰ http://www.ncix.gov/publications/archives/docs/NORTH_KOREA_AND_FOREIGN_IT.pdf

Pacific in Thailand.⁶¹ In December 2009, Star Joint Venture became responsible for North Korea's Internet address allocation. Previously, Internet access was provided by a German satellite link via Korea Computer Center Europe or via direct connections with China Netcom, which was later merged into China Unicom.⁶² By October 2010, North Korea had made its first known direct connection to the Internet, hosting an outward-facing Korean Central News Agency website accessible from the global Internet.⁶³ However, many of North Korea's globally accessible websites are hosted in other countries. In 2001, South Korean reports indicated that North Korea had joined the International Telecommunications Satellite Organization (INTELSAT).⁶⁴ As of April 2012, North Korea reportedly used the Intelsat connection, which appeared in border gateway protocol (BGP) announcements.⁶⁵ Some reports referred to the Intelsat connection as North Korea's backup Internet connection, in case the China Unicom connection fails.⁶⁶ A March 2013 post on the blog *rdns.im* showed that North Korea no longer used the Intelsat connection. In the blog post, the author noted his method for proving that The Pirate Bay was not hosted in North Korea. While his analysis of The Pirate Bay's hosting is irrelevant to our research, he did detail that 175.45.177.0/24 always routes through AS4837, and AS131279. AS131279 is Star-KP, North Korea's Star Joint Venture Company, and AS4837 is China Unicom. The author concluded that "all [traffic] is ONLY routed through China Unicom and NOT through Intelsat."⁶⁷ In February 2014, North Korean and South Korean officials agreed to extend Internet access to Kaesong Industrial Zone, a jointly operated industrial complex just north of the border. However, this would likely require a major electrical and network infrastructure expansion.⁶⁸

North Korea's electrical grid cannot support a large technological infrastructure.⁶⁹ Electrical power is reported to be unreliable and sporadic, with many citizens only receiving a few hours of electricity per day.⁷⁰

⁶¹ <http://www.northkoreatech.org/2011/05/19/more-details-on-star-joint-venture/>

⁶² http://www.computerworld.com/s/article/9177968/North_Korea_moves_quietly_onto_the_Internet?taxonomyId=18&pageNumber=2

⁶³ <http://www.northkoreatech.org/2010/10/09/the-new-face-of-kcna/>

⁶⁴ http://webcache.googleusercontent.com/search?q=cache:http://english.chosun.com/site/data/html_dir/2001/05/29/2001052961197.html

⁶⁵ <http://www.northkoreatech.org/2012/04/08/dprk-gets-second-link-to-internet/>

⁶⁶ http://www.computerworld.com/s/article/9237652/North_Korea_39_s_Internet_returns_after_36_hour_outage

⁶⁷ <https://rdns.im/the-pirate-bay-north-korean-hosting-no-its-fake-p2>

⁶⁸ <http://www.northkoreatech.org/2014/02/10/internet-coming-to-kaesong-industrial-zone/>

⁶⁹ <http://38north.org/2010/09/speak-loudly-and-carry-a-small-stick-the-north-korean-cyber-menace/>

⁷⁰ <http://www.usnews.com/news/blogs/rick-newman/2013/04/12/heres-how-lousy-life-is-in-north-korea>



Figure 3 North and South Korean power grid

The photo above (Figure 3), from the International Space Station, shows North Korea's sparse power grid, in comparison with surrounding nations.⁷¹ We have highlighted North Korea in red.

Koryolink, the country's only cellular phone network,⁷² is tightly controlled by the regime.⁷³ Cell phone data plans are not available to most users. Most cellular phones cannot access the Internet and can only make domestic calls.⁷⁴ According to a 2013 report, North Korea has a 3G data network for cellular phones. Visiting reporter Jean H. Lee purportedly used this 3G network to post to both Twitter and Instagram. However, citizens are not generally allowed to use the 3G network.⁷⁵

Email is also regulated by the regime. The first email provider in North Korea was Silibank. Silibank has servers in Pyongyang and Shenyang and is a joint venture with China. The North Korean Silibank homepage is silibank.net, and the Chinese homepage is silibank.com. In order to use the email service, users had to initially register, provide personal information, and pay a registration fee and monthly service fees.⁷⁶ This registration information was current as of 2001. However, it is unknown whether the same process still applies.

WHOIS records for silibank.net show that the site was registered anonymously via a Japanese registrar. This information can be found in [Appendix A](#) at the end of this paper.

⁷¹ <http://www.citylab.com/work/2014/02/north-korea-night-looks-big-black-hole/8484/>

⁷² <http://www.northkoreatech.org/2014/06/24/chinese-shops-offer-cheap-cellphones-to-north-koreans/>

⁷³ <http://www.defense.gov/pubs/ReporttoCongressonMilitaryandSecurityDevelopmentsInvolvingtheDPRK.pdf>

⁷⁴ http://www.defense.gov/pubs/North_Korea_Military_Power_Report_2013-2014.pdf

⁷⁵ <http://www.austinchronicle.com/daily/sxsw/2013-03-11/social-media-in-north-korea/>

⁷⁶ <http://edition.cnn.com/2001/TECH/internet/11/07/north.korea.email.idg/index.html>

Korea Computer Center (KCC) is North Korea's leading government research center for information technology. KCC has eleven regional information centers and eight development and production centers. Other countries with KCC branch offices include China, Syria, Germany, and United Arab Emirates. KCC has a vested interest in Linux research and is responsible for the development of North Korea's national operating system, Red Star OS, which is discussed in more detail below. KCC's other projects have included a proprietary search engine, a document writer, a game called Jang-Gi, the Kwangmyong intranet, a food study program, a Korean input method editor, a pen-based English-Korean and Korean-English translator, Korean voice recognition software, a video conferencing system, a distance education system, SilverStar Paduk software, HMS Player⁷⁷, and the Samjiyon tablet.⁷⁸ In addition to research and development, KCC also monitors websites of foreign government and business entities and conducts technical reconnaissance to blueprint the technical specifications and vulnerabilities in foreign systems and technologies. KCC has also been involved in clandestine information and cyber operations, serving as a command center.⁷⁹

North Korea's proprietary operating system is Red Star OS. The development of this Linux-based operating system started in 2002. Red Star OS is only offered in the Korean language and features proprietary software including Naenara (a Firefox-based browser), as well as a text editor, email client, audio and video players, and games.⁸⁰ Red Star OS's keyboard layouts include Korean, English, Russian, Chinese, and Japanese. Regime ideals extend to Red Star OS. The readme file, which goes with the installation disc, reportedly includes a quote from Kim Jong-Il regarding the importance of North Korea having its own Linux-based operating system that is compatible with Korean traditions. While prior versions of Red Star were KDE-based, version 3.0 mimics Apple's OS X.⁸¹ ⁸² This could indicate the regime leader Kim Jong Un's preference for the OS X environment, as Kim reportedly uses an iMac.⁸³ Citizens do not need permission to obtain Red Star OS. However, the purchase of computers is heavily regulated.⁸⁴ The OS's design suggests it was developed with means for the regime to monitor user activity.⁸⁵

North Korea is known to use two IP ranges. 175.45.176.0/22 is North Korea's own IP block.⁸⁶ Additionally, North Korea's Telecommunications Ministry is the registered user of China Unicom IP range 210.52.109.0/24.⁸⁷ The country's only autonomous system (AS) number is AS131279, and its only peer is AS4837, the AS for China Unicom.⁸⁸

North Korea's country code top-level domain (ccTLD) is .kp. In 2007, the .kp TLD was initially delegated to and administered by the German-based KCC Europe.⁸⁹ After KCC Europe failed to

⁷⁷ <http://www.naenara.com.kp/en/kcc/>

⁷⁸ <http://www.northkoreatech.org/2012/09/28/samjiyon-android-tablet-debuts-at-pyongyang-trade-fair/>

⁷⁹ <http://www.ists.dartmouth.edu/docs/cyberwarfare.pdf>

⁸⁰ <http://ashen-rus.livejournal.com/4300.html>

⁸¹ <http://news.bbc.co.uk/2/hi/technology/8604912.stm>

⁸² http://www.arnnet.com.au/article/537360/north_korea_goes_osx-like_new_operating_system/

⁸³ <http://www.businessinsider.com/brand-new-photo-confirms-that-kim-jong-un-is-a-mac-user-2013-3>

⁸⁴ <http://rt.com/news/north-korea-cyber-weapon/>

⁸⁵ <http://news.bbc.co.uk/2/hi/technology/8604912.stm>

⁸⁶ <http://binarycore.org/2012/05/29/investigating-north-koreas-netblock-part-2-dns/>

⁸⁷ <https://www.northkoreatech.org/2011/06/26/north-koreas-chinese-ip-addresses/>

⁸⁸ <http://binarycore.org/2012/05/29/investigating-north-koreas-netblock-part-2-dns/>

⁸⁹ <http://www.northkoreatech.org/2011/05/19/kp-domain-switch-came-after-kcc-europe-disappeared/>

maintain the TLD, it was re-delegated to Star Joint Venture Company.⁹⁰ The .kp TLD uses the following nameservers and IP addresses:⁹¹

Nameserver	IP Address
ns1.kptc.kp	175.45.176.15
ns2.kptc.kp	175.45.176.16
ns3.kptc.kp	175.45.178.173

Various U.S., U.N, and other sanctions prohibit export of dual-use technologies to North Korea. In light of this, North Korea has managed to develop both hardware and software and hosts an annual National Exhibition of Invention and New Technologies to promote its products.⁹² However, the regime has historically failed in its attempts at large-scale production of electronic components. The country's sparse electrical grid is one of the major obstacles hindering large-scale manufacturing.⁹³ Additionally, the famine in the early 1990's negatively impacted existing manufacturing facilities, and the regime simply does not have the capital to modernize those factories.⁹⁴ A member of the World Intellectual Property Organization (WIPO), North Korea joined the WIPO Patent Cooperation Treaty that protects patents and trademarks worldwide, and leverages intellectual property laws to ensure Westerners do not take credit for North Korean inventions.⁹⁵ The regime, in its efforts to isolate its citizens from Western influence, leverages intellectual property laws to ensure Westerners do not take credit for North Korean inventions.⁹⁶ This is ironic since foreign-made electronic components are sometimes smuggled into North Korea for military use and for personal use by the regime's upper echelon.

An analysis of developments in North Korean cyberspace since 2010

A comparison of a scan⁹⁷ of North Korea's IP ranges in November 2010, just one month after North Korea made its first direct connection to the Internet, and a series of several scans we conducted in May 2014, shows that North Korea has made significant headway in establishing its Internet presence.

In the November 2010 scan, 175.45.176.0 - 175.45.176.16 showed a variety of devices including D-link, Cisco, Linksys, HP, and Nokia devices, and a Juniper networks firewall. Operating systems detected included FreeBSD 6.x, Linux 2.6.x, and Red Hat Enterprise Linux. 175.45.176.14 returned "Naenara" as an html-title. Most hosts in the 175.45.176.xx and 175.45.177.xx ranges were down. As of 2014, IP addresses 175.45.176.0 - 175.45.177.255 appear to be used for websites, nameservers, databases, email, and voice over IP (VoIP). In November 2010, the 175.45.178.xx range showed all hosts down,⁹⁸ and the 175.45.179.xx range showed most hosts were down.⁹⁹

⁹⁰ <http://www.iana.org/reports/2011/kp-report-20110401.html>

⁹¹ <http://www.iana.org/domains/root/db/kp.html>

⁹² http://yu.edu/admissions/events/yunmun/WIPO/Libenstein_WIPO_Topic1_HAHS.pdf

⁹³ <http://www.apcss.org/Publications/Edited%20Volumes/BytesAndBullets/CH4.pdf>

⁹⁴ <http://sinonk.com/2013/10/11/a-primer-on-north-koreas-economy-an-interview-with-andrei-lankov/>

⁹⁵ http://yu.edu/admissions/events/yunmun/WIPO/Libenstein_WIPO_Topic1_HAHS.pdf

⁹⁶ http://yu.edu/admissions/events/yunmun/WIPO/Libenstein_WIPO_Topic1_HAHS.pdf

⁹⁷ <http://webcache.googleusercontent.com/search?q=cache:http://dprk.sipsik.net/175.45.178.txt>

⁹⁸ <http://webcache.googleusercontent.com/search?q=cache:http://dprk.sipsik.net/175.45.178.txt>

⁹⁹ <http://webcache.googleusercontent.com/search?q=cache:http://dprk.sipsik.net/175.45.179.txt>

In 2014, several webservers and nameservers were found in the 175.45.178.xx range, and several nameservers and mail servers were found in the 175.45.179.xx range. This comparison demonstrates that there has been some growth in DPRK Internet infrastructure over the past four years. However, it seemingly lags behind even most third world nations. The 2014 scans detected dated technology that is potentially susceptible to multiple vulnerabilities and consistently showed the same open ports and active devices on scanned hosts. It is not clear whether the regime failed to notice and react to the scanning or whether the regime allows these open ports and devices to be detected or spoofed to serve as a distraction or possible honeypot.

Domains, nameservers, and mail servers present during the May 2014 scan are listed in [Appendix B](#) at the end of this report.

According to Alexa rankings, the three most visited websites in North Korea are kcna.kp, the official website of the Korean Central News Agency (KCNA)¹⁰⁰; rodong.rep.kp, another North Korean news site¹⁰¹; and naenara.com.kp, North Korea's official web portal.¹⁰² Naenara translates to "my country".

The kcna.kp site was registered using a Loxley.co.th email address and is administrated by Star Joint Venture Company. The WHOIS Record can be found in [Appendix A](#).

¹⁰⁰ <http://dig.do/kcna.kp>

¹⁰¹ <http://dig.do/rodong.rep.kp>

¹⁰² <http://dig.do/naenara.com.kp>

김정은동지의 혁명활동



- ▶ 김정은동지께서 아.노비첸코의 생일 100 위대한 김일성대원수님과 김정일대원수님의 동상을 높이 모신 송도원국제소년단아영소 준공식 성대히 진행
- ▶ 김정은동지께서 항일혁명투사에게 생일상을 보내시었다
- ▶ 김정은동지께서 송도원국제소년단아영소 개건에서 표격적위훈을 세운 조선인민군 제 267군부대 군인건설자들과 함께 기념사진을 찍으시었다
- ▶ 김정은원수님을 모시고 송도원국제소년단아영소에서 전국소년체육경기대회 결승경기와 모란봉악단의 축하공연 진행,축포 발사
- ▶ 위대한 김일성대원수님과 김정일대원수님의 동상을 높이 모신 송도원국제소년단아영소 준공식 성대히 진행
- ▶ 김정은동지께서 새로 건설한 김정숙평양방직공장 노동자합숙을 돌아보시었다

태양절경속소식

- ▶ 김일성동지께서 인류해방과 자주위업에 쌓아올린 업적을 뽐스꺼단체 칭송
(평양 5월 3일밤 조선중앙통신)
위대한 수령 김일성동지의 탄생일에 즈음하여 조선과의 친선협회 협스꺼지부가 4월 15일 성명을 발표하였다.
- ▶ 태양절과 조선인민군항전 82년을 여러 나라에서 경축
- ▶ 태양절경속행사 조선체육대표부들에서 진행
- ▶ 김정은동지께서 러시아,중국인사들이 축전과
- ▶ 태양절경속행사 무바,뽀너지에서 진행

질세위인들의 혁명업적

중요소식

- ▶ 조선총리 숙천군인의 품질영농실적 현 지료해
- ▶ 조선로동당 중앙위원회와 당중앙군사위원회에서 조선인민군 제267군부대장병들에게 감사문을 보내었다
- ▶ 천하역적무리들의 반민족적죄행은 절대로 용납되지 않을것이며 엄중히 계신될것이다-조선평화옹호전국민족위원회 대변인답학
- ▶ 김정은동지께서 양굴리대통령이 축전을 보내어왔다
- ▶ 조선에서 경제개발구전문기토론회 진행
- ▶ 박근혜야말로 한시바빠 제거해야 할 민족의 특등재일거리이다 - 하늘갈까지 치솟는 분노인 민심의 폭발
- ▶ 조선에서 심한 가을현상 지속
- ▶ 5.1절경속 로동자연회 성대히 진행
- ▶ 미국이 락탈한 민족문화재마저 동족대결에 악용하는 박근혜패당의 반민족적죄행은 절대로 용납될수 없다 - 민족유산보호지도국 대변인답학
- ▶ 김정은동지께서 몽골대통령이 축전을 보내어왔다

체육



- ▶ 조선의 전통적이며 대중적인 민족체육종목 협스꺼기

Figure 4 A screenshot from the kcna.kp homepage.¹⁰³

Rodong.rep.kp was registered using the same loxley.co.th email address and is also administered by Star Joint Venture Company. The WHOIS Record for this site can be found in [Appendix A](#).

¹⁰³ <http://kcna.kp/kcna.user.home.retrieveHomeInfoList.kcmsf>

경애하는 김정은원수님을 모시고 송도원국제소년단아영소에서 전국소년축구경기대회 결승경기와 모란봉악단의 축하공연 진행, 축포 발사

우리 당의 후대사망의 최고
경리로 훌륭히 임하신 송도원국제
소년단아영소 준공을 축하하는
체육동화행사가 2일 현지에서
성황리에 진행되었다.

위대한 김일성대원수님과
위대한 김정일대원수님의 통상을
높이 모신 아영소에서 경애하는
김정은원수님을 또다시 한사리
에 모시고 체육경기와 명성높은
모란봉악단의 공연을 관람하게
될 참가자들의 가슴속에는 무한
한 감격과 행복으로 세차게 실재
하고있었다.

동해명승 송도원의 자연풍치
와 어울리게 흥흥히 진행된
이러한운동장에서는 전국소년축
구경기대회 결승경기가 진행되
었다.

우리 당과 인민의 최고명도자
이신 경애하는 김정은원수님께서
관람하게 나오시었다.

전체 관람자들과 선수들은
후대들에게 들려줄 또 하나의
귀중한 세무인 세계일류국의 과
외문화경관기지를 마련해주시고 내세울
은 은정들을 거듭 베풀어주시는 경애하는
원수님을 우리러 열방의 환호성을 터쳐
올리었다.

황해동지, 김기남동지, 최재복동지,
최봉재동지, 한광상동지, 미일환동지, 최희
동지, 이원훈동지, 김이경동지와 전용남 청
년동맹중앙위원회 위원장, 아영소의 일군
들과 운영직원, 동격대원들, 청년동맹일군
들, 강연도내 학생소년들과 일군들이 경기
를 보았다.

이어나갈 후대만이 비친 빛명이전속
불인 아영소의 산뜻한 야외운동장에서 첫
경기를 치른 평안남도팀과 함경남도팀
의 소년축구선수들의 열광이다에는 끝없는
환희의 향연이 한껏 이룩되었다.

선군소년의 영예를 떨치는 미래의 축구
선수로서 자랑 될의인고 우순취 편이세운
자거들의 체육기지를 날김없이 발휘하는
소년축구선수들의 미더운 모습을 보여 관람
자들은 흥취열기를 높여었다.

경기 시작부터 열활약을 하던 함경
의 환호성이 경기장의 하늘가에 예이리쳐
났다.



10분경 모기 좋은 국점으로 첫 골문을
열었다.

많은 점수를 회복하기 위해 상대팀의
골문을 무안히 위협하던 평안남도팀의
5인 김현성선수가 후반전 23분경에
이필대 동점골을 넣기 경기는 더욱 치열
해졌다.

나이는 이케도 능숙한 골물기와 집단주
의경신, 훌륭한 경기도리용성을 발휘하는
선수들에게 관람자들은 아낌없는 박수갈채
를 보내었다.

후반전마감까지 득점이 이루어지지
않아 승부차기가 진행되었다.
경기 경기에서는 함경남도팀이 평안남도
팀을 5:4로 이겼다.

이러 이상이 있었다.
축구경기를 통하여 선수들은 세늘의 나
래를 활짝 쳐고 이날의 체육경극을 피레고
나갈 축구선수로서 자리나는 우리 학생소년
들의 활발한 모습을 잘 보여주었다.

경기가 끝나자 또다시 우렁찬 《만세!》
의 환호성이 경기장의 하늘가에 예이리쳐
났다.

경애하는 김정은원수님께서 끝없는
영광과 행복에 겨워 목청껏 환호를 올리는
선수들과 관중자들에게 마친한 담겨를
편으시었다.

또한 눈물을 흘리며 격정의 환호를
올리는 경기모성성원들까지 들기까지

감격, 심정충동의 손을 빌일이 깊어주시며
그들을 고무해주시고 함께 기념사진을
찍으시었다.

위대한 김정은원수님의 품안의 입적들
우리 식 경승악의 황후하고 융합한 윤민
으로 감명깊게 형성하였다.

부르시어 사랑의 기념사진을 찍어
주시는 현왕상은 은정을 베풀
어주시었다.

전체 관람자들과 선수들은
환없이 승고한 미래사망의 세
력사를 펼쳐가시는 경애하는
김정은원수님의 크나큰 믿음과
사랑을 가슴깊이 간직하고 강경
국가건설에 활달계 이바지하여
선군조선을 빛내어갈 체육인주
이로 역세게 사리날 길에 넘쳐
있었다.

경애하는 김정은원수님을
모시고 이날 송도원국제소년단
아영소 국제친선소년대회에서는
모란봉악단의 축하공연 《세상에
부담없이라!》가 진행되었다.

내성중앙 《소년단행진곡》
으로 시작된 공연부터는 다채
로운 흥취들이 울렸다.

출연자들은 아이들을 나라의
왕이라고 하시기 전국적 경지출
은 뜻이더애 소년공원의 아영소
를 세워주시고 한평생 후대
사망의 역사를 추능하시어 오신



Figure 5 A screenshot from the rodong.rep.kp homepage.¹⁰⁴

The WHOIS information for Naenara.com.kp was not available.

¹⁰⁴ http://rodong.rep.kp/ko/



Figure 6 A screenshot of the Naenara.com.kp website.¹⁰⁵

In March 2013, there were reports that the Chrome browser was blocking Naenara.com.kp due to malware.¹⁰⁶

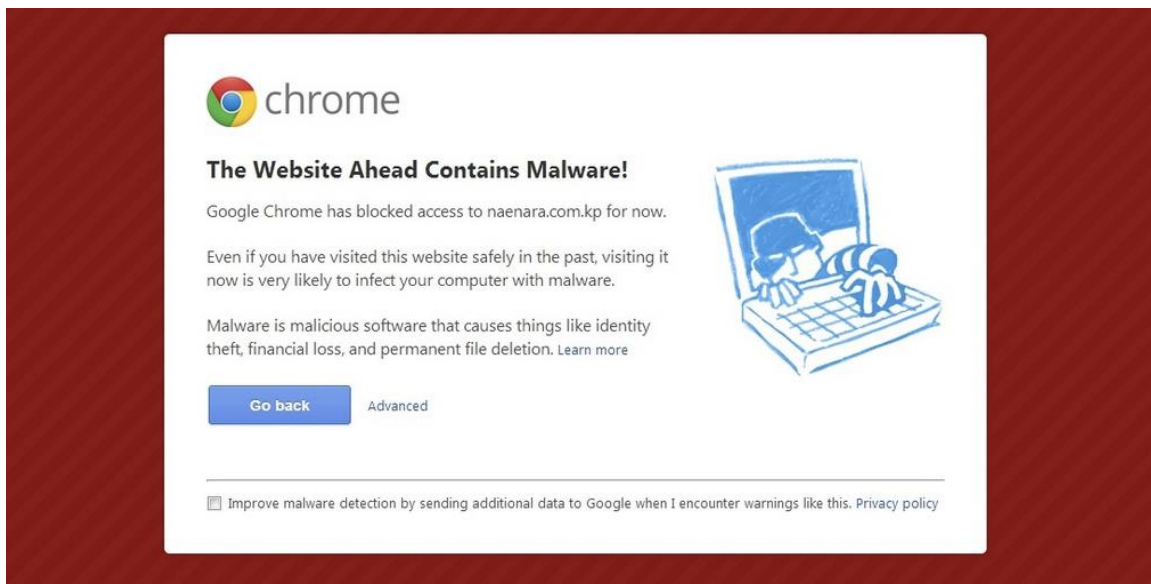


Figure 7 Screenshot of what visitors to Naenara.com.kp saw when using the Chrome browser.¹⁰⁷

¹⁰⁵ <http://naenara.com.kp/en/>

¹⁰⁶ <http://www.nkeconwatch.com/2013/03/25/chrome-blocking-naenara/>

¹⁰⁷ <http://www.nkeconwatch.com/2013/03/25/chrome-blocking-naenara/>

What is the current listing status for naenara.com.kp?

Site is listed as suspicious – visiting this web site may harm your computer.

Part of this site was listed for suspicious activity 2 time(s) over the past 90 days.

What happened when Google visited this site?

Of the 5628 pages we tested on the site over the past 90 days, 18 page(s) resulted in malicious software being downloaded and installed without user consent. The last time Google visited this site was on 2013-03-19, and the last time suspicious content was found on this site was on 2013-03-15.

Malicious software includes 143 exploit(s), 9 trojan(s). Successful infection resulted in an average of 16 new process(es) on the target machine.

Malicious software is hosted on 3 domain(s), including zief.pl/, ecpage.sakura.ne.jp/, chura.pl/.

This site was hosted on 1 network(s) including AS131279 (STAR).

Figure 8 Screenshot detailing why Chrome blocked the site¹⁰⁸

It is difficult to say whether this incident is a case of North Korea serving malware or whether a third party took advantage of an improperly secured website.

Several major North Korean websites are hosted outside of North Korea. The popular Uriminzokkiri.com website, whose name translates to “our nation,” is hosted in China. The administrative contact for the website is Kim Sejun, and the email address given as contact information is hyk1979@hotmail.com. The WHOIS Record for this site can be found in [Appendix A](#).

¹⁰⁸ <http://www.nkeconwatch.com/2013/03/25/chrome-blocking-naenara/>



Figure 9 A screenshot of the Uriminzokkiri website ¹⁰⁹

The website for Kim Il Sung Open University, otherwise known as “Our Nation School” is also hosted in China. The WHOIS record for this site can be found in [Appendix A](#).

¹⁰⁹ <http://www.uriminzokkiri.com/>



최근소식 News

- ▶ 경애하는 김정은 원수님을 모시고 송도원국제소년단아영사에서 전국소년체육대회 결승경기와 모란봉악단의 축하공연 진행, 축포 발사
- ▶ 경애하는 최고사령관 김정은 동지께서 송도원국제소년단아영사개건에서 로력적 위훈을 세운 조선인민군 제267군부대 군인간사들과 함께 기념사진을 찍으시었다
- ▶ 위대한 김일성대원수님과 김정일대원수님의 동상을 높이 모신 송도원국제소년단아영사 준공식 성대히 진행
- ▶ 북남로동자단체 공동결의문
- ▶ 5.1절경축 로동자대회 성대히 진행
- ▶ 반역의 무리들은 더 큰 비난을 불러오기 전에 하루빨리 쓸어버려야 한다.

대학소식 Words from our university

- ▶ 특강 <조선인민군이 걸어온 82년은 수령결사옹위로 주체혁명의 영광을 이어온 자랑찬 역사>
- ▶ 특강 <만경대가문의 송고한 가품>
- ▶ 특강 <위대한 김일성동지는 언제나 남녘동포들에게 뜨거운 사랑과 은정을 베풀어 주신 영원한 민족의 어버이이다 >
- ▶ 김일성방사대학에서 알려드립니다
- ▶ 김일성방사대학 제48기 개학식
- ▶ 우리민족당출판지를 통한 강의형식과 내용을 새롭게 구성하였습니다.
- ▶ 경애하는 김정은 동지의 로작 <사회주의 농촌체제의 기치를 높이 들고 농업생산에서 혁신을 일으키자>



논문 (treatise)

- ▶ 경애하는 김정은 동지를 중심으로 하는 전인민적의 일심단결은 사회주의강성국가건설의 위력한 추진력
- ▶ 육체적성명보다 사회정치적성명을 더 귀중히 여기는 것은 사람의 본성적요구
- ▶ 새로운 주체100년의 첫해를 위대한 승리와 영광으로 빛내이신 불멸의 업적
- ▶ 위대한 김정일동지를 우리 당과 인민의 영원한 수령으로 높이 모시는것은 주체혁명위업, 선군혁명위업완성의 확고한 담보
- ▶ 조선민주주의인민공화국은 인민의 영원한 송과 행복의 요람

물음과 대답 (FAQ)

- ▶ 조선민주주의인민공화국의 본질에 대하여
- ▶ 경애하는 김정은 동지의 로작 <위대한 김정일동지를 우리 당의 영원한 총비서로 높이 모시고 주체혁명위업을 빛나게 완성해나가지자> 의기본사상과 체계에 대하여
- ▶ 자주의 원칙을 견지하는데서 나서는 중요한 요구는 무엇인가?
- ▶ 대고조진군길에서 우리 군대와 인민이 발휘하고있는 공격정신은 어떤 정신인가
- ▶ 진달래학생에게 보내는 해답입니다.
- ▶ 유엔안전보장리사회 <결의>의 부당성은 어디에 있는가

연단 (rostrum)

- ▶ 민족의 안전과 평화수호는 우리 당과 공화국정부의 밀관한 임장
- ▶ 실천행동으로 대답해야 한다
- ▶ 개요 <그이 없인 못살아>를 통해보는 경애하는 김정은원수님의 위인상
- ▶ <집단지자위원>에 대한 승인은 일본반동들을 해외 침략으로 부추기는 전주곡
- ▶ 우리 민족끼리는 6.15북남공동선언의 기본정신
- ▶ 케번으로 진리를 오도할수 없다

Figure 10 A screenshot of ournation-school.com.¹¹⁰

North Korean cyber war and intelligence structure

At the top of North Korea’s military structure is the National Defense Commission (NDC). The NDC is also the highest branch of government and the regime’s supreme policymaking body.¹¹¹ Along with the Central Committee of the Workers’ Party of Korea and the Cabinet, NDC is at the top of

¹¹⁰ <http://www.ournation-school.com/>

¹¹¹ <https://nkleadershipwatch.wordpress.com/dprk-security-apparatus/national-defense-commission/>

North Korea's political hierarchy.¹¹² Article 106 of North Korea's Constitution gives the NDC the following powers:¹¹³

- The power to establish policies of the state in accordance with the military-first revolutionary line.
- The power to guide the armed forces and oversee defense building.
- The power to supervise and ensure the NDC and its chairman's orders are executed and to establish necessary measures.
- The power to override any state decisions or directives that are in opposition to the NDC or its chairman's decisions and directives.
- The power to create or remove central organs of the national defense sector.
- The power to create and bestow military titles above general-grade officer rank.

The NDC oversees several defense and intelligence bodies including the Ministry of State Security, the Ministry of People's Security, the Ministry of People's Armed Forces, and the Korean People's Army. The Ministry of State Security (MSS), also known as the State Security Department, is North Korea's primary counterintelligence service. It is considered an autonomous agent of the regime and reports directly to leader Kim Jong Un. The MSS's duties include oversight of North Korean prison camps, investigation of domestic espionage, repatriation of defectors, and overseas counterespionage operations.¹¹⁴ The Ministry of People's Security is also known as the Ministry of Public Security (MPS). Focused on domestic order, it oversees North Korea's national police force, conducts criminal investigations and preliminary examinations, and oversees correctional facilities, excluding prison camps.¹¹⁵ While the roles of the MSS and MPS focus more on intelligence than on cyber operations, the MSS also reportedly has a communications monitoring and computer hacking group.¹¹⁶

The Ministry of People's Armed Forces (MPAF) administrates the Korean People's Army (KPA) and oversees the General Staff Department (GSD), which is responsible for operational command and control of North Korea's armed forces. The General Staff Department also oversees the Reconnaissance General Bureau (RGB), North Korea's agency for clandestine operations. The RGB has a role in both traditional and cyber operations. In the past, the RGB has sent agents on overseas military assistance missions to train insurgent groups.¹¹⁷ The RGB reportedly has a special operations forces (SOF) element¹¹⁸ and oversees six bureaus that specialize in operations, reconnaissance, technology and cyber matters, overseas intelligence collection, inter-Korean talks, and service support.¹¹⁹ Two of these bureaus have been identified as the No. 91 Office and Unit 121. The No. 91 Office, an office responsible for hacking, operates out of the Mangkyungdae-district of

Unit 121 comprises both an intelligence component and an attack component. One of Unit 121's command posts is Chilbosan Hotel in Shenyang, China. Unit 121 maintains technical reconnaissance teams responsible for infiltration of computer networks, hacking to obtain intelligence, and planting viruses on enemy networks.

¹¹² <http://whataboutnorthkorea.nl/2013/02/the-korean-workers-party/>

¹¹³ <http://asiamatters.blogspot.co.uk/2009/10/north-korean-constitution-april-2009.html>

¹¹⁴ http://www.defense.gov/pubs/North_Korea_Military_Power_Report_2013-2014.pdf

¹¹⁵ <http://www.factba.se/handbook-page.php?id=1129700>

¹¹⁶ [http://www.csmonitor.com/World/Security-Watch/2013/1019/In-cyberarms-race-North-Korea-emerging-as-a-power-not-a-pushover/\(page\)/4](http://www.csmonitor.com/World/Security-Watch/2013/1019/In-cyberarms-race-North-Korea-emerging-as-a-power-not-a-pushover/(page)/4)

¹¹⁷ <http://www.strategicstudiesinstitute.army.mil/pdffiles/pub771.pdf>

¹¹⁸ <http://www.strategicstudiesinstitute.army.mil/pdffiles/pub771.pdf>

¹¹⁹ http://www.defense.gov/pubs/North_Korea_Military_Power_Report_2013-2014.pdf

Pyongyang.¹²⁰ Unit 121 comprises both an intelligence component and an attack component. Unit 121's headquarters is in the Moonshin-dong area of Pyongyang, near the Taedong River.¹²¹ It also has components that conduct operations from within China. One of Unit 121's command posts is Chilbosan Hotel¹²² in Shenyang, the capital of Liaoning Province, which borders North Korea.¹²³ Shenyang is a Chinese military district.¹²⁴ According to Dr. Alexandre Mansourov, an expert on North Korea and a visiting scholar at the U.S.-Korea Institute at Johns Hopkins University, "They [Unit 121] are believed to have conducted hacking operations from inside China that falsify classified data and disrupt U.S. and South Korean systems."¹²⁵ Both Unit 121 and an entity known as Lab 110 are reported to maintain technical reconnaissance teams responsible for infiltrating computer networks, hacking to obtain intelligence, and planting viruses on enemy networks.^{126 127}



Figure 11 A map pinpointing the location of the Chilbosan Hotel.¹²⁸

¹²⁰ <http://www.infosecisland.com/blogview/21577-Concerns-Mount-over-North-Korean-Cyber-Warfare-Capabilities.html>

¹²¹ <http://www.aljazeera.com/indepth/features/2011/06/201162081543573839.html>

¹²² <http://www.scribd.com/doc/15078953/Cyber-Threat-Posed-by-North-Korea-and-China-to-South-Korea-and-US-Forces-Korea>

¹²³ [http://www.csmonitor.com/World/Security-Watch/2013/1019/In-cyberarms-race-North-Korea-emerging-as-a-power-not-a-pushover/\(page\)/4](http://www.csmonitor.com/World/Security-Watch/2013/1019/In-cyberarms-race-North-Korea-emerging-as-a-power-not-a-pushover/(page)/4)

¹²⁴ http://www.defense.gov/pubs/2014_DoD_China_Report.pdf

¹²⁵ [http://www.csmonitor.com/World/Security-Watch/2013/1019/In-cyberarms-race-North-Korea-emerging-as-a-power-not-a-pushover/\(page\)/4](http://www.csmonitor.com/World/Security-Watch/2013/1019/In-cyberarms-race-North-Korea-emerging-as-a-power-not-a-pushover/(page)/4)

¹²⁶ <https://www.usnwc.edu/getattachment/8e487165-a3ef-4ebc-83ce-0ddd7898e16a/The-Republic-of-Korea-s-Counter-asymmetric-Strateg>

¹²⁷ Clarke, R. A. (2012). *Cyber war: The next threat to national security and what to do about it*. New York, NY: Ecco.

¹²⁸ maps.google.com

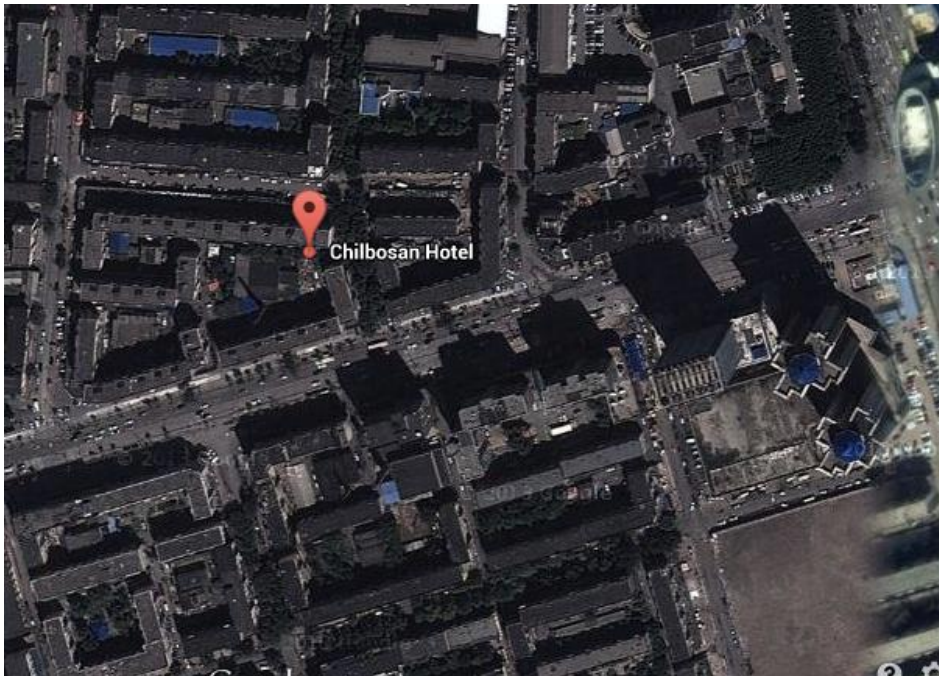


Figure 12 A satellite view of the Chilbosan Hotel.¹²⁹

Several entities are nested under the Workers' Party. The Central Party Committee oversees the Central Party Investigative Group, also known as Unit 35.¹³⁰ Unit 35 is reportedly responsible for technical education and training of cyber warriors.¹³¹ The Unification Bureau's¹³² Operations Department is responsible for cyber-psychological warfare, organizational espionage, and oversight of Unit 204. Unit 204's responsibilities include planning and execution of cyber-psychological warfare operations and technological research. The Psychological Operations Department of the North Korea Defense Commission also engages in cyber-psychological warfare.¹³³ The 225th Bureau, or Office 225, is responsible for training agents, infiltration operations in South Korea, and creation of underground political parties in order to incite disorder and revolution. It plays a more traditional intelligence and psychological operations role, rather than focusing on cyber operations.¹³⁴ The United Front Department (UFD) conducts overt operations to create pro-North Korean groups in South Korea. Examples of this activity include the Korean Asia-Pacific Committee and the Ethnic Reconciliation Council. The UFD also manages inter-Korean dialogue and North Korea's policy toward South Korea. Its operations are also more traditional rather than cyber-focused.¹³⁵

The Unification Bureau falls under the Workers' Party. Its Operations Department is responsible for cyber-psychological warfare, organizational espionage, and oversight of Unit 204. Unit 204's responsibilities include planning and execution of cyber-psychological warfare operations and technological research. The Psychological Operations Department of the North Korea Defense Commission also engages in cyber-psychological warfare.

¹²⁹ maps.google.com

¹³⁰ Clarke, R. A. (2012). *Cyber war: The next threat to national security and what to do about it*. New York, NY: Ecco.

¹³¹ <https://www.usnwc.edu/getattachment/8e487165-a3ef-4ebc-83ce-0ddd7898e16a/The-Republic-of-Korea-s-Counter-asymmetric-Strateg>

¹³² <http://goodfriendsusa.blogspot.co.uk/2008/07/north-korea-today-no174.html>

¹³³ <https://www.usnwc.edu/getattachment/8e487165-a3ef-4ebc-83ce-0ddd7898e16a/The-Republic-of-Korea-s-Counter-asymmetric-Strateg>

¹³⁴ http://www.defense.gov/pubs/North_Korea_Military_Power_Report_2013-2014.pdf

¹³⁵ http://www.defense.gov/pubs/North_Korea_Military_Power_Report_2013-2014.pdf

The Liaison Department of the Worker's Party oversees a faction of ethnic North Koreans residing in Japan who are critical to North Korea's cyber and intelligence programs. This group, which was established in 1955, is referred to by various names including the Chosen Soren, Chongryon, and the General Association of Korean Residents in Japan.¹³⁶ The Chongryon ascribe to *juche* and seek to preserve North Korean culture while living in Japan. They operate North Korean style schools and refuse to assimilate with Japanese culture.¹³⁷ According to Mitsuhiro Suganuma, former section head of the second intelligence department of the Japanese Public Security Intelligence Agency (PSIA), "Chongryon is virtually under the direct control of the Liaison Department of the Workers' Party of Korea, which has been in charge of North Korea's covert operations and underground activities against South Korea. Chongryon in Japan has been a strong support organization aimed at bringing a revolution in South Korea, or a red unification by force." He also stated "North Korea will continue to make Chongryon serve as Pyongyang's pawn in covert operations against South Korea."¹³⁸ The Chongryon are vital to North Korea's military budget, raising funds via weapons trafficking, drug trafficking, and other black market activities.¹³⁹ The group also forms "front companies" abroad that benefit the regime by generating hard currency. One example is Unikotech, which was formed to sell KCC products abroad.¹⁴⁰ The Chongryon's underground group known as the Gakushu-gumi, or "the study group", gathers intelligence for North Korea and helps the regime procure advanced technologies.¹⁴¹ The Chongryon's role in North Korean intelligence and resource acquisition is discussed below in more detail.

"Chongryon is virtually under the direct control of the Liaison Department of the Workers' Party of Korea, which has been in charge of North Korea's covert operations and underground activities against South Korea."

The regime also has several government bodies under the Cabinet¹⁴² that oversee its infrastructure, intelligence, and technological development. These include the Central Scientific and Technological Information Agency (CSTIA), the Ministry of Electronics Industry, and the Ministry of Posts and Telecommunications. The CSTIA collects, analyzes, and processes data regarding advanced science and technology then sends relevant information to appropriate areas of the national economy.¹⁴³ The amount of information contained in CSTIA's technical database makes it North Korea's largest scientific facility. According to a CIA article, review of CSTIA's publications showed that China, Russia, and Japan are important sources of technical data. CSTIA's publications include newsletters and an 18-volume science and technology reference series.¹⁴⁴ The Ministry of Posts and Telecommunications is the body of oversight for Star Joint Venture Co.¹⁴⁵

¹³⁶ <http://www.moj.go.jp/ENGLISH/PSIA/psia02-03.html>

¹³⁷ <http://www.moj.go.jp/ENGLISH/PSIA/psia02-03.html>

¹³⁸ <http://www.nknews.org/2014/02/chongryon-still-pyongyangs-pawn-in-covert-operations-former-intelligence-officer/>

¹³⁹ <http://www.ists.dartmouth.edu/docs/cyberwarfare.pdf>

¹⁴⁰ <http://www.learningace.com/doc/2025666/863b663a9fb13b456304dd0a3bc43547/cyberwarfare>

¹⁴¹ <http://www.ists.dartmouth.edu/docs/cyberwarfare.pdf>

¹⁴² <http://whataboutnorthkorea.nl/2013/02/the-korean-workers-party/>

¹⁴³ <https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/csi-studies/studies/vol48no1/article04.html>

¹⁴⁴ <https://www.cia.gov/library/center-for-the-study-of-intelligence/kent-csi/vol48no1/pdf/v48i1a04p.pdf>

¹⁴⁵ <https://www.northkoreatech.org/tag/ministry-of-posts-and-telecommunications/>

North Korean cyber and intelligence organizational chart

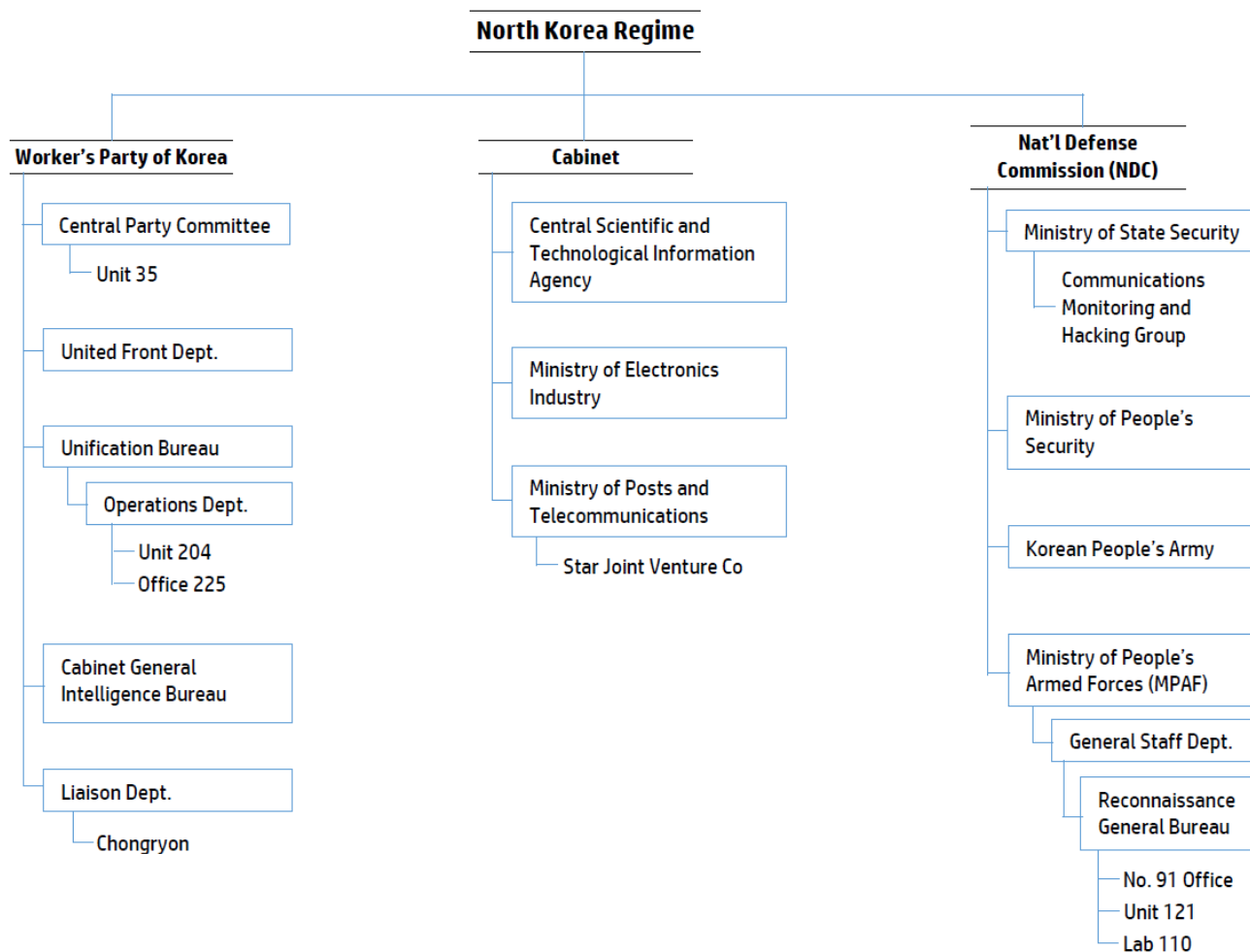


Figure 13 North Korean cyber and intelligence organizational chart

North Korea's cyber doctrine, strategies and goals

North Korea's cyber warfare doctrine has not been clearly stated. However, based on cultural and technical observations, we may deduce that North Korea's cyber doctrine follows the tenets of *juche* nationalism and the *songun* doctrine.

Although North Korea's limited online presence makes a thorough analysis of their cyber warfare capabilities a difficult task, it must be noted that what is known of those capabilities closely mirrors their kinetic warfare tactics. Cyber warfare is simply the modern chapter in North Korea's long history of asymmetrical warfare. North Korea has used various unconventional tactics in the

past, such as guerilla warfare, strategic use of terrain, and psychological operations.¹⁴⁶ The regime also aspires to create viable nuclear weapons.¹⁴⁷ Asymmetrical warfare is defined as “a conflict in which the resources of two belligerents differ in essence and in the struggle, interact and attempt to exploit each other’s characteristic weaknesses. Such struggles often involve strategies and tactics of unconventional warfare, the ‘weaker’ combatants attempting to use strategy to offset deficiencies in quantity or quality”.¹⁴⁸

According to the aforementioned report to the House Armed Service Committee, “Cyber warfare is an important asymmetric dimension of conflict that North Korea will probably continue to emphasize — in part because of its deniability and low relative costs.”¹⁴⁹ North Korea’s poor economic state¹⁵⁰, further explains the regime’s reliance on these tactics. In 2014, the regime reportedly spent 16% of its budget on defense.¹⁵¹ The North Korean military places a strong emphasis on information warfare capabilities including political and psychological warfare¹⁵² and cyber or hacker warfare.¹⁵³

The report by Capt. Duk-Ki Kim, Ph.D. highlighted North Korea’s counter-asymmetric strategy and ranked each based on intensity and frequency:

MAJOR NORTH KOREAN ASYMMETRIC THREATS

Category	Threat	Intensity	Frequency
Core	Nuclear blackmail, hostage threats	A	B
	Threats to turn Seoul into sea of flames	A	B
Major	Threats on Five West Sea Islands	A	A
	Rear disturbance, infiltration threats	B	B
	Cyber-attack threats (DDOS, etc.)	C	A
	Electromagnetic-attack threats	C	B
	Political-psychological offensive threats	C	A
Mixed	Symmetric-asymmetric mixed-attack threats	A	D

Note: A = high; B = medium; C = low; D = very low.

Figure 14 Threat matrix of North Korean asymmetric war capabilities.¹⁵⁴

Cyber warfare operations

Just ten years ago, experts noted that North Korea was one of the “least network-ready and most isolated societies on the planet.”¹⁵⁵ Today North Korea’s air-gapped networks and prioritization of resources for military use provide both a secure and structured base of operations for cyber operations and a secure means of communications.¹⁵⁶ North Korea’s hermit infrastructure creates

¹⁴⁶ <http://www.history.army.mil/brochures/kw-balance/balance.htm>

¹⁴⁷ <http://www.bbc.com/news/world-asia-pacific-11813699>

¹⁴⁸ http://www.princeton.edu/~achaney/tmve/wiki100k/docs/Asymmetric_warfare.html

¹⁴⁹ <http://docs.house.gov/meetings/AS/AS00/20140402/101985/HHRG-113-AS00-Wstate-ScaparrottiUSAC-20140402.pdf>

¹⁵⁰ http://www.foreignpolicy.com/articles/2013/04/29/7_things_north_korea_is_really_good_at

¹⁵¹ <http://blogs.wsj.com/korearealtime/2014/04/10/north-korea-details-budget-plans/>

¹⁵² <https://www.usnwc.edu/getattachment/8e487165-a3ef-4ebc-83ce-0ddd7898e16a/The-Republic-of-Korea-s-Counter-asymmetric-Strateg>

¹⁵³ <http://www.giac.org/paper/gsec/1870/information-warfare/103284>

¹⁵⁴ <https://www.usnwc.edu/getattachment/8e487165-a3ef-4ebc-83ce-0ddd7898e16a/The-Republic-of-Korea-s-Counter-asymmetric-Strateg>

¹⁵⁵ <http://www.apcss.org/Publications/Edited%20Volumes/BytesAndBullets/CH4.pdf>

¹⁵⁶ <http://docs.house.gov/meetings/AS/AS00/20140402/101985/HHRG-113-AS00-Wstate-ScaparrottiUSAC-20140402.pdf>

a cyber-terrain that deters reconnaissance. Because North Korea has few Internet connections to the outside world, anyone seeking intelligence on North Korea's networks has to expend more resources for cyber reconnaissance.¹⁵⁷ A 2003 article by the U.S. Office of the National Counterintelligence Executive assessed that "Development of the nation, rather than empowerment of the individual, appears to be driving DPRK efforts to develop domestic IT infrastructure and industry."¹⁵⁸ In November 2013, Kim Jong Un referred to cyber warfare capabilities as a "magic weapon" in conjunction with nuclear weapons and missiles.¹⁵⁹

According to Kim Heung-kwang, a North Korean defector and former computer science professor, the regime has the following motivations for expanding its cyber warfare capabilities:¹⁶⁰

- Cyber capabilities are a cost-effective way to offset North Korea's lack of kinetic military prowess.
- North Korea's school systems place a strong emphasis on math, giving the nation confidence in its programmers, cryptographers, and security researchers.
- In the modern warfare landscape, cyber capabilities are potentially more utilitarian than heavy artillery or aircraft.
- Cyber warfare capabilities provide a platform for espionage, psychological operations, and other forms of non-kinetic warfare.
- Considering the separatist nature of North Korea's infrastructure, cyber warfare provides a strategic advantage since outbound attacks are possible, but inbound attacks would have limited reach.
- Cyber warfare allows North Korea to leverage the Internet's inherent flaws for offensive purposes while maintaining its defenses, primarily via air-gapping its most critical networks from the outside world.

North Korea's attack and defense capabilities reportedly include the following cyber warfare and electronic warfare components: offensive cyber operations (OCO); computer network operations (CNO), which includes both computer network attack (CNA) and computer network exploitation (CNE); distributed denial of service (DDoS);¹⁶¹ satellite monitoring; drones; GPS jamming capabilities¹⁶²; and deployment of electromagnetic pulse (EMP).¹⁶³ North Korea's OCO and CNO capabilities became apparent as early as 2004, when North Korea reportedly gained access to 33 of 80 South Korean military wireless communication networks. In June 2006, an attack on the U.S. State Department originating in the East Asia-Pacific region coincided with U.S.-North Korea negotiations over the regime's nuclear missile testing.¹⁶⁴ A month later, a South Korean military report implicated North Korea's Unit 121 in hacking the South Korean and U.S. Defense Departments. North Korea also tested a logic bomb in October 2007. A logic bomb is malicious

¹⁵⁷ http://www.huffingtonpost.com/2011/07/25/digital-revolution-north-korea_n_908368.html

¹⁵⁸ http://www.ncix.gov/publications/archives/docs/NORTH_KOREA_AND_FOREIGN_IT.pdf

¹⁵⁹ http://english.chosun.com/site/data/html_dir/2013/11/05/2013110501790.html

¹⁶⁰ <http://www.aljazeera.com/indepth/features/2011/06/201162081543573839.html>

¹⁶¹ <http://www.defense.gov/pubs/ReporttoCongressonMilitaryandSecurityDevelopmentsInvolvingtheDPRK.pdf>

¹⁶² <https://www.usnwc.edu/getattachment/8e487165-a3ef-4ebc-83ce-0ddd7898e16a/The-Republic-of-Korea-s-Counter-asymmetric-Strateg>

¹⁶³ http://www.theregister.co.uk/2014/04/22/norks_drones_made_in_china/

¹⁶⁴ <http://www.informationweek.com/state-department-releases-details-of-computer-system-attacks/d/d-id/1045112>

code programmed to execute based on a pre-defined triggering event. Following the logic bomb test, the UN passed a resolution banning sales of certain computer hardware to North Korea.¹⁶⁵

North Korea considers its cyber warfare capabilities an important asymmetric asset in the face of its perceived enemies, the U.S. and South Korea. While North Korea does not have an immersive digital culture, both the U.S. and South Korea are heavily dependent upon technological infrastructure for social, economic, and political stability.¹⁶⁶ For this reason, a cyber attack that cripples or compromises the reliability of the U.S. or South Korea's technological infrastructure could have a far-reaching impact.

Gaming for profit and pwnage

North Korea has reportedly used computer games for both illegal capital gain and orchestrating cyber attacks. In 2011, South Korean police arrested five individuals, including one Chinese national, for allegedly collaborating with North Korean hackers affiliated with the Korea Computer Center to steal money via online games.¹⁶⁷

North Korea has used computer games for both illegal capital gain and orchestrating cyber attacks.

According to South Korean reports, the culprits used an auto-player to quickly progress in the massively multiplayer online role-playing game (MMORPG) "Lineage" and were able to use the game's market to obtain real currency.¹⁶⁸ In 2013, South Korean officials released information stating they had found evidence that North Korea was using games as a medium for infecting machines and launching cyber attacks. North Korea had used game downloads to infect 100,000 South Korean machines for a botnet used to launch a distributed denial of service (DDoS) attack against Incheon Airport.¹⁶⁹ This clever tactic sought to leverage a seemingly innocent game as a force multiplier in order to amplify the effects of a DDoS attack on a critical infrastructure target. However, in this case, there was little impact on the target.

Intelligence and counterintelligence

North Korea's intelligence program is one of its strongest military assets, providing foundational support for all other military operations. The regime's cyber warfare capabilities, in particular, rely heavily on open-source intelligence (OSINT) collection and cyber-espionage.¹⁷⁰ As noted in a CIA publication, "It is a significant irony of our information age that open-source intelligence is contributing to the survival and development of one of the world's most secretive regimes."¹⁷¹ Historically, the primary goals of the regime's intelligence program included collection and dissemination of intelligence concerning any possible political, military, or economic threat to the regime's security and stability. Secondary goals have included "acquisition of foreign military and civilian technologies and equipment, support of the DPRK's foreign policy goals, training and

¹⁶⁵ <http://www.scribd.com/doc/15078953/Cyber-Threat-Posed-by-North-Korea-and-China-to-South-Korea-and-US-Forces-Korea>

¹⁶⁶ <http://www.apcss.org/Publications/Edited%20Volumes/BytesAndBullets/CH2.pdf>

¹⁶⁷ <http://www.theguardian.com/technology/2011/aug/04/south-north-korean-hackers-china>

¹⁶⁸ http://english.chosun.com/site/data/html_dir/2011/05/06/2011050600827.html

¹⁶⁹ <http://www.zdnet.com/blog/security/north-korea-ships-malware-infected-games-to-south-korean-users-uses-them-to-launch-ddos-attacks/12383>

¹⁷⁰ <http://docs.house.gov/meetings/AS/AS00/20140402/101985/HHRG-113-AS00-Wstate-ScaparrottiUSAC-20140402.pdf>

¹⁷¹ <https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/csi-studies/studies/vol48no1/article04.html>

support for foreign revolutionary and terrorist organizations, and the acquisition of foreign capital for state and intelligence operations."¹⁷²

North Korea has a broad reach for intelligence collection, which extends to cyber intelligence.¹⁷³ In April 2013, Solutionary, a company providing managed security services, reported a marked increase in both overt attacks and information gathering attempts originating from North Korean IPs. Solutionary refers to any overt external attacks on company networks or attempts to steal data as "touches." They reportedly recorded 12,473 of these touches in February 2013, 11,000 of which were directed at a single financial institution. As a baseline, Solutionary noted that typically only 200 incidents per month are traced to North Korean origin.¹⁷⁴ This is an interesting claim, considering that attacks attributed to North Korea are usually routed through other countries.

A faction of ethnic North Koreans residing in Japan, known as the Chongryon, are critical to North Korea's cyber and intelligence programs.

As mentioned above, a faction of ethnic North Koreans residing in Japan, known as the Chongryon, are critical to North Korea's cyber and intelligence programs and help generate hard currency for the regime. The Chongryon headquarters has been recognized as the de facto North Korean embassy in Japan. In 2012, the organization's headquarters was seized to pay for the group's past due debts.¹⁷⁵



Chongryon Headquarters in Tokyo | Picture: Wikipedia

Figure 15 Headquarters of the Chongryon.¹⁷⁶

¹⁷² <http://www.apcss.org/Publications/Edited%20Volumes/BytesAndBullets/CH13.pdf>

¹⁷³ <http://docs.house.gov/meetings/AS/AS00/20140402/101985/HHRG-113-AS00-Wstate-ScaparrottiUSAC-20140402.pdf>

¹⁷⁴ <http://www.usatoday.com/story/tech/2013/04/26/cyberspying-from-north-korean-ip-addresses-spike/2115349/>

¹⁷⁵ http://sundaytimes.lk/?option=com_content&view=article&id=21034:japan-court-approves-seizure-of-nkorea-embassy-media&catid=81:news&Itemid=625

¹⁷⁶ <http://www.nknews.org/2014/02/chongryon-still-pyongyangs-pawn-in-covert-operations-former-intelligence-officer/>

It was then purchased by a monk named Ekan Ikeguchi, who let the Chongryon continue to use the building in what he referred to as a “goodwill gesture”. Ikeguchi is one of the Chongryon’s many ties to organized crime. Ikeguchi was arrested in the past for an attempted coup against the Japanese government. He also has ties to the political group Nihon Seinensya, which is involved in illegal activities in conjunction with the yakuza syndicate Sumiyoshi-kai, which imports and sells amphetamines made in North Korea.¹⁷⁷ North Korea also has black market ties to Sumiyoshi-kai’s rival syndicate, Yamaguchi-gumi. Many members of the Kodo-kai, Yamaguchi-gumi’s ruling faction, are Korean-Japanese, with ties to North Korea.¹⁷⁸ Masahiro Namikawa, leader of the drug trafficking Seido-kai yakuza organization, also has ties to the Chongryon.¹⁷⁹

The Chongryon operate at least two websites, chongryon.com, which is in Japanese, and korea-np.co.jp.

WHOIS records for chongryon.com indicate that it was registered by “guanin o” using the email address park2@mac.com. The WHOIS information for korea-np.co.jp. shows that it was registered by Choson Shinbo Company Inc. The WHOIS records for these sites can be found in [Appendix A](#).

Additionally, the Chongryon operate a ferry called the *Mangyongbong-92*, the only direct transit from Japan to North Korea. In 2003, they were suspected of using the ferry to smuggle missile parts.¹⁸⁰ In 2006, the ferry was temporarily banned from Japanese waters when Japanese officials discovered the Chongryon were using it to smuggle dual-use electronics to North Korea to be used for military purposes.¹⁸¹

North Korea has a global network of state-run businesses located in 30 to 40 countries that is used for espionage activities. The Reconnaissance General Bureau is responsible for oversight of this network.¹⁸² The businesses include cafes and other non-suspect establishments. The highest concentration of these is in China. Members of this espionage network reportedly “send more than \$100 million in cash per year to the regime and provide cover for spies.”¹⁸³ These establishments are also used for money laundering and drug trafficking.¹⁸⁴

North Korea has a global network of state-run businesses located in 30 to 40 countries that is used for espionage activities. These establishments are also used for money laundering and drug trafficking.

The regime is also known to kidnap foreign citizens and use them as instruments for intelligence. Prisoners are first tortured and psychologically conditioned to bend to the regime’s will. They are then used based on their skillset. This may include teaching their language to North Koreans, spreading propaganda in their native language, providing translation services,

¹⁷⁷ <http://japandailynews.com/religious-group-that-bought-north-korean-embassy-building-has-mob-ties-0826568/>

¹⁷⁸ <http://culturmag.de/crimemag/jake-adelstein-the-yakuza-2/20212>

¹⁷⁹ <http://www.thedailybeast.com/articles/2013/06/25/the-great-japanese-gang-wars.html>

¹⁸⁰ <http://news.bbc.co.uk/2/hi/asia-pacific/2958968.stm>

¹⁸¹ <http://www.washingtontimes.com/news/2006/oct/16/20061016-122859-4745r/>

¹⁸² <http://www.ibtimes.com/north-koreas-international-network-restaurants-used-gain-hard-currency-espionage-1427242>

¹⁸³ http://www.outsideonline.com/outdoor-adventure/politics/Did-North-Korea-Kidnap-This-American-Hiker.html?utm_content=buffer6bd46&utm_medium=social&utm_source=twitter.com&utm_campaign=buffer

¹⁸⁴ <http://freebeacon.com/national-security/north-koreas-overseas-restaurants-used-for-espionage-and-gaining-hard-currency/>

conducting military training, or other skills the regime deems useful.¹⁸⁵ In July 2014, Japanese officials agreed to lift some sanctions on North Korea when the regime agreed to investigate the whereabouts of Japanese citizens who were allegedly abducted by North Korean agents decades ago. Sanctions to be lifted include the ban on port calls to Japan by North Korean ships.¹⁸⁶

North Korea has also infiltrated important positions in South Korea for both intelligence and psychological operations purposes.¹⁸⁷ In 2011, South Korea's National Intelligence Service reportedly discovered the presence of Communist spies. These spies within their trusted circles had been reporting back to North Korea for almost 10 years. The embedded spies included a Democratic Party representative. According to the agency, the spies were on a mission to infiltrate and influence the Democratic Party and to gather military intelligence.¹⁸⁸ The regime also attempts to infiltrate organizations made up of North Koreans who seek shelter in South Korea, in order to gain intelligence. In the past several years, South Korea has arrested at least 14 defectors who were found to be spies.¹⁸⁹

These intelligence collection and counterintelligence capabilities are an attempt to provide the regime with a strategic asymmetrical advantage. The regime leverages its human and cyber resources around the globe to provide an influx of intelligence, while very little credible intelligence about the regime's activities and capabilities ever becomes available to the outside world.

Psychological operations

North Korea continues to be a master of propaganda and deception and leverages the cyber realm for psychological operations. Modern North Korean psychological operations tactics include distribution of propaganda via traditional media outlets, websites, and social media. Many of these psychological operations campaigns are politically focused.¹⁹⁰ According to Dr. Andrei Lankov, the North Korean government has "very rational and highly successful manipulators who usually get what they want by outsmarting everybody else in the process."¹⁹¹

The regime's Unit 204 is responsible for cyber-psychological operations. These operations are PSYOP tailored for the cyber arena. In order to be successful, cyber-psychological campaigns require speed, precision, and creativity. These campaigns leverage the phenomenon of viral, unverified news stories that tend to rapidly propagate via social media, mobile text messaging, and other electronic communications. This phenomenon creates an arena for strategic propagation of both fact and fiction for the purposes of sentiment manipulation. Such messages may be used for

Such messages can be used for recruitment, cyber mobilization, and to instill fear in a target population.

¹⁸⁵ http://www.outsideonline.com/outdoor-adventure/politics/Did-North-Korea-Kidnap-This-American-Hiker.html?utm_content=buffer6bd46&utm_medium=social&utm_source=twitter.com&utm_campaign=buffer

¹⁸⁶ <http://m.us.wsj.com/articles/tokyo-to-lift-some-sanctions-on-pyongyang-1404354699?mobile=y>

¹⁸⁷ <http://www.nytimes.com/2013/10/02/world/asia/northern-spy-lifts-cloak-on-koreas-deadly-rivalry.html?pagewanted=2>

¹⁸⁸ http://www.kccoc.org/home/?mid=eng_kccoc_info_korea&document_srl=3223&sort_index=readed_count&order_type=desc

¹⁸⁹ http://www.washingtonpost.com/world/prominent-n-korean-defector-acquitted-of-espionage-by-s-korean-court/2013/08/22/642b3712-0b19-11e3-89fe-abb4a5067014_story.html

¹⁹⁰ <https://www.usnwc.edu/getattachment/8e487165-a3ef-4ebc-83ce-0ddd7898e16a/The-Republic-of-Korea-s-Counter-asymmetric-Strateg>

¹⁹¹ http://www.reddit.com/r/NorthKoreaNews/comments/296ryd/i_am_dr_andrei_lankov_i_studied_in_north_korea/

recruitment, cyber mobilization, and to instill fear in a target population. Cyber-psychological operations may also include mental suggestion using technology as a delivery mechanism for subliminal cues. It is unknown whether North Korea possesses this capability.¹⁹²

North Korean citizens have access to state-approved social networks on the Kwangmyong.¹⁹³

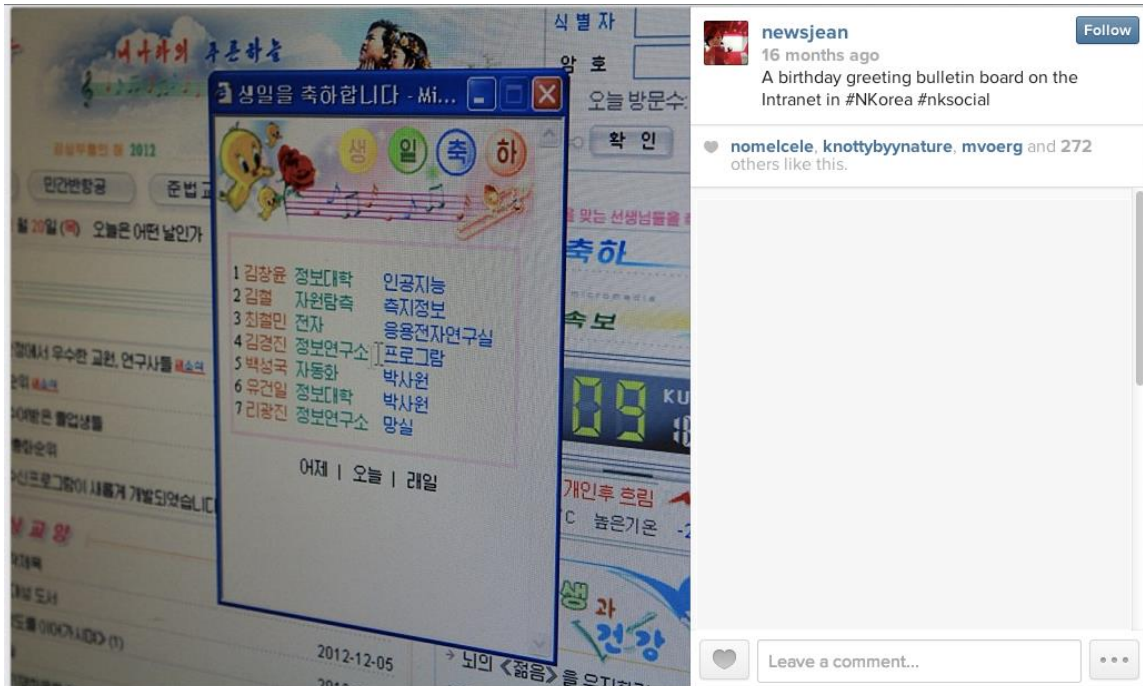


Figure 16 A photo posted by Jean Lee on Instagram shows one of the social networking sites on the Kwangmyong.¹⁹⁴

The regime has a limited overt social media presence on the Internet. Some of the known social media platforms employed by the regime include Twitter, Facebook, and YouTube. The YouTube channel North Korea Today, operated by user rodrigorajo1, features news clips from North Korea. It is unclear whether this channel is officially sanctioned.¹⁹⁵ The North Korea Today YouTube channel also has corresponding profiles on Twitter¹⁹⁶ and Facebook.¹⁹⁷

¹⁹² <http://fmso.leavenworth.army.mil/documents/new-psyop.pdf>

¹⁹³ <http://www.austinchronicle.com/daily/sxsw/2013-03-11/social-media-in-north-korea/>

¹⁹⁴ <http://instagram.com/p/WpJc10Ckb/>

¹⁹⁵ <https://www.youtube.com/user/rodrigorajo1>

¹⁹⁶ <https://twitter.com/NorthKoreaToday>

¹⁹⁷ <https://www.facebook.com/pages/Korean-Central-Television/380193555435568?fref=ts>

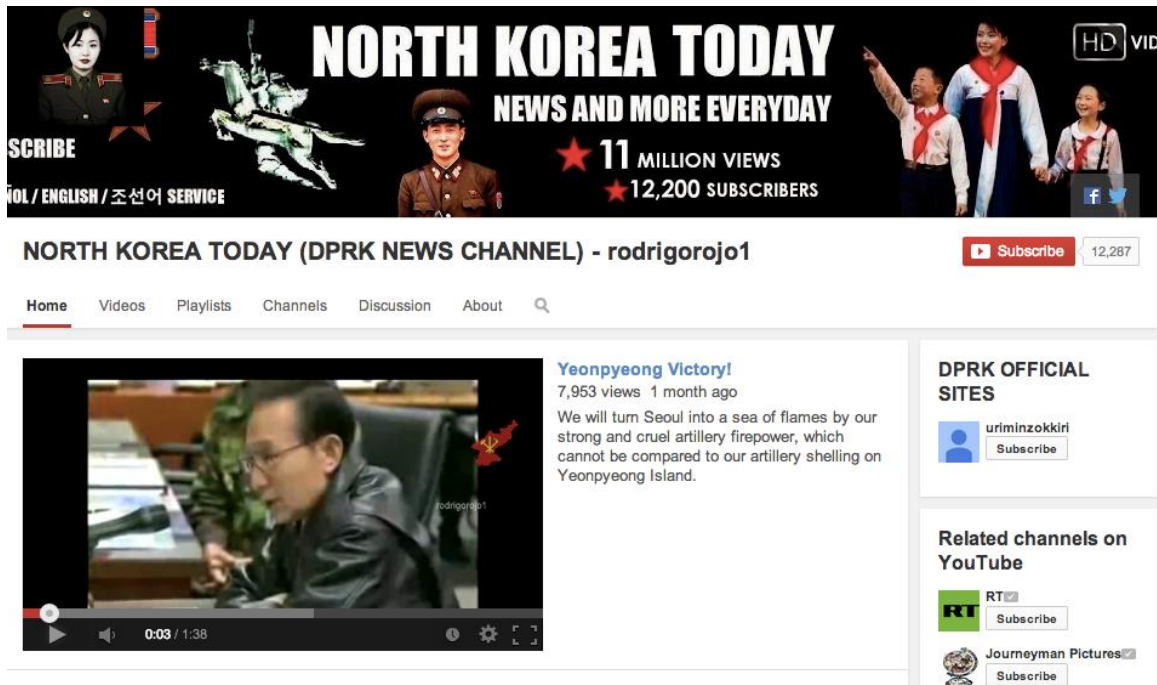


Figure 17 A screenshot of the North Korea Today YouTube Channel.¹⁹⁸

The Uriminzokkiri website, known for pushing *juche* ideology and anti-American and anti-South Korean messages, has accompanying social media profiles on YouTube,¹⁹⁹ Google+,²⁰⁰ and Facebook.²⁰¹ It also has Twitter profiles in both Korean²⁰² and English.²⁰³

¹⁹⁸ <https://www.youtube.com/user/rodrigojo1>

¹⁹⁹ <https://www.youtube.com/user/uriminzokkiri>

²⁰⁰ <https://plus.google.com/u/0/112306344682887627095>

²⁰¹ <https://www.facebook.com/pages/Uriminzokkiri/124452740935216>

²⁰² <https://twitter.com/uriminzok>

²⁰³ https://twitter.com/uriminzok_engl

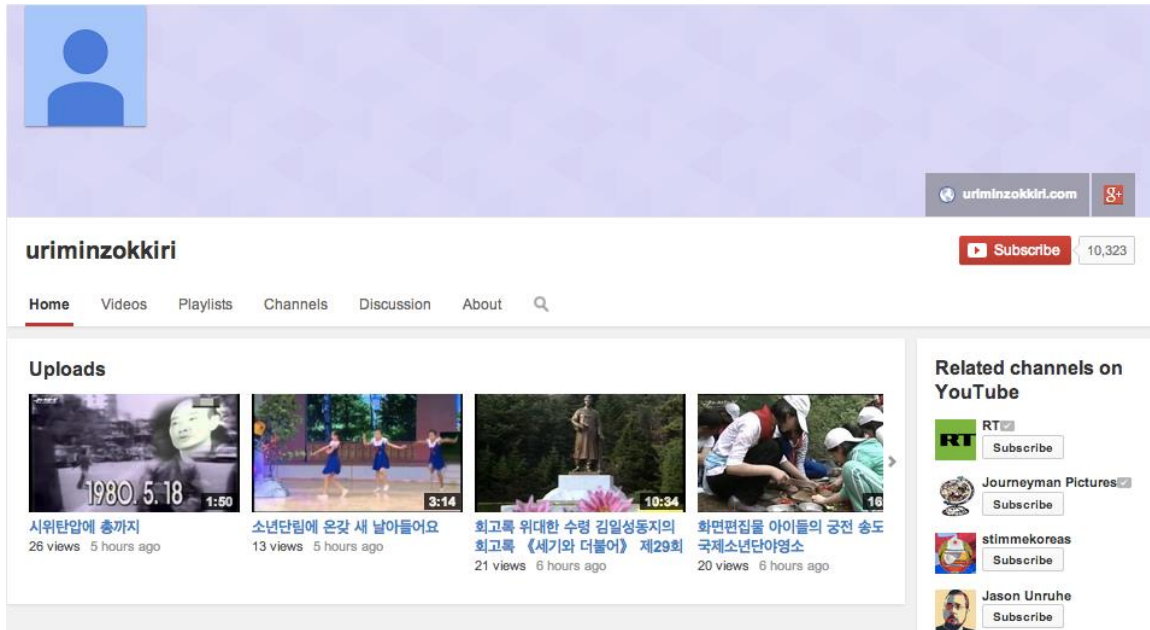


Figure 18 A screenshot of the Uriminzokkiri YouTube channel.²⁰⁴

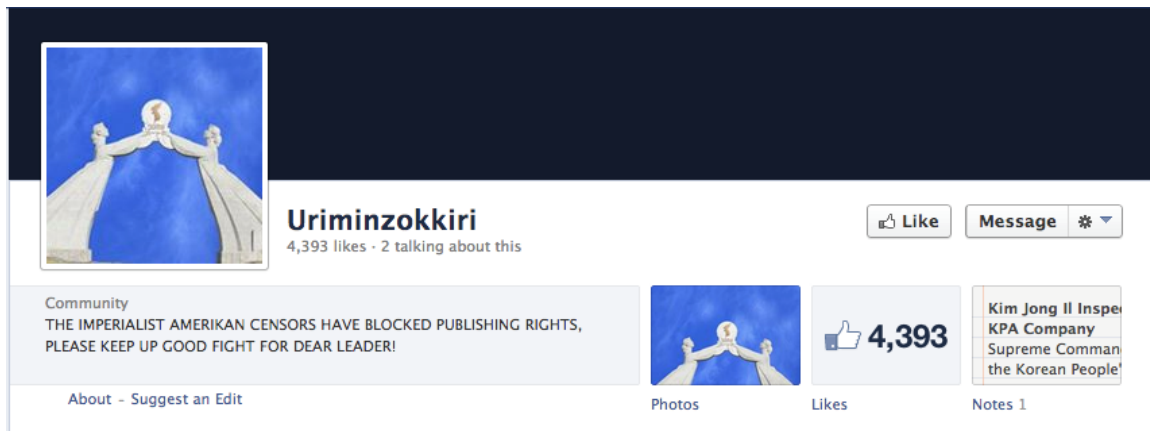


Figure 19 A screenshot from the Uriminzokkiri Facebook page shows anti-U.S. and pro-*juche* rhetoric.²⁰⁵

²⁰⁴ <https://www.youtube.com/user/uriminzokkiri/featured>

²⁰⁵ <https://www.facebook.com/pages/Uriminzokkiri/124452740935216>

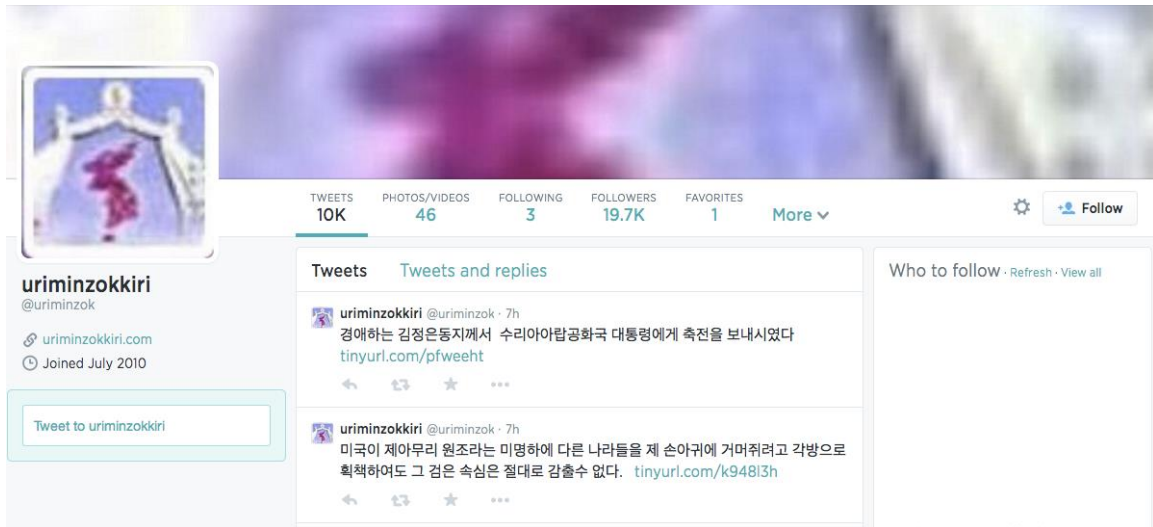


Figure 20 A screenshot of the Uriminzokkiri Korean language Twitter profile.²⁰⁶



Figure 21 A screenshot of the Uriminzokkiri English language Twitter profile.²⁰⁷

North Korean propaganda²⁰⁸ is used for several purposes: to enforce the ideals of allies and sympathizers, to frame North Korea in a favorable light to outsiders, to sensationalize the regime’s perceived self-reliance and military prowess, and to shield its own citizens from the outside world.²⁰⁹ *Juche* ideology and indoctrination of the regime’s youth ensure support of the local population. North Koreans accept military duty as an honor and strive to excel in their service to the regime. In the spirit of *juche*, the regime uses disinformation to “hide lapses or tout accomplishments that may have never been

In the spirit of *juche*, the regime uses disinformation to “hide lapses or tout accomplishments that may have never been achieved.”

²⁰⁶ <https://www.facebook.com/pages/Uriminzokkiri/124452740935216>

²⁰⁷ https://twitter.com/uriminzok_engl

²⁰⁸ http://www.ncix.gov/publications/archives/docs/NORTH_KOREA_AND_FOREIGN_IT.pdf

²⁰⁹ <http://fas.org/irp/eprint/cno-dprk.pdf>

achieved.”²¹⁰ Limiting citizen access to the outside world by instituting the Kwangmyong intranet, North Korea ensures its citizens are not exposed to outside information that is counterproductive to citizen indoctrination or in conflict with *juche* ideals. North Korea portrays the West, particularly the United States, as an enemy. The regime uses this strategy of shifting the population’s negative sentiments toward an external entity to keep its citizens ignorant of North Korea’s own economic hardship, regime brutality, and systemic incompetence.²¹¹ For example, prior to Kim Jong Il’s death in 2011, North Korean media altered photos of their “Dear Leader” to make him appear younger and healthier than he really was. This became obvious when the altered photos were compared to those taken by Western media around the same time.²¹²

According to Dr. Andrei Lankov, “North Koreans now have a much better understanding of what is going on in the outside than they did before. This is largely thanks to the spread of DVDs and video content in the country, but also because some of them have been to China and talk about what they have seen...many [of] them sincerely believe that the United States remains ready to attack at any moment and that Japan is an incurably aggressive place...nearly all of them swallow the official propaganda myths about the Korean War being started by the 'American Imperialists' who invaded them. Hence, they see the outside world as an inherently dangerous place.”²¹³ Some human rights groups seek to reach out to North Korean citizens and break them from this isolation. In August 2014, the New York-based charity Human Rights Foundation sponsored a hackathon in San Francisco called “Hack North Korea” to find new ways to get information in, out, and around North Korea. The event brought together many programmers, human rights campaigners, and defectors.²¹⁴

North Korea even uses “trolling” as a PSYOP tactic. On the Internet, “trolls” are users who post messages that are often crass, controversial, inflammatory, or offensive, in order to evoke a strong reaction or influence a reader’s opinion. Often, the motivation for trolling is simply for the troll’s enjoyment. The rude and offensive trolling tactics are in stark contrast to traditional forms of persuasive rhetoric. However, North Korea reportedly utilizes over 200 military intelligence operatives to troll South Korean message boards and social media pages with pro-North Korean sentiments.²¹⁵ Matt Rhoades, director of the cyberspace and security program at the Truman National Security Project, said, “North Korea’s cyber-development is almost just a new harassment mechanism for them, a low-cost, asymmetric method to harass its neighbor in the south...”²¹⁶

Leveraging the cyber and intelligence resources noted above, North Korea’s psychological operations serve an important strategic role. The ability to influence outsiders, while effectively isolating its own population from most outside influence, allows North Korea to remain an enigma. Additionally, in line with its PSYOP tactics, North Korea may strategically take credit for cyber attacks that were, in reality, launched by another entity. Whether the targeted entity blames

²¹⁰ <http://www.ists.dartmouth.edu/docs/cyberwarfare.pdf>

²¹¹ <http://docs.house.gov/meetings/AS/AS00/20140402/101985/HHRG-113-AS00-Wstate-ScaparrottiUSAC-20140402.pdf>

²¹² <https://www.strategypage.com/htmww/htmww/articles/20131106.aspx>

²¹³ http://www.reddit.com/r/NorthKoreaNews/comments/296ryd/i_am_dr_andrei_lankov_i_studied_in_north_korea/

²¹⁴ <http://www.northkoreatech.org/2014/08/05/hack-north-korea-focuses-silicon-valley-on-information-flow/>

²¹⁵ <http://www.strategypage.com/htmww/htiw/articles/20131213.aspx>

²¹⁶ [http://www.csmonitor.com/World/Security-Watch/2013/1019/In-cyberarms-race-North-Korea-emerging-as-a-power-not-a-pushover/\(page\)/4](http://www.csmonitor.com/World/Security-Watch/2013/1019/In-cyberarms-race-North-Korea-emerging-as-a-power-not-a-pushover/(page)/4)

North Korea for the attacks, or the regime simply takes credit for an attack that has not yet been attributed, several PSYOP goals can come into play. First, to claim credit for an attack amplifies the impact of a show of force, particularly if South Korea is the target. This tactic can be used to stir sentiments in order to provoke a reaction. Second, North Korea may lay claim to responsibility for an attack that exceeds its capabilities in order to seem more technologically advanced and more capable. Third, any success, or the appearance thereof, enforces the *juche* ideal of regime self-sufficiency. Finally, North Korea may act as a scapegoat and claim credit for a cyber attack of an ally such as China so the attack is not attributed to the real actors.²¹⁷

Electronic warfare

North Korea reportedly has the electronic warfare capabilities to jam GPS and to inject false GPS coordinates.²¹⁸ North Korea demonstrated these capabilities in March 2011 by jamming South Korea's GPS signals during a joint U.S.-South Korea military exercise.²¹⁹ North Korea has the capability to create an EMP.²²⁰ An EMP is a sudden, extreme outburst of atmospheric electricity creating an intense magnetic field that can burn out electrical equipment.²²¹ A report from the U.S. Department of Homeland Security (DHS) noted North Korea's ability to deliver a nuclear warhead as a satellite over the South Pole, effectively creating the burst needed to deliver an EMP targeting the United States. An EMP could effectively disrupt electronic communications including critical infrastructure components such as telecommunications, financial institutions, the energy sector, transportation, food and water delivery, emergency services, and space systems.²²² North Korea reportedly acquired its EMP technology from Russia.²²³

North Korea also has a drone program. The regime reportedly acquired its first drones in the late 1980's or early 1990's. The regime's drones are complimentary to its intelligence program and are primarily used for surveillance.²²⁴ In early 2014 a North Korean drone crashed south of the 38th parallel, the line dividing North Korea from the south.²²⁵ While early reports noted that the drones appeared similar to those manufactured by Chinese company Taoyuan Navigation Friend Aviation Technology, the company denied involvement.²²⁶

²¹⁷ <http://fas.org/irp/doddir/army/fm3-05-301.pdf>

²¹⁸ <https://www.usnwc.edu/getattachment/8e487165-a3ef-4ebc-83ce-0ddd7898e16a/The-Republic-of-Korea-s-Counter-asymmetric-Strateg>

²¹⁹ <http://www.reuters.com/article/2011/05/03/us-korea-north-cyber-idUSTRE7421Q520110503>

²²⁰ <http://defensetech.org/2007/12/24/inside-dprks-unit-121/>

²²¹ http://usatoday30.usatoday.com/tech/science/2010-10-26-emp_N.htm

²²² <http://www.wnd.com/2014/04/dhs-study-north-korea-capable-of-emp-attack-on-u-s/>

²²³ <http://www.extremetech.com/extreme/170563-north-korea-emp>

²²⁴ http://38north.org/2014/07/jbermudez070114/?utm_source=feedly&utm_reader=feedly&utm_medium=rss&utm_campaign=jbermudez070114

²²⁵ <http://www.popsoci.com/blog-network/eastern-arsenal/north-koreas-new-drones-are-chinese-which-opens-new-mystery>

²²⁶ <http://www.scmp.com/news/china-insider/article/1494207/north-korean-drones-not-theirs-says-chinese-retailer>



The underside of the drone found in Paju, with a hole that appears to allow photos to be taken of the ground area.
— South Korea's Ministry of Defense

Figure 22 A drone attributed to North Korea.²²⁷

Stressing the importance of the regime's electronic warfare capabilities, in 1999 former regime leader Kim Jong Il said "The basic key to victory in modern warfare is to do well in electronic warfare."²²⁸ Since the regime's advanced technology lags behind that of South Korea and the U.S., its capability to disrupt the communications of these perceived adversaries is a vital asymmetric capability.²²⁹

Training cyber warriors

North Korea utilizes primary and secondary education and the university system to train its cyber warfare operators. According to reports by defectors, the regime seeks out children who show mathematical talent and sends them through rigorous advanced training.²³⁰ A vintage North Korean animation stresses the importance of mathematics in North Korean education. The short film follows a young boy as he does his geometry homework. The frustrated boy begins to daydream then has visions of going to war with the U.S. and needing geometry to effectively calculate missile trajectory during the battle.²³¹

²²⁷ <http://blogs.wsj.com/korearealtime/2014/04/02/seoul-points-to-north-korea-in-crashed-drones-investigation/>

²²⁸ <http://www.apcss.org/Publications/Edited%20Volumes/BytesAndBullets/CH13.pdf>

²²⁹ <http://www.apcss.org/Publications/Edited%20Volumes/BytesAndBullets/CH5.pdf>

²³⁰ <http://www.aljazeera.com/indepth/features/2011/06/201162081543573839.html>

²³¹ <http://theweek.com/article/index/255243/how-to-kill-americans-with-geometry-a-north-korean-propaganda-film-for-kids>



North Korea Animation DPRK anti USA Imperialism Invasion

Figure 23 A screenshot from the North Korean animation depicting geometry as a necessary skill for battle.²³²

Science and technology students are expected to learn foreign languages, which may include Chinese, Japanese, and English.²³³ Student emails, chats, and web browsing activities are heavily monitored.²³⁴ Around age twelve or thirteen, chosen students are enrolled in accelerated computer courses at First and Second Geumseong Senior-Middle Schools.

²³² <https://www.youtube.com/watch?v=ujtp-70zQME>

²³³ <https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/csi-studies/studies/vol48no1/article04.html>

²³⁴ http://www.thestar.com/news/world/2014/02/23/north_korea_where_the_internet_has_just_5500_sites.html#



Figure 24 North Korean students training for cyber war.²³⁵

The successful students are then sent to Kim Il-sung University, Kim Chaek University of Technology,²³⁶ or the Command Automation University, traditionally known as Mirim University.

Kim Il-sung University's computer center was started in 1985. Its computer courses have a heavy programming element. The university reportedly developed the Intelligent Locker hard disc protection program, Worluf Antivirus, SIMNA (simulation and system analysis program), a war games program, a hepatitis diagnosis and prescription system, and a C++ program development tool called FC 2.0.²³⁷ Kim Il-sung University also has programs focusing on nuclear research.²³⁸

Kim Chaek University of Technology was established in 1948. In the late 1990s, it began to restructure its computer-focused courses to reflect more modern technologies. As of 2002, the university had three colleges focusing on computer science, information science and technology, and machine science. Software developed by the university includes Computer Fax and SGVision, an image-reprocessing program used for steganography.²³⁹ Students and instructors must submit a formal request for permission in order to use the Internet for research.²⁴⁰

²³⁵ <http://www.courierpress.com/news/2013/apr/19/young-north-koreans-train-seek-revenge-us/>

²³⁶ <http://www.aljazeera.com/indepth/features/2011/06/201162081543573839.html>

²³⁷ <http://www.ists.dartmouth.edu/docs/cyberwarfare.pdf>

²³⁸ <http://www.nti.org/facilities/789/>

²³⁹ <http://www.ists.dartmouth.edu/docs/cyberwarfare.pdf>

²⁴⁰ <http://www.theguardian.com/world/2013/jan/08/north-korean-google-chief-search>

The Command Automation University periodically chooses around 100 students for an intensive five-year course prior to their assignment to serve in cyber intelligence and cyber warfare capacities.²⁴¹ Programs at the Command Automation University include command automation, computers, programming, automated reconnaissance, and electronic warfare.²⁴² Other students attend a two-year accelerated university program, then study abroad in Russia or China before they are assigned to a cyber-operator role.²⁴³

The elite cyber operators are given special incentives. For example, parents of students graduating from the cyber program with top scores are given the opportunity to live in Pyongyang; and married cyber operators are given housing, a food allowance, and a stipend if operating overseas. Due to the nature of their profession, these cyber elite are some of the only North Koreans allowed to access the outside Internet.²⁴⁴

Important political and military ties

While this report focuses on North Korea's cyber warfare capabilities, these capabilities cannot be fully separated from the implications of partnerships with countries known to deal in illegal weapons trade with the regime. Now that cyberspace has become a legitimate arena for warfare, these nations are also potential allies in the cyber realm. For this reason, the regime's key political and military relationships are explored below.

China

North Korea has a longstanding historical relationship with China. During the Korean War (1950-1953), China allied with North Korea's Communist forces. China has also provided ongoing political and economic support to the regime's leadership and is a primary trade partner. North Korea is economically dependent on China. North Korea gets an estimated 90 percent of its energy imports, 80 percent of its consumer goods, and 45 percent of its food supply from China. This relationship is prudent – in the event of a military conflict, China can strategically use North Korea as a buffer zone between itself and South Korea, where many U.S. military personnel are stationed. Chinese aid to North Korea also deters the likelihood that the regime will collapse, resulting in internal destabilization that could catalyze a U.S.-China conflict.²⁴⁵

North Korea relies heavily on China for technological resources. As noted above, North Korea relies on China's Unicom for Internet access.²⁴⁶ Additionally, the regime sends some of its cyber warriors to train in China²⁴⁷ and stations a portion of its Unit 121 personnel in Shenyang.²⁴⁸ Some of North Korea's official websites are hosted in China,²⁴⁹ and KCC has a branch office there.²⁵⁰

²⁴¹ <https://www.usnwc.edu/getattachment/8e487165-a3ef-4ebc-83ce-0ddd7898e16a/The-Republic-of-Korea-s-Counter-asymmetric-Strateg>

²⁴² <http://www.ists.dartmouth.edu/docs/cyberwarfare.pdf>

²⁴³ <http://www.aljazeera.com/indepth/features/2011/06/201162081543573839.html>

²⁴⁴ <http://www.aljazeera.com/indepth/features/2011/06/201162081543573839.html>

²⁴⁵ <http://www.cfr.org/china/china-north-korea-relationship/p11097#p1>

²⁴⁶ <https://rdns.im/the-pirate-bay-north-korean-hosting-no-its-fake-p2>

²⁴⁷ <http://www.aljazeera.com/indepth/features/2011/06/201162081543573839.html>

²⁴⁸ [http://www.csmonitor.com/World/Security-Watch/2013/1019/In-cyberarms-race-North-Korea-emerging-as-a-power-not-a-pushover/\(page\)/4](http://www.csmonitor.com/World/Security-Watch/2013/1019/In-cyberarms-race-North-Korea-emerging-as-a-power-not-a-pushover/(page)/4)

²⁴⁹ <http://binarycore.org/2012/05/30/investigating-north-koreas-netblock-part-3-topology/>

²⁵⁰ <http://www.naenara.com.kp/en/kcc/>

North Korea also relies on China to provide much of its network hardware, including servers and routers.²⁵¹

Russia

North Korea has a long history of ties to Russia. The former Soviet Union was the major sponsor of the North Korean state and a major trading partner. Following the dissolution of the Soviet Union, aid to North Korea was halted and trade diminished significantly. This chain of events contributed to North Korea's eventual economic collapse, as it could not survive without aid.²⁵²

North Korea currently has a collaborative relationship with Russia in the cyber realm. The regime's CSTIA relies on Russia as one of several sources for technical data.²⁵³ North Korea also sends some of its cyber warriors to train in Russia,²⁵⁴ and the regime reportedly acquired its EMP technology from there.²⁵⁵

Political ties between Russia and North Korea have become stronger in recent months. In 2014, potentially as a result of the U.S. response to the Russian-Ukrainian conflict, Russia began to strengthen ties with North Korea. Negotiations reportedly included promises of trade and development projects. Narushige Michishita, a North Korea and Asia security expert at Japan's National Graduate Institute for Policy Studies, stated "By strengthening its relationship with North Korea, Russia is trying to enhance its bargaining position vis-à-vis the United States and Japan."²⁵⁶ Russia also recently forgave most of the regime's debts.²⁵⁷

Iran

North Korea and Iran have longstanding political and military ties. North Korea supplied Iran with conventional arms during the Iran-Iraq War. Iran and North Korea reportedly collaborate closely in ballistic missile development efforts. In the past, Iran provided the North Korean regime with necessary funds and oil in exchange for missile parts and technology.^{258 259} In 2009, a North Korean plane transporting 35 tons of weapons and allegedly bound for Iran was seized after making an unscheduled stop in Bangkok, Thailand. That same year, United Arab Emirates seized a ship bound for Iran that was transporting several containers of North Korean weapons, including rocket-propelled grenades and ammunition. Reportedly, the customer was a company affiliated with Iran's Islamic Revolutionary Guard Corps.^{260 261}

North Korea also has cyberwar ties with Iran. In 2012, North Korea and Iran signed a technology treaty to help combat "common enemies" in cyberspace. The treaty included provisions for cooperation in research, student exchanges, and joint laboratories. Joint projects reportedly

²⁵¹ [http://www.csmonitor.com/World/Security-Watch/2013/1019/In-cyberarms-race-North-Korea-emerging-as-a-power-not-a-pushover/\(page\)/4](http://www.csmonitor.com/World/Security-Watch/2013/1019/In-cyberarms-race-North-Korea-emerging-as-a-power-not-a-pushover/(page)/4)

²⁵² <http://www.aljazeera.com/indepth/opinion/2014/06/n-korea-russia-step-toward-worl-201462253320470677.html>

²⁵³ <https://www.cia.gov/library/center-for-the-study-of-intelligence/kent-csi/vol48no1/pdf/v48i1a04p.pdf>

²⁵⁴ <http://www.aljazeera.com/indepth/features/2011/06/201162081543573839.html>

²⁵⁵ <http://www.extremetech.com/extreme/170563-north-korea-emp>

²⁵⁶ <http://www.theguardian.com/world/2014/jun/04/russia-bolster-ties-north-korea>

²⁵⁷ <http://www.voanews.com/content/russia-forgives-north-korean-debt/1939188.html>

²⁵⁸ <http://thediplomat.com/2013/10/the-iran-secret-explaining-north-koreas-rocket-success/2/>

²⁵⁹ <http://humanities.tau.ac.il/iranian/en/previous-reviews/10-iran-pulse-en/117-10>

²⁶⁰ <http://www.armscontrol.org/factsheets/dprkchron>

²⁶¹ <http://www.irantracker.org/foreign-relations/north-korea-iran-foreign-relations>

include IT information sharing, engineering, biotechnology, renewable energy, and sustainability. F-Secure's Mikko Hypponen stated, "It's highly likely that one of the reasons for this co-operation is for them to work together regarding their cyber defence and cyber offense strategies". Hypponen cited Flame malware as a possible triggering event for the creation of this treaty. Others also suspect that Iran and North Korea's mutual interest in development of nuclear weapons and the need to protect refineries against malware such as Stuxnet were driving factors in the establishment of the treaty.²⁶² U.S. House Foreign Affairs Committee leaders assert that the treaty indicates North Korea and Iran are collaborating on a joint nuclear weapons program.²⁶³

Additionally, North Korea, in conjunction with Iran and Syria, reportedly supports both Hamas and Hezbollah in procuring kinetic weaponry and communications equipment and in establishing operational infrastructure.^{264 265 266}

Syria

North Korea has both a cyber relationship and kinetic weapons ties with Syria. KCC reportedly has a branch in Syria.²⁶⁷

In 2007, Israel launched an airstrike, destroying a Syrian target that was allegedly a nuclear facility under construction with North Korea's assistance. U.S. officials noted the facility was modeled on the North Korean nuclear reactor at Yongbyon.²⁶⁸

The North Korea-Syria relationship becomes more important in the context of both countries' ties with Iran. As noted above, Iran, North Korea, and Syria jointly provide support to extremist groups Hamas and Hezbollah.^{269 270 271} Additionally, as we explored in [HPSR Security Briefing Episode 11](#), Iran and Syria's military alliances extend to joint SIGINT and cyber operations.²⁷²

Cuba

North Korea also has an interesting relationship with Cuba – one that includes supplying weapons and apparent attempts to illegally smuggle weapons. In 2013, a North Korean cargo ship on its return voyage was stopped near the Panama Canal. The ship was carrying surface-to-air missile parts, disguised as containers of sugar. In an attempt to save face, Cuba's Ministry of Foreign Affairs stated that the cargo included "240 metric tons of obsolete defensive weapons -- two anti-aircraft missile complexes Volga and Pechora, nine missiles in parts and spares, two Mig-21 Bis and 15 motors for this type of airplane, all of it manufactured in the mid-20th century -- to be

²⁶² <http://www.v3.co.uk/v3-uk/news/2202493/iran-and-north-korea-sign-technology-treaty-to-combat-hostile-malware>

²⁶³ <http://www.voanews.com/content/ties-among-north-korea-syria-iran-a-major-security-threat/1639769.html>

²⁶⁴ http://38north.org/2014/08/aberge080514/?utm_source=feedburner&utm_medium=feed&utm_campaign=Feed%3A+38North+%2838+North%3A+Informed+Analysis+of+North+Korea%29

²⁶⁵ http://www.jewishjournal.com/opinion/article/hamas_global_support_network_must_be_targeted

²⁶⁶ <http://www.ibtimes.com/north-korea-send-hamas-weapons-communication-equipment-secret-arms-deal-1640088>

²⁶⁷ <http://www.naenara.com.kp/en/kcc/>

²⁶⁸ <http://www.armscontrol.org/factsheets/dprkchron>

²⁶⁹ http://38north.org/2014/08/aberge080514/?utm_source=feedburner&utm_medium=feed&utm_campaign=Feed%3A+38North+%2838+North%3A+Informed+Analysis+of+North+Korea%29

²⁷⁰ http://www.jewishjournal.com/opinion/article/hamas_global_support_network_must_be_targeted

²⁷¹ <http://www.ibtimes.com/north-korea-send-hamas-weapons-communication-equipment-secret-arms-deal-1640088>

²⁷² http://h30499.www3.hp.com/t5/HP-Security-Research-Blog/HPSR-Threat-Intelligence-Briefing-Episode-11/ba-p/6385243#.U_TIZGSwL-0

repaired and returned to Cuba." Experts said the cargo appeared to include a SNR-75 Fan Song fire-control radar system for an SA-2 missile, a Soviet-era missile system that was also used in Cuba.²⁷³ Following the incident, Fidel Castro credited former North Korean leader Kim Il-Sung for providing Cuba with weapons near the end of the Cold War. Weapons included 100,000 AK rifles and necessary ammunition.²⁷⁴

While no apparent cyber relationship exists between North Korea and Cuba at this time, their track record for weapons trade means the potential for future collaboration in the cyber realm cannot be discounted.

Timeline of significant North Korean cyber activity

2004

- North Korea gains access to 33 South Korean military wireless communication networks²⁷⁵

2006

- The U.S. State Department is attacked by entities in the East Asia-Pacific region. The attacks coincided with State Department negotiations with North Korea regarding the regime's nuclear missile tests. (June)²⁷⁶
- A South Korean military official states North Korea's Unit 121 has breached South Korean and U.S. military entities. (July)²⁷⁷

2007

- North Korea tests a logic bomb (October)²⁷⁸

2009

- North Korea states that it is "fully ready for any form of high-tech war." (June)²⁷⁹
- DarkSeoul DDoS and disk wiping malware targeting South Korean and U.S. government, media outlet, and financial websites. These attacks also coincided with U.S. Independence Day. (July)^{280 281}
- Malware for "Operation Troy" was likely planted.²⁸²

2010

- DarkSeoul Backdoor.Prioxer detected (June)²⁸³
- Korean Central News Agency website becomes North Korea's first known direct connection to the Internet (October)²⁸⁴

²⁷³ <http://www.nbcnews.com/news/other/north-korean-ship-carrying-hidden-missile-equipment-detained-after-leaving-f6C10647045>

²⁷⁴ <http://www.abc.net.au/news/2013-08-15/fidel-castro-cuba-north-korea-war-ussr/4887920>

²⁷⁵ <http://www.scribd.com/doc/15078953/Cyber-Threat-Posed-by-North-Korea-and-China-to-South-Korea-and-US-Forces-Korea>

²⁷⁶ <http://www.informationweek.com/state-department-releases-details-of-computer-system-attacks/d/d-id/1045112?>

²⁷⁷ <http://www.scribd.com/doc/15078953/Cyber-Threat-Posed-by-North-Korea-and-China-to-South-Korea-and-US-Forces-Korea>

²⁷⁸ <http://www.scribd.com/doc/15078953/Cyber-Threat-Posed-by-North-Korea-and-China-to-South-Korea-and-US-Forces-Korea>

²⁷⁹ http://www.huffingtonpost.com/2009/07/11/north-korea-army-lab-110-_n_229986.html

²⁸⁰ <http://www.symantec.com/connect/blogs/four-years-darkseoul-cyberattacks-against-south-korea-continue-anniversary-korean-war>

²⁸¹ <http://powerofcommunity.net/poc2009/si.pdf>

²⁸² <http://www.darkreading.com/attacks-and-breaches/south-korean-bank-hackers-target-us-military-secrets/d/d-id/1110674?>

²⁸³ <http://www.symantec.com/connect/blogs/four-years-darkseoul-cyberattacks-against-south-korea-continue-anniversary-korean-war>

²⁸⁴ <http://www.northkoreatech.org/2010/10/09/the-new-face-of-kcna/>

2011

- “10 Days of Rain” Attack - DarkSeoul DDoS and disk wiping malware against South Korean media, financial, and critical infrastructure targets (March)^{285 286}
- North Korea disrupts South Korean GPS signals (March)²⁸⁷
- North Korea reportedly attempts DDoS attack against Incheon Airport ²⁸⁸
- Nonghyup bank suffers DDoS attack (April)²⁸⁹

2012

- South Korean newspaper JoongAng Ilbo attacked (June)²⁹⁰
- DarkSeoul Downloader.Castov detected (October)²⁹¹
- North Korea signs treaty with Iran, agreeing to combat “common enemies” in cyberspace²⁹²

2013

- “March 20” disk wiping attacks against South Korean media and financial institutions (March)²⁹³
- Whois Team claims responsibility for attacking LG +U website with wiper malware and defacement, impacting South Korean media and financial institutions (March) ^{294 295}
- The New Romantic Cyber Army Team claims responsibility for the same attacks²⁹⁶
- North Korea experiences 36-hour Internet outage. The cause was never definitively determined²⁹⁷
- Anonymous launches #OpNorthKorea and targets North Korean websites (March)²⁹⁸
- Anonymous allegedly hacks Uriminzokkiri and takes over its Twitter and Flickr pages ²⁹⁹ (April)
- DarkSeoul attack on South Korean financial institutions (May)³⁰⁰
- DarkSeoul DDoS attacks against South Korean government’s DNS server (June)³⁰¹
- Details on Kimsuky malware, which targeted South Korean think tanks, first released (September)³⁰²

2014

- North Korean drones found near South Korean border (March and April)³⁰³

²⁸⁵ <http://www.symantec.com/connect/blogs/four-years-darkseoul-cyberattacks-against-south-korea-continue-anniversary-korean-war>

²⁸⁶ <https://docs.google.com/file/d/0B6CK-ZBGUe4dGVHdTznenJMRUk/preview?pli=1>

²⁸⁷ <http://www.reuters.com/article/2011/05/03/us-korea-north-cyber-idUSTRE7421Q520110503>

²⁸⁸ <http://threatpost.com/report-north-korea-accused-ddos-attack-south-korean-airport-060712/76664>

²⁸⁹ <http://koreajoongangdaily.joins.com/news/article/article.aspx?aid=2965629>

²⁹⁰ <http://www.theaustralian.com.au/news/latest-news/south-korean-newspaper-joongang-ilbo-hit-by-major-cyber-attack/story-fn3dxix6-1226391202749>

²⁹¹ <http://www.symantec.com/connect/blogs/four-years-darkseoul-cyberattacks-against-south-korea-continue-anniversary-korean-war>

²⁹² <http://www.v3.co.uk/v3-uk/news/2202493/iran-and-north-korea-sign-technology-treaty-to-combat-hostile-malware>

²⁹³ <http://www.symantec.com/connect/blogs/four-years-darkseoul-cyberattacks-against-south-korea-continue-anniversary-korean-war>

²⁹⁴ <http://www.zdnet.com/massive-attack-on-lg-uplus-sparks-n-korea-reprisal-fears-7000012881/>

²⁹⁵ http://www.theregister.co.uk/Print/2013/03/22/sk_megahack/

²⁹⁶ [http://www.csmonitor.com/World/Security-Watch/2013/1019/In-cyberarms-race-North-Korea-emerging-as-a-power-not-a-pushover/\(page\)/2](http://www.csmonitor.com/World/Security-Watch/2013/1019/In-cyberarms-race-North-Korea-emerging-as-a-power-not-a-pushover/(page)/2)

²⁹⁷ http://www.computerworld.com/s/article/9237652/North_Korea_39_s_Internet_returns_after_36_hour_outage

²⁹⁸ <http://www.northkoreatech.org/2013/03/30/tango-down-more-attacks-on-dprk-websites/>

²⁹⁹ <http://www.washingtontimes.com/news/2013/apr/4/anonymous-hackers-bring-down-north-korean-websites/>

³⁰⁰ <http://www.symantec.com/connect/blogs/four-years-darkseoul-cyberattacks-against-south-korea-continue-anniversary-korean-war>

³⁰¹ <http://www.symantec.com/connect/blogs/four-years-darkseoul-cyberattacks-against-south-korea-continue-anniversary-korean-war>

³⁰² http://www.securelist.com/en/analysis/204792305/The_Kimsuky_Operation_A_North_Korean_APT

³⁰³ <http://blogs.wsj.com/korearealtime/2014/04/02/seoul-points-to-north-korea-in-crashed-drones-investigation/>

Patterns in the noise: cyber incidents attributed to North Korean actors

It is interesting to note that much of North Korea's cyber activity follows a distinct pattern. Analysis of North Korean cyber activity gives insight into these patterns and also helps tie together North Korea's strategic, tactical, and operational capabilities. Strategic capabilities refer to the assets used in support of a long-term, overarching goal. Tactical capabilities refer to the methods and maneuvers actually implemented in pursuit of the strategic goal.³⁰⁴ Operational capabilities refer to the potential use of these capabilities.³⁰⁵

In 2004, in response to the annual U.S. – South Korea joint military exercises, North Korea reportedly gained access to 33 South Korean military wireless communication networks.³⁰⁶ The next significant cyber attack attributed to North Korea was in June 2006. The U.S. State Department was attacked by entities in the East Asia-Pacific region. The attacks coincided with State Department negotiations with North Korea regarding the regime's nuclear missile tests.³⁰⁷ In July 2006, North Korea's Unit 121 reportedly breached South Korean and U.S. military entities.³⁰⁸ This attack was concurrent with the regime's test-fire of at least one long-range missile and several medium-range missiles.³⁰⁹

2007 was politically tumultuous for North Korea. Following multi-national talks, the UN's International Atomic Energy Agency (IAEA) ordered the shutdown of the regime's nuclear facilities in Yongbyon in July.³¹⁰ Its nuclear efforts temporarily thwarted, North Korea tested a logic bomb in October 2007.³¹¹

In April 2009, North Korea ejected IAEA and U.S. nuclear compliance officials. The regime indicated refusal to comply with any UN agreements regarding nuclear weaponry and announced it would reinstate its nuclear materials production. The next month, North Korea conducted an underground nuclear test and voiced its confidence that the regime was well on its way to producing viable nuclear technology. The UN called an emergency meeting condemning the nuclear weapons test, and South Korea joined the Proliferation Security Initiative (PSI). North Korea issued a statement via KCNA calling South Korea's involvement in PSI an act of war.³¹² In June 2009, North Korea stated that it was "fully ready for any form of high-tech war."³¹³ The following month, DDoS and disk wiping malware, later known as DarkSeoul, targeted South Korean and U.S. government entities, media outlets, and financial websites. The attacks coincided

³⁰⁴ <http://www.scholastic.com/teachers/article/strategy-and-tactics-military>

³⁰⁵ <http://www.dau.mil/pubscats/Pages/preface.aspx>

³⁰⁶ <http://www.scribd.com/doc/15078953/Cyber-Threat-Posed-by-North-Korea-and-China-to-South-Korea-and-US-Forces-Korea>

³⁰⁷ <http://www.informationweek.com/state-department-releases-details-of-computer-system-attacks/d/d-id/1045112?>

³⁰⁸ <http://www.scribd.com/doc/15078953/Cyber-Threat-Posed-by-North-Korea-and-China-to-South-Korea-and-US-Forces-Korea>

³⁰⁹ <https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=2&ved=0CCMQFjAB&url=http%3A%2F%2Fwww.bbc.com%2Fnews%2Fworld-asia-pacific-15278612&ei=fabyU6XQLsLFigLH94GIaw&usq=AFQjCNGbrzkNZJ5tz4jmLyMPsCHEHc41WA&sig2=l8FMadbvzFxEbBOAMW06Q&bvmm=bv.73231344,d.cGE&cad=rja>

³¹⁰ <http://www.armscontrol.org/factsheets/dprkchron>

³¹¹ <http://www.scribd.com/doc/15078953/Cyber-Threat-Posed-by-North-Korea-and-China-to-South-Korea-and-US-Forces-Korea>

³¹² <http://www.armscontrol.org/factsheets/dprkchron>

³¹³ http://www.huffingtonpost.com/2009/07/11/north-korea-army-lab-110-_n_229986.html

with U.S. Independence Day.^{314 315} Other malware used for Operation Troy was also planted. Operation Troy would continue for several years, largely undetected.³¹⁶

In early 2011, political and military tensions were high. In February, James Clapper, United States Director of National Intelligence, testified that North Korea likely had undeclared uranium enrichment facilities as part of its nuclear weapons program.³¹⁷ In March 2011, South Korean media, financial, and critical infrastructure targets suffered a DDoS and disk-wiping malware attack later known as the “10 Days of Rain”. U.S. and South Korean military entities were also targeted by DDoS during this attack. The attack used the DarkSeoul malware.³¹⁸ North Korea also disrupted South Korean GPS signals. Additionally, North Korean actors reportedly attempted a DDoS attack against South Korea’s Incheon Airport that same month.³¹⁹ These incidents coincided with the annual U.S. – South Korea joint military exercises.³²⁰ The following month, North Korean actors reportedly launched a DDoS attack against South Korea’s Nonghyup bank.³²¹

In 2012, an attack on South Korean Newspaper JoongAng Ilbo was attributed to North Korean actors. This attack also coincided with the timing of the annual joint U.S. – South Korea military exercises.³²² In September 2012, North Korea signed a cyber treaty with Iran, agreeing the two nations would collaborate to combat “common enemies” in cyberspace.³²³

The week of March 11, 2013, the U.S. and South Korea began their annual joint military exercise near the Korean Peninsula. Like clockwork, attacks attributed to North Korea and now known as the March 20 attacks targeted three South Korean media outlets and Shinhan, Nonghyup, and Jeju banks. North Korea also exhibited other hostile activity at that time. North Korea cut communication with Seoul and announced it had scrapped the 1953 armistice between the two Koreas. North Korea’s foreign ministry also issued a statement that it perceived this exercise as a precursor to invasion and that the regime would respond with a “strong military counteraction” if the situation escalated.³²⁴ That same week, the North Korean military conducted a drone attack simulation.³²⁵

On March 18, the Uriminzokkiri YouTube channel posted an anti-U.S. video entitled “Firestorms Will Rain on the Headquarters of War” that showed a depiction of the White House in crosshairs, followed by an explosion.³²⁶

³¹⁴ <http://www.symantec.com/connect/blogs/four-years-darkseoul-cyberattacks-against-south-korea-continue-anniversary-korean-war>

³¹⁵ <http://powerofcommunity.net/poc2009/si.pdf>

³¹⁶ <http://www.symantec.com/connect/blogs/four-years-darkseoul-cyberattacks-against-south-korea-continue-anniversary-korean-war>

³¹⁷ <http://www.armscontrol.org/factsheets/dprkchron>

³¹⁸ <http://www.symantec.com/connect/blogs/four-years-darkseoul-cyberattacks-against-south-korea-continue-anniversary-korean-war>

³¹⁹ <http://threatpost.com/report-north-korea-accused-ddos-attack-south-korean-airport-060712/76664>

³²⁰ <http://www.reuters.com/article/2011/05/03/us-korea-north-cyber-idUSTRE7421Q520110503>

³²¹ <http://koreajoongangdaily.joins.com/news/article/article.aspx?aid=2965629>

³²² <http://www.theaustralian.com.au/news/latest-news/south-korean-newspaper-joongang-ilbo-hit-by-major-cyber-attack/story-fn3dxix6-1226391202749>

³²³ <http://www.v3.co.uk/v3-uk/news/2202493/iran-and-north-korea-sign-technology-treaty-to-combat-hostile-malware>

³²⁴ <http://www.presstv.com/detail/2013/03/20/294499/north-korea-threatens-us-over-bombers/>

³²⁵ http://www.huffingtonpost.com/2013/03/20/north-koreas-drone-n_2914794.html

³²⁶ <https://www.youtube.com/watch?v=Dyap eCi0l9A>

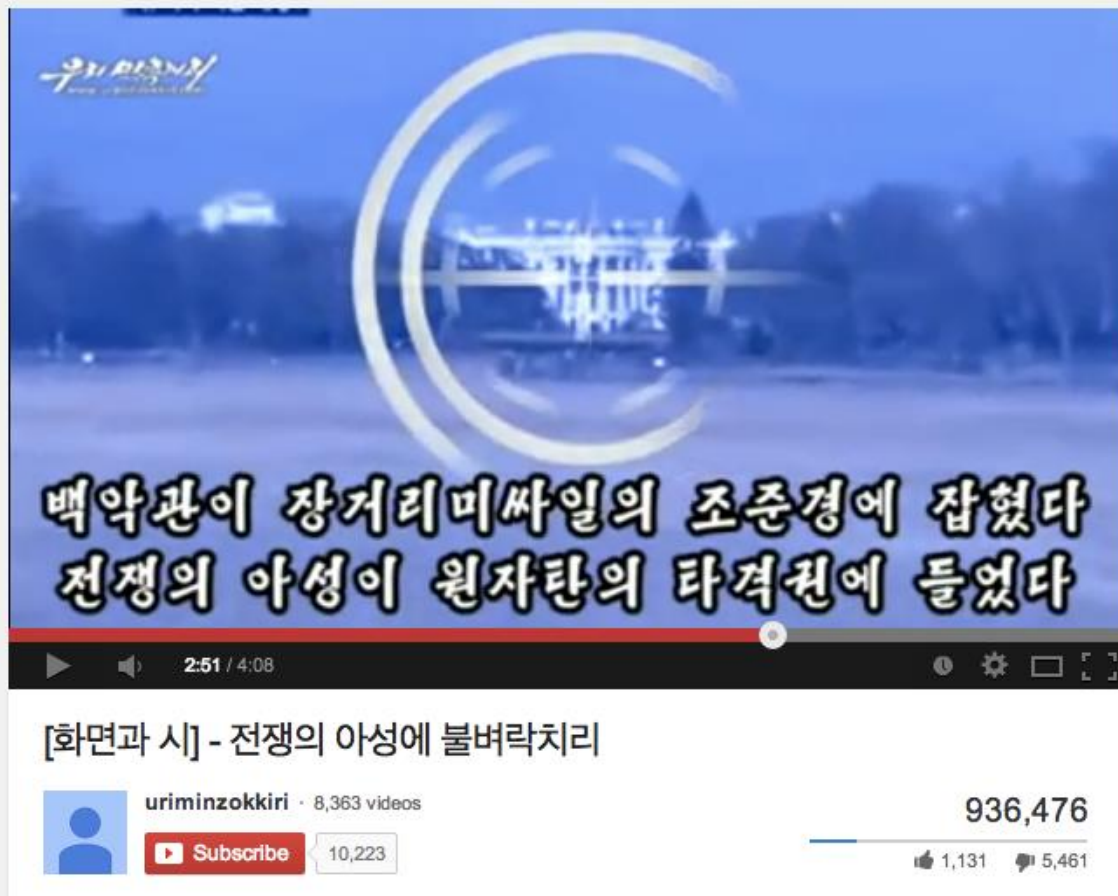


Figure 25 Uriminzokkiri YouTube video portraying anti-U.S. sentiments.³²⁷

In May 2013, DarkSeoul malware was used to attack several South Korean financial institutions; and in June, DarkSeoul DDoS attacks were launched against the South Korean government's DNS server. The latter took place on June 25, the anniversary of the start of the Korean War.³²⁸

As evidenced above, much of North Korea's cyber activity coincides with the annual U.S. – South Korea joint military exercises. Attacks not following that pattern were typically in response to political events impacting the regime or correlated with significant dates, such as the anniversary of the start of the Korean War. The regime's strategic assets and tactical capabilities in the cyber arena seem to have evolved only slightly since 2009. Most of the attacks attributed to North Korea employ limited tactics, and their operational capability demonstrates an increase in the frequency and volume of attacks but is otherwise unimpressive to date.

In June 2014, the regime demanded cancellation of the annual U.S. - South Korea joint military exercise, attempting to use participation in the upcoming Asian Games as a bargaining chip.³²⁹ The regime's demands may have had other political motivations, as they preceded the July 2014 meeting between South Korean president Park and Chinese President Xi Jinping. The meeting

³²⁷ <https://www.youtube.com/watch?v=DyapeCi0I9A>

³²⁸ <http://www.symantec.com/connect/blogs/four-years-darkseoul-cyberattacks-against-south-korea-continue-anniversary-korean-war>

³²⁹ <http://www.theguardian.com/world/2014/jun/30/north-korea-demands-cancellation-drills>

centered on trade and regional security issues, including the ever-present rhetoric around denuclearization of North Korea.³³⁰ Both leaders were critical of Japan's recent announcement to soften sanctions on North Korea.³³¹ As this report headed to press, the annual U.S. – South Korea joint military exercises were underway.³³²

DarkSeoul

The most prominent North Korean threat actor group is the group responsible for the DarkSeoul malware. According to statements from the South Korean government, North Korea's Lab 110 were the actors behind the DarkSeoul malware. South Korean intelligence reports stated that Lab 110, which is affiliated with the regime's defense ministry, was ordered by the North Korean regime to destroy South Korean communications networks.³³³ Although the March 20 attacks used DarkSeoul malware, it is interesting to note that two groups, Whols Team and New Romantic Cyber Army Team, claimed responsibility for the "March 20" 2013 attacks on South Korean media and financial institutions.³³⁴

According to statements from the South Korean government, North Korea's Lab 110 were the actors behind the DarkSeoul malware attacks.

Some of the DarkSeoul attacks corresponded with significant dates, such as U.S. Independence Day or the anniversary of the start of the Korean War. DarkSeoul attacks go beyond denial of service and sabotage. As early as 2009, the group responsible for the Dark Seoul attacks launched "Operation Troy", an espionage campaign targeting the South Korean military. The operation was codenamed "Troy" due to the frequent use of the word "Troy" in the malware's compile path strings.³³⁵ The malware used in these attacks sought out and exfiltrated data, based on keyword searches. While the malware was clearly intended to search for and exfiltrate certain types of data, its true impact on the targets was never revealed.³³⁶ The March 2011 "10 Days of Rain" DDoS attacks on U.S. and South Korean sites have also been attributed to the actors associated with DarkSeoul.³³⁷ According to Symantec, the politically motivated attacks have required a level of intelligence, coordination, monetary support, and technical sophistication that suggests state sponsorship.³³⁸ This designation means the group can be considered an advanced persistent threat (APT).

A March 20, 2013 attack attributed to the DarkSeoul actors targeted three South Korean media outlets and Shinhan, Nonghyup, and Jeju banks. The impact of the March 20 attacks included disruption of service at financial institutions and data deletion. However, the targeted entities resumed normal operations shortly thereafter.³³⁹ According to South Korean reports, the media outlets targeted corresponded with those listed by the North Korean regime in 2012 as right-wing press that manipulated South Korea's public opinion. In April 2012, the regime reportedly listed

³³⁰ http://edition.cnn.com/2014/07/02/world/asia/south-korea-xi-visit/index.html?hpt=hp_bn7

³³¹ <http://mobile.nytimes.com/blogs/sinosphere/2014/07/07/q-and-a-john-delury-on-chinese-south-korean-ties/?smid=tw-share>

³³² <http://www.globalpost.com/dispatch/news/yonhap-news-agency/140825/n-korea-urges-un-action-against-s-korea-us-military-drill>

³³³ <http://www.theguardian.com/world/2009/jul/11/south-korea-blames-north-korea-cyber-attacks>

³³⁴ [http://www.csmonitor.com/World/Security-Watch/2013/1019/In-cyberarms-race-North-Korea-emerging-as-a-power-not-a-pushover/\(page\)/2](http://www.csmonitor.com/World/Security-Watch/2013/1019/In-cyberarms-race-North-Korea-emerging-as-a-power-not-a-pushover/(page)/2)

³³⁵ <http://www.darkreading.com/attacks-and-breaches/south-korean-bank-hackers-target-us-military-secrets/d/d-id/1110674?>

³³⁶ <http://motherboard.vice.com/blog/the-dark-seoul-hackers-were-after-south-korean-military-secrets>

³³⁷ <http://blogs.mcafee.com/wp-content/uploads/2011/07/McAfee-Labs-10-Days-of-Rain-July-2011.pdf>

³³⁸ <http://www.symantec.com/connect/blogs/four-years-darkseoul-cyberattacks-against-south-korea-continue-anniversary-korean-war>

³³⁹ http://www.nytimes.com/2013/03/21/world/asia/south-korea-computer-network-crashes.html?pagewanted=all&_r=1&

those entities as attack targets.³⁴⁰ The malware used in the March 20, 2013 attacks were wiper malware. The malware attempted to disable AhnLab and Hauri AV antivirus products then proceeded to overwrite the master boot record (MBR). The attack was capable of wiping both Linux and Windows machines.³⁴¹ McAfee found that these attacks were the culmination of the malware campaign they dubbed “Operation Troy”.³⁴²

A report from IssueMakersLab tied the actors responsible for the March 20, 2013 attacks to cyber attack activity occurring as early as 2007. IssueMakersLab found that these actors consistently used the same 16-digit password for file compression, the same stage 1 C2 protocol, the same collection keywords and encryption keys, and the same development path.³⁴³ According to South Korea’s Korea Internet and Security Agency, the North Korean IP address 175.45.178.xx was found scanning South Korean routes the month before the attacks,³⁴⁴ and the same IP was reportedly logged as accessing one of the targets 13 times.³⁴⁵ Details of the March 20 attack also suggested possible ties to China. AlienVault suspected the Chinese exploit kit GonDad was used to spread the malware, and the Korean domains serving the malware were registered using a Chinese email address. Additionally, researchers at AhnLab in South Korea noted a Chinese IP address linked to the attacks.³⁴⁶

While no concrete evidence has been released that indicates Lab 110 was responsible for the DarkSeoul attacks, the responsible group’s targets, TTP, and attack timing demonstrate a strong pro-North Korean sentiment.

Known tactics, techniques and procedures

- Customized wiper malware³⁴⁷
- DDoS
- Multi-staged, coordinated attacks³⁴⁸
- Destructive payloads with politically significant trigger dates
- Use of politically themed strings when overwriting disk sectors
- Utilizing legitimate patching mechanisms to spread malware across corporate networks
- Encryption and obfuscation methods that have become their signature
- Repeated use of a specific webmail server
- Consistent C2 structures
- Antivirus disablement and evasion³⁴⁹
- Watering hole attacks
- Zero-days
- Spearphishing³⁵⁰

³⁴⁰ <http://english.yonhapnews.co.kr/northkorea/2013/03/21/71/0401000000AEN20130321006700315F.HTML>

³⁴¹ http://www.theregister.co.uk/Print/2013/03/22/sk_megahack/

³⁴² <http://www.darkreading.com/attacks-and-breaches/south-korean-bank-hackers-target-us-military-secrets/d/d-id/1110674?>

³⁴³ <https://docs.google.com/file/d/0B6CK-ZBGUme4dGVHdTznenJMRUk/preview?pli=1>

³⁴⁴ <http://english.yonhapnews.co.kr/national/2013/04/11/79/0301000000AEN20130411008351320F.HTML>

³⁴⁵ <http://www.darkreading.com/attacks-and-breaches/how-south-korea-traced-hacker-to-pyongyang/d/d-id/1109491?>

³⁴⁶ http://www.theregister.co.uk/Print/2013/03/22/sk_megahack/

³⁴⁷ <http://news.sky.com/story/1108704/darkseoul-gang-behind-years-of-korea-hacking>

³⁴⁸ <http://www.symantec.com/connect/blogs/four-years-darkseoul-cyberattacks-against-south-korea-continue-anniversary-korean-war>

³⁴⁹ http://www.theregister.co.uk/Print/2013/03/22/sk_megahack/

³⁵⁰ <http://www.infoworld.com/t/data-security/mcafee-uncovers-massive-cyber-espionage-campaign-against-south-korea-222245>

Targets

- South Korean military
- U.S. sites
- Shinhan Bank
- Nonghyup Bank³⁵¹
- Jeju Bank³⁵²
- Munhwa Broadcasting Corp.
- YTN
- Korea Broadcasting System³⁵³
- South Korean government DNS server
- South Korea financial institutions

Whols Team

Whols Team is one of two groups that claimed responsibility for the “March 20” attacks targeting South Korea. A defacement on the LG +U webpage stated that it was “Hacked by Whols Team” and that the attackers would return. The page featured three skulls.³⁵⁴ However, no other attacks by Whols Team have been observed.

³⁵¹ <http://www.reuters.com/article/2011/05/03/us-korea-north-cyber-idUSTRE7421Q520110503>

³⁵² http://www.nytimes.com/2013/03/21/world/asia/south-korea-computer-network-crashes.html?pagewanted=all&_r=1&

³⁵³ <http://www.businessweek.com/news/2013-03-20/s-dot-korea-hit-by-cyber-attack-roiling-banks-to-broadcasters>

³⁵⁴ <http://www.zdnet.com/massive-attack-on-lg-uplus-sparks-n-korea-reprisal-fears-7000012881/>

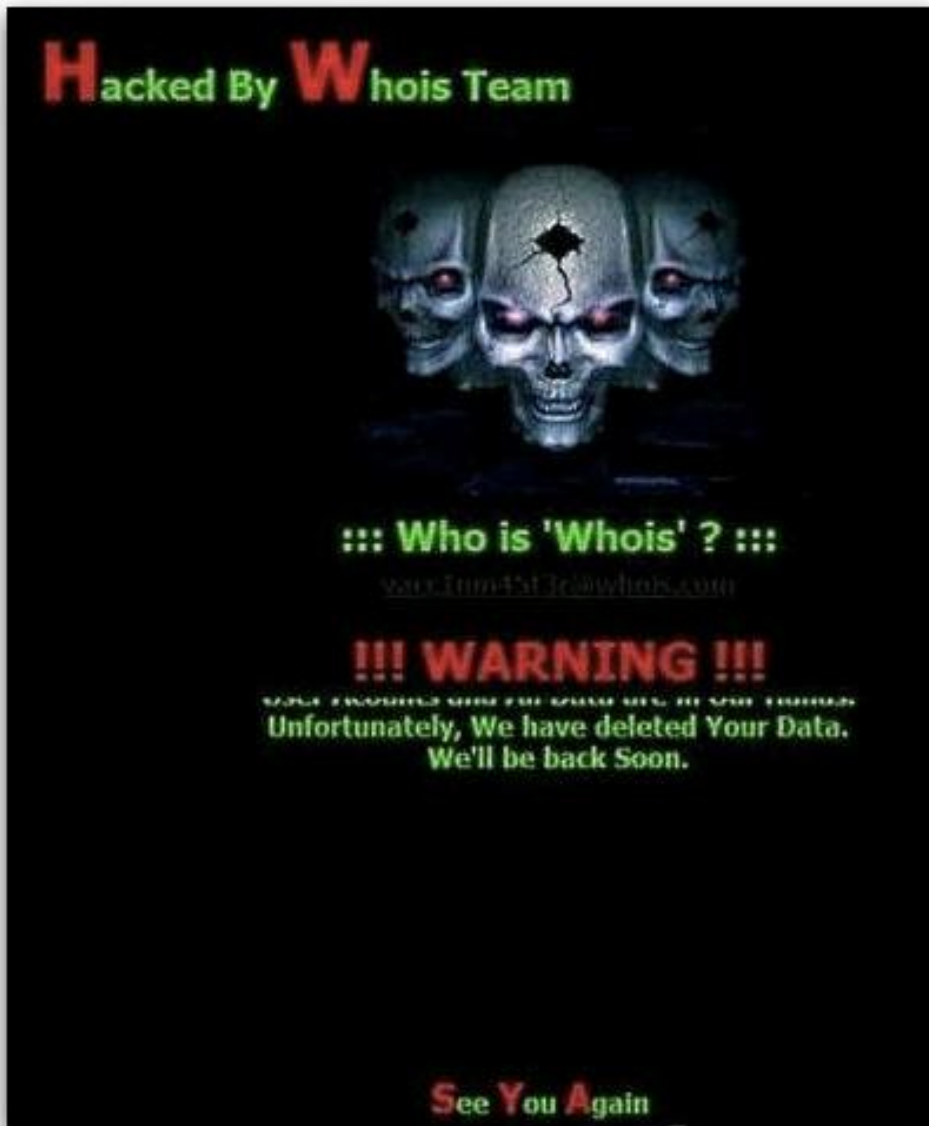


Figure 26 A defacement by “Whois Team” ³⁵⁵

Known tactics, techniques, and procedures

- Wiper malware³⁵⁶
- Defacements

Targets

- Took credit for an attack on the LG +U website.

³⁵⁵ <http://nakedsecurity.sophos.com/2013/03/20/south-korea-cyber-attack/>

³⁵⁶ <http://www.mcafee.com/sg/resources/white-papers/wp-dissecting-operation-troy.pdf>

Associated actors

- dbM4st3r
- d3sign3r
- APTM4st3r
- s3ll3r
- vacc1nm45t3r
- r3cycl3r

Based on North Korea's affinity for disinformation and counterintelligence, we must note the distinct possibility that operatives claiming to be Whols Team are part of another group and that the defacement was a false flag operation meant to pin blame on RAON_ASRT. RAON_ASRT is a South Korean white hat capture the flag (CTF) team, whose members also operate under the name "Whols".³⁵⁷

The screenshot shows the CTF TIME website interface. At the top, there is a navigation bar with 'CTF TIME' logo and links for 'CTFs', 'Upcoming', 'Archive', 'Calendar', 'Teams', 'FAQ', 'About', and 'Contact us'. A 'Sign in' button is in the top right. Below the navigation is a breadcrumb trail: 'Home / Teams / RAON_ASRT'. The main content area features the team name 'RAON_ASRT' with a small icon. Underneath, it says 'Also known as' followed by a list containing 'whols'. There is a large empty rectangular box, likely a placeholder for a team photo or logo. Below this are social media icons for Pinterest, Facebook, Twitter, YouTube, and a generic share icon. To the right, there is a 'Sign in to join the team.' link and a note: 'Overall rating place: 36 with 171,608 pts this year'. At the bottom, there is a section titled 'Participated in CTF events' with tabs for the years 2014, 2013, and 2012. A table lists the events:

Place	Team	CTF points	Rating points
8	DEF CON CTF Qualifier 2014	34.0000	73.699
3	Nuit du Hack CTF Quals 2014	2400.0000	43.810
10	PHD CTF Quals 2014	57800.0000	54.100

Figure 27 A screenshot showing that South Korea's RAON_ASRT white hat CTF team also uses the moniker Whols.³⁵⁸

RAON_ASRT (the RaonSecure Advanced Security Research Team) and its sub-teams Whols Team and Cpark Team³⁵⁹ have participated in and performed well in CTF contests such as the one hosted by [DefCon](#).³⁶⁰ In 2013, a member of RAON_ASRT was invited to Blue House, the residence of the South Korean president, to meet with president Park and discuss the security industry.³⁶¹ RAON_ASRT runs the Secuinside CTF competition.³⁶² Their parent organization RaonSecure operates a whitehat training program.³⁶³ The group also runs the Korea WhiteHat Contest, which is hosted by South Korea's Ministry of National Defense and National Intelligence Service and

³⁵⁷ <https://ctftime.org/team/3206>

³⁵⁸ <https://ctftime.org/team/3206>

³⁵⁹ <http://ls-al.org/asrt-has-become-the-winner-of-codegate-2013/>

³⁶⁰ <http://blog.raonsecure.com/62>

³⁶¹ <http://ls-al.org/asrt-researcher-meets-the-president-park-in-korea/>

³⁶² <http://ls-al.org/asrt-runs-secuinside-ctf/>

³⁶³ <http://www.whitehat.co.kr/>

supervised by South Korean Cyber Command.³⁶⁴ For these reasons, it seems unlikely that the RAON_ASRT Whols Team would maliciously target South Korean entities.

IsOne

IsOne is the group that claimed responsibility for the June 2012 attack on the website of South Korean newspaper JoongAng Ilbo. The attack included an attempt to wipe JoongAng Ilbo's servers as well as a defacement depicting a laughing cat. Despite efforts to wipe the target's servers, the target only suffered defacement and temporary downtime.³⁶⁵



Figure 28 Defacement by “IsOne”.³⁶⁶

Although the groups have a similar name and both use a cat theme, it is unclear whether a CTF team known as “The Cat is Number 1” and IsOne are the same actors. “The Cat is Number 1” members claim to hail from North Korea, but there is no hard evidence linking team members to

³⁶⁴ <http://ls-a.org/%EB%8C%80%ED%95%9C%EB%AF%BC%EA%B5%AD-%ED%99%94%EC%9D%B4%ED%8A%B8%ED%96%87-%EC%BD%98%ED%85%8C%EC%8A%A4%ED%8A%B8korea-whitehat-contest-%EA%B0%9C%EC%B5%9C/>

³⁶⁵ <http://koreajoongangdaily.joins.com/news/article/article.aspx?aid=2965629>

³⁶⁶ <http://bad-bytes.blogspot.co.uk/2012/06/joongang-ilbo-cyber-attack.html>

the region.³⁶⁷ Again, it seems that the actors responsible for the attack borrowed the moniker of another group.

CTF TIME CTFs Upcoming Archive Calendar Teams FAQ About Contact us Sign in

Home / Teams / The Cat is #1!!

The Cat is #1!!

Also known as

- The Cat is Number 1
- ¡¡El Gato es Número Uno!!
- thecat
- The_Cat_is_#1!!
- The_Cat_is_Number_1

we firmly believe that the cat is #1!!

Website: <http://worlds.fattest.cat/>

Sign in to join the team.
Overall rating place: 31 with 162.567 pts this year

Figure 29 A screenshot of “The Cat is Number One” profile on CTF Time ³⁶⁸

According to South Korea’s National Police Agency, the attack on JoongAng Ilbo shares characteristics with previous attacks attributed to North Korean actors. An investigation conducted by the agency’s Cyber Terror Response Center found that the actors targeting JoongAng Ilbo used two North Korean servers and 17 servers in 10 other countries. One server maintained a constant connection to an IP address belonging to Josen Telecommunication Company, which is affiliated with North Korea’s Ministry of Posts and Telecommunications. Investigators found that one of the servers used in the attack on JoongAng Ilbo was also used in the March 2011 DDoS attacks on South Korean critical infrastructure sites and the April 2011 attack on Nyongyup Bank.³⁶⁹

Known tactics, techniques and procedures

- Wiper malware
- Defacements

Targets

- Took credit for defacing JoongAng Ilbo.

³⁶⁷ <https://ctftime.org/team/2538>

³⁶⁸ <https://ctftime.org/team/2538>

³⁶⁹ <http://koreaajoongdaily.joins.com/news/article/article.aspx?aid=2965629>

Kimsukyang

The Kimsuky malware, which targeted South Korean think tanks, is loosely attributed to an actor referred to as Kimsukyang. Little is known about the actor or group responsible for the malware. However, the following email addresses are associated with the Kimsuky operation:³⁷⁰

- beautifl@mail.bg
- ennemyman@mail.bg
- fasionman@mail.bg
- happylove@mail.bg
- lovest000@mail.bg
- monneyman@mail.bg
- sportsman@mail.bg
- veryhappy@mail.bg
- iop110112@hotmail.com
- rsh1213@hotmail.com

The email address iop110112@hotmail.com was registered using the alias “kimsukyang”, and rsh1213@hotmail.com was registered using the alias “Kim asdfa”.

Kaspersky found that the Kimsuky operation used 10 IP addresses in two Chinese provinces that border North Korea: Jilin and Liaoning.³⁷¹

Known tactics, techniques and procedures

- Malware with keylogger and data exfiltration capabilities
- Malware disables AhnLab security software³⁷²

Targets

- Sejong Institute
- Korea Institute for Defense Analyses (KIDA)
- Ministry of Unification
- Hyundai Merchant Marine
- The Supporters of Korean Unification³⁷³

New Romantic Cyber Army Team / Hastati

The New Romantic Cyber Army Team also took credit for the March 20, 2013 attacks. McAfee suspected New Romantic Cyber Army Team were responsible for Operation Troy and the resulting March 20, 2013 attacks due to the group’s “frequent use of Roman and classical terms in their

³⁷⁰ http://www.securelist.com/en/analysis/204792305/The_Kimsuky_Operation_A_North_Korean_APT

³⁷¹ [http://www.csmonitor.com/World/Security-Watch/2013/1019/In-cyberarms-race-North-Korea-emerging-as-a-power-not-a-pushover/\(page\)/5](http://www.csmonitor.com/World/Security-Watch/2013/1019/In-cyberarms-race-North-Korea-emerging-as-a-power-not-a-pushover/(page)/5)

³⁷² http://www.securelist.com/en/analysis/204792305/The_Kimsuky_Operation_A_North_Korean_APT

³⁷³ http://www.securelist.com/en/analysis/204792305/The_Kimsuky_Operation_A_North_Korean_APT

code.”³⁷⁴ It is unknown whether Hastati is an alternate name for the group or whether Hastati is an individual actor within the group.

It is interesting to note that the malware associated with these actors uses the strings “HASTATI” and “PRINCIPIES” to overwrite the MBR. The name Hastati likely refers to a class of infantrymen of the early Roman Republic. The Hastati were less experienced soldiers who fought on the frontlines with spears and swords. Principes likely refers to more experienced Roman soldiers who fought on the second line of battle.³⁷⁵

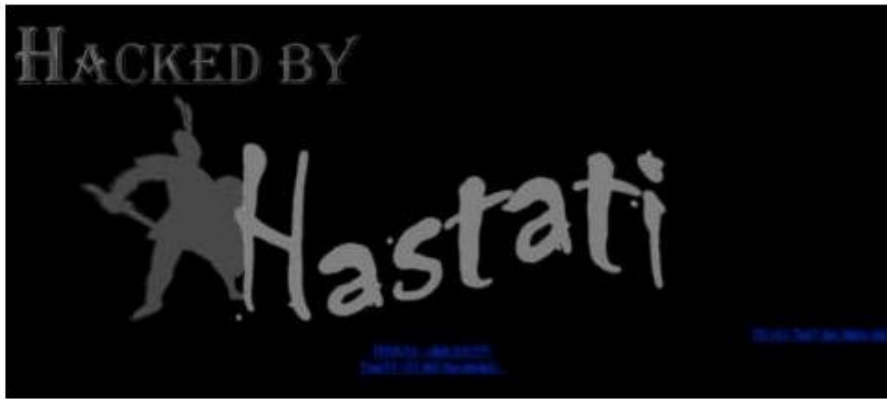


Figure 30 Defacement by Hastati.³⁷⁶

Known tactics, techniques and procedures

- Wiper malware

Targets

- KBS TV³⁷⁷
- Entities targeted in Operation Troy³⁷⁸

Malware summary

HP researchers had previously analyzed samples of the DarkSeoul dropper, and findings were published in our annual [HP Cyber Risk Report 2013](#). Analysis of this malware is included in [Appendix C](#). Analysis of additional malware used in these campaigns produced no new findings and only corroborated what was found by external security researchers. These publicly available analyses have been cited throughout the report. Some of the malware samples were no longer publicly available. However, CrowdStrike obtained these missing samples before they disappeared from the wild and conducted thorough analysis, which was released in their subscription-only reports. While we cannot divulge detailed information from those reports, an overview of the findings is provided below.

³⁷⁴ <http://www.darkreading.com/attacks-and-breaches/south-korean-bank-hackers-target-us-military-secrets/d/d-id/1110674?>

³⁷⁵ <http://www.roman-empire.net/army/army.html#earlylegion>

³⁷⁶ <http://eromang.zataz.com/2013/04/02/dark-south-korea-total-war-review/>

³⁷⁷ <http://eromang.zataz.com/2013/04/02/dark-south-korea-total-war-review/>

³⁷⁸ <http://www.mcafee.com/us/resources/white-papers/wp-dissecting-operation-troy.pdf>

The majority of the malware used in cyber incidents attributed to North Korea were variations of three types of malware: dropper, wiper, and IRC remote access trojan (RAT). CrowdStrike's attribution of this malware to North Korean actors stemmed from two primary factors: Korean language characters found in the binaries and the propensity to specifically target South Korean entities.³⁷⁹

Dropper samples consistently targeted AhnLab Policy Center as a propagation method. This information is corroborated in a Black Hat Asia 2014 presentation by Fortinet researcher Kyle Yang.³⁸⁰ CrowdStrike's report also briefly noted the use of an update server vector.³⁸¹ Yang analyzed the malware's update config metadata and matched its format to the AhnLab Policy Center. To test its payload, Yang set up a server/client and executed the update through the server. As Yang had predicted, it wiped the client.³⁸² While the method for initial compromise of the update server is not noted in detail, CrowdStrike's report cites "collateral information" that suggests targeted email attacks were used to gain initial entry, and policy servers were then compromised. The upload server vector included a time-based logic bomb that allowed the wiper to target a large number of systems, on a set time and date, with full permissions on all of the targeted systems.³⁸³

According to CrowdStrike, the wiper malware was dropped on the systems as AgentBase.exe. The wiper used the Windows utility 'taskkill' to kill the processes pasvc.exe and clisvc.exe, which are the main processes for the Ahnlab and Hauri antivirus applications.³⁸⁴ ³⁸⁵ The wiper then performed system reconnaissance, gathering drive information and operating system version. Depending on the OS used, the wiper recursively deleted files on the file system, deleting the Windows folder last. It then overwrote the MBR with the strings "HASTATI", "PRINCPES", "PRINCIPES", or "PRINCPES".³⁸⁶

While there are several variants of the wiper, all seem to have been used on the same date. It is unclear why multiple wiper variants with slightly differing behavior were used for the same campaign. One possible explanation is that multiple variants were used to minimize the operational damage to the mission in the case of an early detection of one of the variants. For example, if one wiper variant was compromised or detected by antivirus or IDS signatures, the other variants may have differed enough to remain undetected, still resulting in mission success.

According to CrowdStrike, a third malware component downloaded an IRC RAT from various compromised websites. This RAT is detected by Symantec as Backdoor.Prioxer. Prioxer has been linked to other 2011 attacks on South Korea. It is unclear whether these downloaders were

³⁷⁹ CrowdStrike Intelligence Report CSIR-13013

³⁸⁰ Yang, Kyle. *Z:\Make Troy\, Not War: Case Study of the Wiper APT in Korea, and Beyond*. Black Hat Asia, March 2014.

³⁸¹ CrowdStrike Intelligence Report CSIR-13013

³⁸² Yang, Kyle. *Z:\Make Troy\, Not War: Case Study of the Wiper APT in Korea, and Beyond*. Black Hat Asia, March 2014.

³⁸³ CrowdStrike Intelligence Report CSIR-13013

³⁸⁴ CrowdStrike Intelligence Report CSIR-13030

³⁸⁵ Yang, Kyle. *Z:\Make Troy\, Not War: Case Study of the Wiper APT in Korea, and Beyond*. Black Hat Asia, March 2014.

³⁸⁶ CrowdStrike Intelligence Report CSIR-13030

pushed out in the same update server vector as the wipers. However, the two malware types both use the same packer 'Jokra' and both contain the strings "HASTATI" and "PRINCPES".³⁸⁷

Analysis

Based on the information above, we have identified strategic challenges that impact the development of North Korea's cyber warfare capabilities. We have also noted relevant implications:

- The North Korean regime strictly controls all Internet infrastructure,³⁸⁸ meaning cyber activity by dissidents or autonomous hacker groups are very unlikely. In other words, any cyber attacks originating in North Korea can be assumed to be state sponsored. For this reason, according to defectors, the regime's cyber operators do not typically launch attacks directly from within North Korea. Instead, many regime-sponsored attacks are launched from cells based in China, U.S., South Asia, Europe, and even South Korea.³⁸⁹
- North Korea has a limited number of outgoing connections.³⁹⁰ For this reason, there is a low probability of DDoS originating from within. However, this does not preclude the use of botnets with a local C2 server or the use of networks in third-party nations to launch attacks. As seen in the July 2009 attacks on South Korean and U.S. targets, North Korea has leveraged networks in countries such as Austria, Georgia, Germany, and even South Korea and the U.S., in order to launch cyber attacks.³⁹¹ North Korea will likely be forced to rely on third parties for quite some time, due to its lack of sufficient infrastructure for launching large-scale CNO.
- Several outward facing websites are hosted in China and other countries. This implies two possibilities: that North Korea's infrastructure cannot handle a heavy incoming traffic load³⁹² or that the regime wants to separate the propaganda crafted for an outside target audience from internally-focused propaganda. This arrangement seems unlikely to change in the foreseeable future.
- North Korea is known to have unstable power supplies³⁹³, which limits scalability of the regime's current CNO capabilities. This is another reason why expansion of CNO capabilities using the nation's own infrastructure seems unlikely in the foreseeable future.
- North Korea is known to have monetary deficiencies,³⁹⁴ which further limit expansion of infrastructure and CNO capabilities, at least without third-party aid. North Korea continues to rely heavily on China for sustainment.³⁹⁵
- Although we see few instances of overt cyber operations, that North Korea reportedly spends so much of its limited resources on training and equipping cyber operators speaks volumes. The human element of the regime's cyber war program, at least, has potential.

³⁸⁷ CrowdStrike Intelligence Report CSIR-13013

³⁸⁸ http://www.defense.gov/pubs/North_Korea_Military_Power_Report_2013-2014.pdf

³⁸⁹ [http://www.csmonitor.com/World/Security-Watch/2013/1019/In-cyberarms-race-North-Korea-emerging-as-a-power-not-a-pushover/\(page\)/5](http://www.csmonitor.com/World/Security-Watch/2013/1019/In-cyberarms-race-North-Korea-emerging-as-a-power-not-a-pushover/(page)/5)

³⁹⁰ http://www.defense.gov/pubs/North_Korea_Military_Power_Report_2013-2014.pdf

³⁹¹ <http://www.theguardian.com/world/2009/jul/11/south-korea-blames-north-korea-cyber-attacks>

³⁹² <http://binarycore.org/2012/05/30/investigating-north-koreas-netblock-part-3-topology/>

³⁹³ <http://38north.org/2010/09/speak-loudly-and-carry-a-small-stick-the-north-korean-cyber-menace/>

³⁹⁴ http://www.defense.gov/pubs/North_Korea_Military_Power_Report_2013-2014.pdf

³⁹⁵ <http://docs.house.gov/meetings/AS/AS00/20140402/101985/HHRG-113-AS00-Wstate-ScaparrottiUSAC-20140402.pdf>

- Sanctions against North Korea and export laws prohibit the sale of certain technologies to the regime.³⁹⁶ In other words, in order to obtain the technology needed for a cyber warfare program, the regime must improvise. North Korea must develop its own technology, manufacture technology using plans obtained via industrial espionage, or rely on third parties to procure it for them. However, the regime has historically failed in its attempts of large-scale production of electronic components. At present, North Korea relies on China to provide much of its network hardware, including servers and routers.³⁹⁷ It is unlikely that North Korea will compromise on its nuclear program, meaning sanctions will likely be longstanding, and the regime will have to continue to rely on third parties to procure technology.

Cyber incidents attributed to North Korean actors seem to follow distinct patterns:

- According to reports by other researchers, the conventions and C2 structure used by North Korean cyber actors show continuity and consistency over time.
- The majority of the incidents attributed to North Korean actors consistently used wiper malware.
- Several of the incidents included defacements, with a different group taking credit each time. Additionally, little information or attack history was found about any of the groups, aside from information acknowledged in this report. These factors seem to indicate that a single group may have been responsible for several attacks over time, using different group names as a false flag.
- On more than one occasion, the malware included provisions to disable security software made by South Korean security company AhnLab. This detail strengthens the case that the malware was written or modified to specifically target South Korean machines.
- The attacks followed an explicit pattern: most were around the time of U.S. – South Korean joint military exercises, while the others fell on a significant date or were in response to political events.
- The primary targets were South Korean and U.S. entities. While these nations are traditionally targeted by the regime, it is also possible that South Korean entities are quick to attribute any attack on their infrastructure to North Korean actors. In fact, in some cases, South Korean reports were the only source of attribution.

Summary

Does North Korea have sufficient cyber infrastructure and cyber warfare capabilities to harm the U.S. and its allies? While North Korea's cyber warfare capabilities pale in comparison to those of wealthier nations, the regime has made significant progress in developing its infrastructure and in establishing cyber operations. The rate of this progress warrants a closer look at North Korea's motivations, TTPs, and capabilities. As noted above, North Korea views the U.S. and South Korea as its primary adversaries. The U.S. and South Korea are high-tech nations with economies that

³⁹⁶ <http://www.foxnews.com/world/2012/04/03/exclusive-cash-for-computers-is-un-busting-its-own-sanctions-in-north-korea/>

³⁹⁷ [http://www.csmonitor.com/World/Security-Watch/2013/1019/In-cyberarms-race-North-Korea-emerging-as-a-power-not-a-pushover/\(page\)/4](http://www.csmonitor.com/World/Security-Watch/2013/1019/In-cyberarms-race-North-Korea-emerging-as-a-power-not-a-pushover/(page)/4)

depend heavily on technology.³⁹⁸ In contrast, North Korea does not have a high tech culture. For these reasons, we should not overestimate the regime's *advanced* cyber capability, yet we should never underestimate the potential impact of North Korea utilizing less advanced, quick-and-dirty tactics like DDoS to cripple their high-tech targets. Both government and corporate entities are susceptible to being targeted by North Korean cyber attacks. North Korean *juche* ideology places the survival of the regime as its primary goal, and any perceived threat to the regime may be targeted. Several attacks on U.S. and South Korean government, financial, and critical infrastructure entities have been attributed to North Korean origins.. These attacks were often preceded by or occurred in conjunction with North Korea voicing negative sentiments about the targeted entities. As we saw with Iranian cyber actors in [HPSR Security Briefing Episode 11](#),³⁹⁹ state sponsored cyber actors often launch an attack in response to a political trigger. The same pattern seems to apply to pro-North Korean cyber actors, who have launched attacks to coincide with U.S. Independence Day and the anniversary of the start of the Korean War, as well as propaganda and cyber attacks in response to joint military exercises between the U.S. and South Korea.^{400 401}

As shown by North Korea's past behavior (which is consistent with their doctrine), they are easily "pushed into a corner". At the slightest perceived threat, the regime responds with saber-rattling and peacocking. The regime is extremely defensive and will, in turn, flex its muscles to show the world how capable it is, even if this is an inaccurate display of their overall capabilities.

The regime fears losing its control and the nation's culture to the ever-growing threat of outside influence, as is evidenced in the regime's reaction to the comedy film "The Interview". The regime has represented itself to its citizens as a powerful and capable entity and has used this status to control the populace. For this reason, the regime's leaders are forced to continually demonstrate this strength and power, or an illusion thereof, both domestically and globally, in order to maintain the status needed to ensure continued suppression of the population. This show of power may require that the regime takes chances and stretches beyond its abilities at times, but in the spirit of *juche* and *songun*, the regime will continue this façade, fearful of losing the image its leaders have worked so hard to maintain.

HP Security Research recommendations

North Korean cyber operations are not generally observed originating from home field IP address space, so geo-IP based blocking of traffic originating from those net-blocks is ineffective.

³⁹⁸ <http://www.apcss.org/Publications/Edited%20Volumes/BytesAndBullets/CH2.pdf>

³⁹⁹ <http://h30499.www3.hp.com/t5/HP-Security-Research-Blog/HPSR-Threat-Intelligence-Briefing-Episode-11/ba-p/6385243#U5HkbpRdV90>

⁴⁰⁰ <http://www.zdnet.com/south-korea-braces-for-norths-cyberattacks-7000012587/>

⁴⁰¹ <http://www.symantec.com/connect/blogs/four-years-darkseoul-cyberattacks-against-south-korea-continue-anniversary-korean-war>

Given that North Korea has capable and technically trained forces and will demonstrate their power when they feel provoked, western entities should consciously avoid promoting ideas or doctrine that is blatantly slanderous to the regime. Encouraging such ideas could cause those entities to become a focal point for North Korean cyber attacks.

Due to the fact that North Korean infrastructure is aging and its resources are not able to keep up with the rest of the world, entities with interesting R&D or IP (intellectual property) - especially military in nature – could become targets of interest for North Korea. Interest in defense-related IP and R&D could also stem from North Korea's relationship with China. In the Chinese business culture, taking another entity's IP or R&D is not stealing – it is accepted as business as usual. It is possible that North Korea, if under Chinese influence, would adopt the same attitude, given the regime's limited capacity for homegrown innovation.

Known DPRK targets have been limited primarily to South Korean and U.S. organizations and government entities. For these targets, prudent measures should include:

- Following traditional defense in depth approaches and security best practices
- Monitoring for malware that disables Korean language antivirus software, such as that from AhnLab
- To protect against the attack vectors used in North Korean malware campaigns, an advisable prevention tactic is to focus on hardening update/patch management systems. These systems are appealing targets due to the potential for a large impact

Appendix A – WHOIS records

WHOIS record for silibank.net:

Domain Name: silibank.net

Registry Domain ID:

Registrar WHOIS Server: whois.discount-domain.com

Registrar URL: http://www.onamae.com

Updated Date: 2014-03-11 17:27:55.0

Creation Date: 2006-03-13 13:14:53.0

Registrar Registration Expiration Date: 2015-03-13 03:14:53.0

Registrar: GMO INTERNET, INC.

Registrar IANA ID: 49

Registrar Abuse Contact Email: abuse@gmo.jp

Registrar Abuse Contact Phone:

Domain Status: ACTIVE

Registry Registrant ID:

Registrant Name: Whois Privacy Protection Service by MuuMuuDomain

Registrant Organization: Whois Privacy Protection Service by MuuMuuDomain

Registrant Street1: 2-7-21 Tenjin Chuo-ku

Registrant Street2: Tenjin Prime 8F

Registrant City: Fukuoka-shi

Registrant State/Province: Fukuoka

Registrant Postal Code: 810-0001

Registrant Country: **JP**

Registrant Phone: 81-927137999

Registrant Phone Ext:

Registrant Fax: 81-927137944

Registrant Fax Ext:

Registrant Email: privacy@whoisprivacyprotection.info

Registry Admin ID:

Admin Name: Whois Privacy Protection Service by MuuMuuDomain

Admin Organization: Whois Privacy Protection Service by MuuMuuDomain

Admin Street1: 2-7-21 Tenjin Chuo-ku

Admin Street2: Tenjin Prime 8F

Admin City: Fukuoka-shi

Admin State/Province: Fukuoka

Admin Postal Code: 810-0001

Admin Country: JP

Admin Phone: 81-927137999

Admin Phone Ext:

Admin Fax: 81-927137944

Admin Fax Ext:

Admin Email: privacy@whoisprivacyprotection.info

Registry Tech ID:

Tech Name: Whois Privacy Protection Service by MuuMuuDomain
Tech Organization: Whois Privacy Protection Service by MuuMuuDomain
Tech Street1: 2-7-21 Tenjin Chuo-ku
Tech Street2: Tenjin Prime 8F
Tech City: Fukuoka-shi
Tech State/Province: Fukuoka
Tech Postal Code: 810-0001
Tech Country: JP
Tech Phone: 81-927137999
Tech Phone Ext:
Tech Fax: 81-927137944
Tech Fax Ext:
Tech Email: privacy@whoisprivacyprotection.info
Name Server: ns1.dns.ne.jp
Name Server: ns2.dns.ne.jp

WHOIS Record for kcna.kp:

inetnum: 175.45.176.0 - 175.45.179.255
netname: STAR-KP
descr: Ryugyong-dong
descr: Potong-gang District
country: KP
admin-c: SJVC1-AP
tech-c: SJVC1-AP
status: ALLOCATED PORTABLE
mnt-by: APNIC-HM
mnt-lower: MAINT-STAR-KP
mnt-routes: MAINT-STAR-KP
remarks: -+-+-+
remarks: This object can only be updated by APNIC hostmasters.
remarks: To update this object, please contact APNIC
remarks: hostmasters and include your organisation's account
remarks: name in the subject line.
remarks: -+-+-+
mnt-irt: IRT-STAR-KP
changed: hm-changed@apnic.net 20091221
source: APNIC
irt: IRT-STAR-KP
address: Ryugyong-dong Potong-gang District
e-mail: sahayod@loxley.co.th
abuse-mailbox: sahayod@loxley.co.th
admin-c: SJVC1-AP
tech-c: SJVC1-AP
auth: # Filtered

mnt-by: MAINT-STAR-KP
changed: sahayod@loxley.co.th 20120202
source: APNIC
role: STAR JOINT VENTURE CO LTD - network administrat
address: Ryugyong-dong Potong-gang District
country: KP
phone: +66 81 208 7602
fax-no: +66 2 240 3180
e-mail: sahayod@loxley.co.th
admin-c: SJVC1-AP
tech-c: SJVC1-AP
nic-hdl: SJVC1-AP
mnt-by: MAINT-STAR-KP
changed: hm-changed@apnic.net 20091214
source: APNIC

WHOIS Record for rodong.rep.kp:

inetnum: 175.45.176.0 - 175.45.179.255
netname: STAR-KP
descr: Ryugyong-dong
descr: Potong-gang District
country: KP
admin-c: SJVC1-AP
tech-c: SJVC1-AP
status: ALLOCATED PORTABLE
mnt-by: APNIC-HM
mnt-lower: MAINT-STAR-KP
mnt-routes: MAINT-STAR-KP
remarks: -+-+-+-+-+-+-+
remarks: This object can only be updated by APNIC hostmasters.
remarks: To update this object, please contact APNIC
remarks: hostmasters and include your organisation's account
remarks: name in the subject line.
remarks: -+-+-+-+-+-+-+
mnt-irt: IRT-STAR-KP
changed: hm-changed@apnic.net 20091221
source: APNIC
irt: IRT-STAR-KP
address: Ryugyong-dong Potong-gang District
e-mail: sahayod@loxley.co.th
abuse-mailbox: sahayod@loxley.co.th
admin-c: SJVC1-AP
tech-c: SJVC1-AP
auth: # Filtered

mnt-by: MAINT-STAR-KP
changed: sahayod@loxley.co.th 20120202
source: APNIC
role: STAR JOINT VENTURE CO LTD - network administrat
address: Ryugyong-dong Potong-gang District
country: KP
phone: +66 81 208 7602
fax-no: +66 2 240 3180
e-mail: sahayod@loxley.co.th
admin-c: SJVC1-AP
tech-c: SJVC1-AP
nic-hdl: SJVC1-AP
mnt-by: MAINT-STAR-KP
changed: hm-changed@apnic.net 20091214
source: APNIC

WHOIS Record for uriminzokkiri.com:

Domain Name : uriminzokkiri.com
PunnyCode : uriminzokkiri.com
Creation Date : 2003-02-09 00:00:00
Updated Date : 2012-06-28 13:22:18
Expiration Date : 2015-02-09 00:00:00
Registrant:
Organization : chaoxianLiuYiYuBianJishe ShenYang Ban SHICHU
Name : Korea 615 Shenyang company
Address : shenyang hepingqu xifudalu 168 hao 2 danyuan 2-12-1
City : shenyangshi
Province/State : liaoningsheng
Country : china
Postal Code : 123456
Administrative Contact:
Name : kim sejun
Organization : Shenyang xin neng yuang
Address : shenyang hepingqu xifudalu 168 hao 2 danyuan 2-12-1
City : shenyangshi
Province/State : liaoningsheng
Country : china
Postal Code : 123456
Phone Number :
Fax : 86-024-22523102
Email : hyk1979@hotmail.com
Technical Contact: Name : kim sejun
Organization : Shenyang xin neng yuang
Address : shenyang hepingqu xifudalu 168 hao 2 danyuan 2-12-1

City : shenyangshi
Province/State : liaoningsheng
Country : china
Postal Code : 123456
Phone Number :
Fax : 86-024-22523102
Email : hyk1979@hotmail.com
Billing Contact:
Name : kim sejun
Organization : Shenyang xin neng yuang
Address : shenyang hepingqu xifudalu 168 hao 2 danyuan 2-12-1
City : shenyangshi
Province/State : liaoningsheng
Country : china
Postal Code : 123456
Phone Number :
Fax : 86-024-22523102
Email : hyk1979@hotmail.com

WHOIS Record for ournation-school.com:

Domain Name: ournation-school.com
Registry Domain ID:
Registrar WHOIS Server:whois.paycenter.com.cn
Registrar URL:<http://www.xinnet.com>
Updated Date:2012-06-28 13:22:20
Creation Date:2004-10-29 00:00:00
Registrar Registration Expiration Date:2014-10-29 00:00:00
Registrar:XINNET TECHNOLOGY CORPORATION
Registrar IANA ID:120
Registrar Abuse Contact Email: supervision@xinnet.com
Registrar Abuse Contact Phone:+86.1087128064
Domain Status:
Registry Registrant ID:
Registrant Name:Korea 615 Shenyang company
Registrant Organization:chaoxian liuyiyubianjishe shenyangbanshichu
Registrant Street:shenyang hepingqu xifudalu 168 hao 2 danyuan 2-12-1
Registrant City:shenyangshi
Registrant State/Province:liaoningsheng
Registrant Postal Code:123456
Registrant Country:China
Registrant Phone:+86.024 22523102
Registrant Phone Ext:
Registrant Fax:+86.024 22523102
Registrant Fax Ext:

Registrant Email:urimanager@silibank.com
Registry Admin ID:
Admin Name:Korea 615 Shenyang company
Admin Organization:Korea 615 Shenyang company
Admin Street:shenyang hepingqu xifudalu 615 hao 2 danyuan 6-1-5
Admin City:shenyangshi
Admin State/Province:liaoningsheng
Admin PostalCode:123456
Admin Country:China
Admin Phone:+86.024 22523102
Admin Phone Ext:
Admin Fax:+86.024 22523102
Admin Fax Ext:
Admin Email:urimanager@silibank.com
Registry Tech ID:
Tech Name:Korea 615 Shenyang company
Tech Organization:Korea 615 Shenyang company
Tech Street:shenyang hepingqu xifudalu 615 hao 2 danyuan 6-1-5
Tech City:shenyangshi
Tech State/Province:liaoningsheng
Tech PostalCode:123456
Tech Country:China
Tech Phone:+86.024 22523102
Tech Phone Ext:
Tech Fax:+86.024 22523102
Tech Fax Ext:
Tech Email:urimanager@silibank.com
Name Server:ns13.xincache.com
Name Server:ns14.xincache.com
DNSSEC:unsigned

WHOIS Record for chongryon.com:

Domain Name: chongryon.com
Registry Domain ID: 69711868_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.melbourneit.com
Registrar URL: http://www.melbourneit.com.au
Updated Date: 2014-03-26T00:31:24Z
Creation Date: 2001-04-20T06:45:46Z
Registrar Registration Expiration Date: 2015-04-20T06:45:46Z
Registrar: Melbourne IT Ltd
Registrar IANA ID: 13
Registrar Abuse Contact Email: abuse@melbourneit.com.au
Registrar Abuse Contact Phone: +61.386242300
Domain Status: ok

Registry Registrant ID:

Registrant Name: o guanin

Registrant Organization: o guanin

Registrant Street: "hujimi2-14-15,"

Registrant City: chiyodaku

Registrant State/Province: tokyo

Registrant Postal Code: 1028138

Registrant Country: JP

Registrant Phone: +81.332627111

Registrant Phone Ext:

Registrant Fax:

Registrant Fax Ext:

Registrant Email: park2@mac.com

Registry Admin ID:

Admin Name: guanin o

Admin Organization:

Admin Street: "hujimi2-14-15,"

Admin City: chiyodaku

Admin State/Province: tokyo

Admin Postal Code: 1028138

Admin Country: JP

Admin Phone: +81.332627111

Admin Phone Ext:

Admin Fax:

Admin Fax Ext:

Admin Email: park2@mac.com

Registry Tech ID:

Tech Name: Link Club

Tech Organization: Link Club

Tech Street: 5-39-6 Jingumae Shibuya-ku

Tech City: TOKYO

Tech State/Province: 150-0001

Tech Postal Code: JP

Tech Country: JP

Tech Phone: +81.462643403

Tech Phone Ext:

Tech Fax:

Tech Fax Ext:

Tech Email: mel-tech@hosting-link.ne.jp

Name Server: USR-NS1.LINKCLUB.JP

Name Server: USR-NS2.LINKCLUB.JP

DNSSEC: unsigned

URL of the ICANN WHOIS Data Problem Reporting System: <http://wdrprs.internic.net>

>>> Last update of WHOIS database: 2014-05-13T18:15:18Z

WHOIS Record for korea-np.co.jp:

Domain Information: [B%I%a%\$%s>pJs]

a. [B%I%a%\$%sL>] **KOREA-NP.CO.JP**
e. [B\$=\$7\$-\$a\$\$] B\$+\$V\$7\$-\$,\$\$\$7\$c B\$A\$g\$&\$;\$s\$7\$s\$]\$&\$7\$c
f. [BAH?%L>] B3t<02q<R BD+A/?7Js<R
g. [Organization] The Choson Shinbo Company Inc.
k. [BAH?%<oJL] B3t<02q<R
l. [Organization Type] CO
m. [BEPO?C4Ev<T] YK18923JP
n. [B5;=QO"MmC4Ev<T] YK18923JP
p. [B%M!<%`%5!<%P] uns01.usen.ad.jp
p. [B%M!<%`%5!<%P] uns02.usen.ad.jp
s. [B=pL>80]
[B>uBV] Connected (2015/02/28)
[BEPO?G/7nF[]] 1997/02/14
[B@\B3G/7nF[]] 1997/06/03
[B:G=*99?7] 2014/03/01 01:16:34 (JST)

Appendix B – Sites found on North Korean IP space

smtp.star-co.net.kp	175.45.176.10
smtp.start-di.net.kp	175.45.176.10
spinef1.star.net.kp	175.45.176.10
spinef2.star.net.kp	175.45.176.11
ns1.co.kp	175.45.176.15
ns1.com.kp	175.45.176.15
ns1.edu.kp	175.45.176.15
ns1.gov.kp	175.45.176.15
ns1.kptc.kp	175.45.176.15
ns1.kptc.kp	175.45.176.15
ns1.net.kp	175.45.176.15
ns1.org.kp	175.45.176.15
ns1.org.kp	175.45.176.15
ns1.rep.kp	175.45.176.15
ns2.co.kp	175.45.176.16
ns2.com.kp	175.45.176.16
ns2.edu.kp	175.45.176.16
ns2.gov.kp	175.45.176.16
ns2.kptc.kp	175.45.176.16
ns2.kptc.kp	175.45.176.16
ns2.net.kp	175.45.176.16
ns2.org.kp	175.45.176.16
ns2.rep.kp	175.45.176.16
friend.com.kp	175.45.176.39
friend.com.kp	175.45.176.67
gnu.rep.kp	175.45.176.67
koredfund.org.kp	175.45.176.67
korelcfund.org.kp	175.45.176.67
ksf.com.kp	175.45.176.67
naenara.com.kp	175.45.176.67
vok.rep.kp	175.45.176.67
rodong.rep.kp	175.45.176.68

airkoryo.com.kp	175.45.176.69
spwebh2.star.net.kp	175.45.176.7
mail.silibank.net.kp	175.45.176.70
kcna.kp	175.45.176.71
gnu.rep.kp	175.45.176.73
vok.rep.kp	175.45.176.75
friend.com.kp	175.45.176.8
korelcfund.org.kp	175.45.176.8
ns1.cooks.org.kp	175.45.176.8
ns1.friend.com.kp	175.45.176.8
ns1.gnu.rep.kp	175.45.176.8
ns1.kcna.kp	175.45.176.8
ns1.koredfund.org.kp	175.45.176.8
ns1.korelcfund.org.kp	175.45.176.8
ns1.korfilm.com.kp	175.45.176.8
ns1.ksf.com.kp	175.45.176.8
ns1.naenara.com.kp	175.45.176.8
ns1.rodong.rep.kp	175.45.176.8
ns1.silibank.net.kp	175.45.176.8
ns1.star-co.net.kp	175.45.176.8
ns1.star-di.net.kp	175.45.176.8
ns1.star.net.kp	175.45.176.8
ns1.vok.rep.kp	175.45.176.8
ns2.airkoryo.com.kp	175.45.176.8
friend.com.kp	175.45.176.9
gnu.rep.kp	175.45.176.9
koredfund.org.kp	175.45.176.9
korelcfund.org.kp	175.45.176.9
ns2.airkoryo.com.kp	175.45.176.9
ns2.cooks.org.kp	175.45.176.9
ns2.friend.com.kp	175.45.176.9
ns2.gnu.rep.kp	175.45.176.9

ns2.kcna.kp	175.45.176.9
ns2.koredfund.org.kp	175.45.176.9
ns2.korelcfund.org.kp	175.45.176.9
ns2.korfilm.com.kp	175.45.176.9
ns2.ksf.com.kp	175.45.176.9
ns2.naenara.com.kp	175.45.176.9
ns2.rodong.rep.kp	175.45.176.9
ns2.silibank.rep.kp	175.45.176.9
ns2.star-co.net.kp	175.45.176.9
ns2.star-di.net.kp	175.45.176.9
ns2.star.net.kp	175.45.176.9
ns2.vok.rep.kp	175.45.176.9
vok.rep.kp	175.45.176.9
gnu.rep.kp	175.45.177.73
vok.rep.kp	175.45.177.75

friend.com.kp	175.45.177.77
koredfund.org.kp	175.45.177.77
korelcfund.org.kp	175.45.177.77
naenara.com.kp	175.45.177.77
vok.rep.kp	175.45.177.77
mail.chosunexpo.com	175.45.178.101
ns3.kptc.kp	175.45.178.173
ns3.kptc.kp	175.45.178.173
ns1.knic.com.kp	175.45.178.8
ns1.knic.com.kp	175.45.178.8
ns1.star.edu.kp	175.45.179.66
ns1.star.edu.kp	175.45.179.66
email.kp.col.cn	175.45.179.67
mail.star.edu.kp	175.45.179.69

Appendix C – Analysis of DarkSeoul Dropper

Dropper

MD5: 9263e40d9823aecf9388b64de34eae54

Also known as/detected as :

- Dropper-FDH (McAfee)
- Trojan:Win32/Dembr.A (Microsoft)
- Trojan.Jokra (Symantec)

The dropper component that we examined was distributed as a UPX-packed binary.

Installation

When executed it creates the following files in the affected user's %Temp% directory:

- alg.exe: A legitimate binary used to open SSH connections with remote servers
MD5 e45cd9052dd3dd502685dfd9aa2575ca
Size: 166,912 bytes
- conime.exe: A legitimate binary used to open SSH connections with remote servers
MD5: 6a702342e8d9911bde134129542a045b
Size: 153,600 bytes
- ~pr1.tmp: Payload - A destructive bash script
MD5: dc789dee20087c5e1552804492b042cd
Size: 1,186 bytes
Also known as/detected as:
 - KillMBR-FBIA (McAfee)
 - Trojan:SH/Kofornix.A (Microsoft)
 - Trojan.Jokra (Symantec)
- AgentBase.exe: Payload - Win32 wiper component (see details below)
MD5: db4bbdc36a78a8807ad9b15a562515c4
Size: 24,576

Payload—attempts to connect to remote servers and upload a destructive bash script

After determining the location of user profile directories on the affected computer, the malware searches these directories for configuration files and directories that may be associated with the connection manager clients mRemote and SecureCRT.

- mRemote—an open source tool for centrally managing remote server connections using a GUI (Kevin Kline, 2008).⁶⁹ This tool is no longer being actively developed or supported.
- SecureCRT—a commercial SSH and Telnet client by VanDyke Software.

If an mRemote installation is located, the dropper reads the configuration file and checks if there's a NODE that is defined with "Username=root", "Protocol=SSH", and a password that is not blank. If

those conditions are satisfied it extracts the information. The password is decrypted after being extracted.

If a SecureCRT installation is located, the dropper extracts information from sessions that have Username=root, Protocol=SSH and a saved password. If these conditions are satisfied, the username, hostname, port, and password are extracted. The password is then decrypted.

After extracting these connection and server details, the dropper uses the previously dropped alg.exe and conime.exe to attempt to connect remote servers, upload and run the bash script ~pr1.tmp.

The bash script initially checks which UNIX it is running on (of HP-UX, SunOS, Linux, or AIX) and then attempts to wipe the /kernel, /usr /etc and /home directories, thus rendering the machine inoperative.

Win32 Wiper component

When the AgentBase.exe component is executed, it first attempts to stop the following processes, presumably in order to evade detection:

- pasvc.exe – policy agent from AhnLab
- clisvc.exe – ViRobot ISMS from Hauri

It then enumerates all physical drives and overwrites the first 512 bytes with the string: “princpes”, effectively destroying the MBR (master boot record) of the affected drive.

It continues to look for removable and fixed drives, locates the root directory on these drives, and then attempts to delete all files and folders in this directory.

Finally, the affected computer is shut down and rebooted, although if the wiping mechanisms were successful then the machine will not be able to boot.

Learn more at

hp.com/go/hpsr