NOTRH KOREA, DAVID OF THE CYBER WORLD

Maj Gen P K Mallick, VSM (Retd)

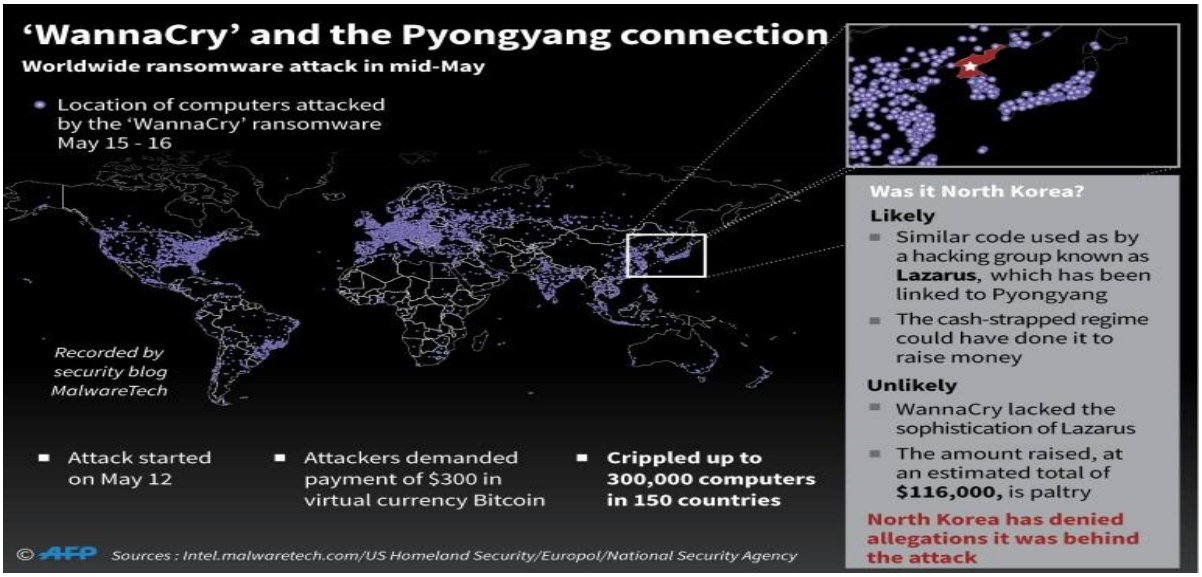
In 2004 I went to deliver a talk and chair a session on Cyber War at College of Defence Management, Secunderabad. After the session one of the participant officers of Higher Defence Management Course who was doing his dissertation on a relevant topic engaged me in a discussion that North Korea has no internet connection and how do they do business. My answer that in today's world no country can afford to have complete disconnect seemed not to satisfy him. Of course Sony happened later. Now Russia is providing them with internet connectivity when others have blocked.

Here is a take on North Korea's Cyber capabilities.

According to Kaspersky, the malware was the work of Lazarus, "an umbrella name that typically describes hacking activity which advances Pyongyang's interests".

Frequently, senior political leaders, cyber security professionals, and diplomats describe North Korean leaders or their respective actions as "crazy," "erratic," or "not rational." This is not the case. When examined through the lens of North Korean military strategy, national goals, and security perceptions, cyber activities correspond to their larger approach. North Korean cyber actors are not crazy or irrational: they just have a wider operational scope than most other intelligence services.

And just as Western analysts once scoffed at the potential of the North's nuclear program, so did experts dismiss its cyber potential — only to now acknowledge that hacking is an almost perfect weapon for a Pyongyang that is isolated and has little to lose. The country's primitive infrastructure is far less vulnerable to cyber retaliation. North Korean hackers operate outside the country, anyway. Sanctions offer no useful response, since a raft of sanctions are already imposed. And Mr. Kim's advisers are betting that no one will respond to a cyber attack with a military attack, for fear of a catastrophic escalation between North and South Korea.



North Korea is emerging as a significant actor in cyberspace with both its clandestine and military organizations gaining the ability to conduct cyber operations. Cyber attacks in South Korea and the United States have recently been associated with North Korea. The U.S. and Republic of Korea (ROK) governments attribute recent incidents, including the November 2014 attack against Sony Pictures Entertainment and the March 2013 attacks against South Korean banks and media agencies, respectively, to North Korea. These attacks have shown that the country is capable of conducting damaging and disruptive cyber attacks during peacetime. North Korea seems heavily invested in growing and developing its cyber capabilities for both political and military purposes.

As per the 2016 University of Washington study succinctly summarizes North Korea's asymmetric military strategy: Since the end of the Korean War, North Korea has developed an asymmetric military strategy, weapons, and strength because its conventional military power is far weaker than that of the U.S. and South Korea. Thus, North Korea has developed three military strategic pillars: surprise attack; quick decisive war; mixed tactics. First, its surprise attack strategy refers to attacking the enemy at an unexpected time and place. Second, its quick decisive war strategy is to defeat the South Korean military before the U.S. military or international community could intervene. Lastly, its mixed tactics strategy is to use multiple tactics at the same time to achieve its strategic goal.

Despite their near constant tirade of bellicose rhetoric and professions of strength, North Korea fundamentally views the world from a position of weakness and has developed a national strategy that utilizes its comparative strengths — complete control over a population of 25 million people and unflinching devotion to the Kim hereditary dynasty.

In this context, criminality, terrorism, and destructive cyber attacks all fit within the North Korean asymmetric military strategy which emphasizes surprise attacks and mixed tactics. The criminality and cyber attacks also have the added bonus of enabling North Korea to undermine the very international economic and political systems that constrain and punish it.

North Korea has relied on various asymmetric and irregular means to sidestep the conventional military deadlock on the peninsula while also preparing these means for use should a war break out. Cyber capabilities provide another means of exploiting U.S. and ROK vulnerabilities at relatively low intensity while minimizing risk of retaliation or escalation. In this context, cyber capabilities are logical extensions of both North Korea's peacetime and wartime operations

Cyber Capabilities and Asymmetric Strategy. North Korea sees cyber operations as a relatively low-cost and low risk means of targeting the vulnerabilities of a state that relies heavily on cyberspace for national and military activity. Disruptive or destructive cyber attacks allow for direct power projection against a distant adversary without physical infiltration or attack. Cyber capabilities are also an effective means to severely disrupt or neutralize the benefits of having a networked military. Issues of attribution and the lack of firmly established norms make it hard for the defender to communicate red lines and threats.

North Korea's Cyber Strategy. Cyber operations should be thought of as an extension of North Korea's broader national strategy. During peacetime, cyber capabilities allow the DPRK to upset the status quo with little risk of retaliation or immediate operational risk. During wartime, the DPRK would target U.S. and ROK command, control, communications, computers, intelligence, surveillance, and reconnaissance (C4ISR) in support of the DPRK's "quick war, quick end" strategy. North Korean cyber doctrine, if one exists, may be premised on the idea that an extensively networked military is vulnerable to cyber capabilities.

North Korea began identifying promising students at an early age for special training, sending many to China's top computer science programs. In the late 1990s, the Federal Bureau of Investigation's counterintelligence division noticed that North Koreans assigned to work at the United Nations were also quietly enrolling in university computer programming courses in New York.

"Cyber is a tailor-made instrument of power for them," said Chris Inglis, a former deputy director of the National Security Agency, who now teaches about security at the United States Naval Academy. "There's a low cost of entry, it's largely asymmetrical, there's some degree of anonymity and stealth in its use. It can hold large swaths of nation state infrastructure and private-sector infrastructure at risk. It's a source of income." Mr. Inglis, speaking at the Cambridge Cyber Summit added: "You could argue that they have one of the most successful cyber programs on the planet, not because it's technically sophisticated, but because it has achieved all of their aims at very low cost."

From Minor Leaguers to Serious Hackers

Kim Jong-il, the father of the current dictator and the initiator of North Korea's cyber operations, was a movie lover who became an internet enthusiast, a luxury reserved for the country's elite. When Mr. Kim died in 2011, the country was estimated to have 1,024 IP addresses, fewer than on most New York City blocks. Mr. Kim, like the Chinese, initially saw the internet as a threat to his regime's ironclad control over information. But his attitude began to change in the early 1990s, after a group of North Korean computer scientists returned from travel abroad proposing to use the web to spy on and attack enemies like the United States and South Korea, according to defectors.

North Korea began identifying promising students at an early age for special training, sending many to China's top computer science programs. "The North's cyber warfare unit gained priority after the 2003 invasion of Iraq by the United States. After watching the American "shock and awe" campaign on CNN, Kim Jong-il issued a warning to his military: "If warfare was about bullets and oil until now," he told top commanders, warfare in the 21st century is about information."

When Kim Jong-un succeeded his father, in 2011, he expanded the cyber mission beyond serving as just a weapon of war, focusing also on theft, harassment and political-score settling. "Cyber warfare, along with nuclear weapons and missiles, is an 'all-purpose sword' that guarantees our military's capability to strike relentlessly," Kim Jong-un reportedly declared

“We’re already sanctioning anything and everything we can,” said Robert P. Silvers, the former assistant secretary for cyber policy at the Department of Homeland Security during the Obama administration. “They’re already the most isolated nation in the world.” By 2012, government officials and private researchers say North Korea had dispersed its hacking teams abroad, relying principally on China’s internet infrastructure. This allowed the North to exploit largely non secure internet connections and maintain a degree of plausible deniability.

The Organization of DPRK’s Cyber Operations

North Korea’s cyber operations are not ad hoc, isolated incidents. They are the result of deliberate and organized efforts under the direction of preexisting organizations with established goals and missions that directly support the country’s national strategy. Knowing which North Korean organizations plan and execute cyber operations is important because North Korea does not publish its own cyber strategy or doctrine. Examining an organization’s historic goals and missions as well as analyzing their known patterns of behavior are the next best option for predicting how North Korea will operationalize cyber capabilities. A top-down perspective on North Korea’s cyber operations shows which organizations conduct cyber operations and how strongly they influence operational purposes. The Reconnaissance General Bureau and the General Staff Department of the KPA generally control most of North Korea’s known cyber capabilities. These two organizations are responsible for peacetime provocations and wartime disruptive operations, respectively.

The Reconnaissance General Bureau: The RGB is the primary intelligence and clandestine operations organ known within the North Korean government and is historically associated with peacetime commando raids, infiltrations, disruptions and other clandestine operations, including the 2014 Sony Pictures Entertainment attack. The RGB controls the bulk of known DPRK cyber capabilities, mainly under Bureau 121 or its potential successor, the Cyber Warfare Guidance Bureau. There may be a recent or ongoing reorganization within the RGB that promoted Bureau 121 to a higher rank or even established it as the centralized entity for cyber operations. RGB cyber capabilities are likely to be in direct support of the RGB’s aforementioned missions. In peacetime, it is also likely to be the more important or active of the two main organizations with cyber capabilities in the DPRK.

The General Staff Department (GSD): The General Staff Department of the KPA oversees military operations and units, including the DPRK’s growing conventional military cyber capabilities. It is tasked with operational planning and ensuring the readiness of the KPA should war break out on the Korean peninsula. It is not currently associated with direct cyber provocations in the same way that the RGB is, but its cyber units may be tasked with preparing disruptive attacks and cyber operations in support of conventional military operations. North Korea’s emphasis on combined arms and mixed operations suggests that cyber units will coordinate with or be incorporated as elements within larger conventional military formations.

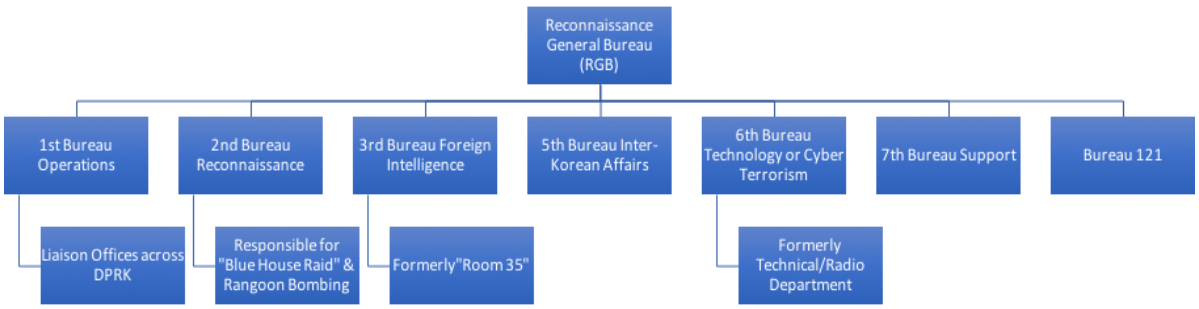
North Korea’s Technology Base: The DPRK maintains an information technology base that can serve as a general research and development foundation for computer technology and programming. The existence of a software and computer industry means the DPRK’s technical industries are not as primitive as many think.

The Reconnaissance General Bureau (RGB), also known as “Unit 586,” was formed in 2009 after a large restructure of several state, military, and party intelligence elements. It has since emerged as not just the dominant North Korean foreign intelligence service, but also the center for clandestine operations.

As North Korea’s lead for clandestine operations, the RGB is also likely the primary cyber operations organization as well. As described by the Center for Strategic and International Studies in 2015 report:

For the RGB to be in control of cyber assets indicates that the DPRK intends to use these assets for provocative purposes. The RGB probably consists of seven bureaus; six original bureaus and a new seventh (Bureau 121) that was likely added sometime after 2013.

RGB organizational chart, compiled with information from The Korea Herald, 38 North, and CSIS.



Bureau 121 is probably North Korea’s primary cyber operations unit, but there are other units within the KPA and KWP that may also conduct cyber operations.

Lazarus Group, now known to be North Korean state-sponsored actors, have been conducting operations since at least 2009, with a DDoS attack on U.S. and South Korean websites using the MYDOOM worm. Until late 2015, Lazarus Group cyber activities primarily focused on South Korean and U.S. government and financial organizations, including destructive attacks on South Korean banking and media sectors in 2013 and highly publicized attack on Sony Pictures Entertainment in 2014.

North Korean Cyber Activities

Sony Cyber Attack. North Korea’s most famous cyber attack came in 2014, against Sony Pictures Entertainment, in a largely successful effort to block the release of a movie that satirized Mr. Kim. In August 2014, North Korean hackers went after a British broadcaster, Channel Four, which had announced plans for a television series about a British nuclear scientist kidnapped in Pyongyang.

First, the North Koreans protested to the British government. “A scandalous farce,” North Korea called the series. When that was ignored, British authorities found that

the North had hacked into the television network's computer system. The attack was stopped before inflicting any damage, and David Abraham, the chief executive of Channel Four, initially vowed to continue the production.

That attack, however, was just a prelude. When Sony Pictures Entertainment released a trailer for "The Interview," Pyongyang wrote a letter of complaint to the secretary general of the United Nations to stop the production. Then came threats to Sony. In September 2014, while still attempting to crack Channel 4, North Korean hackers buried deep into Sony's networks, lurking patiently for the next three months, as both Sony and American intelligence completely missed their presence. On Nov. 24, the attack on Sony began: Employees arriving at work that day found their computer screens taken over by a picture of a red skeleton with a message signed "GOP," for "Guardians of Peace."

"We've obtained all your internal data including your secrets and top secrets," the message said. "If you don't obey us, we'll release data shown below to the world." That was actually a diversion: The code destroyed 70 percent of Sony Pictures' laptops and computers. Sony employees were reduced to communicating via pen, paper and phone.

Sony struggled to distribute the film as theaters were intimidated. In London, outside investors in Channel Four's North Korea project suddenly dried up, and the project effectively died. The Obama White House responded to the Sony hack with sanctions that the North barely noticed, but with no other retaliation.

Stealing of Operational Plan of South Korea.

North Korean hackers stole a huge trove of classified U.S. and South Korean military documents last year, including a plan to "decapitate" the leadership in Pyongyang in the event of war. North Korean hackers broke into the Defense Integrated Data Center in September last year to steal secret files, including American and South Korean "operational plans" for wartime action. The data center is the main headquarters of South Korea's defense network. The stolen documents included OPLAN 5015, a plan drafted two years ago for dealing with full-blown war with North Korea and said to include procedures to "decapitate" the North Korean leadership. The cache also included OPLAN 3100, outlining the military response to infiltration by North Korean commandos or another local provocation, as well as a contingency plan in case of a sudden change in North Korea. Yonhap News Agency reported that the hackers took 235 gigabytes of military documents and that almost 80 percent of the stolen documents have not yet been identified. The documents also included reports on key South Korean and U.S. military personnel, the minutes of meetings about South Korean-U.S. military drills, and data on military installations and power plants in South Korea, reported the Chosun Ilbo, South Korea's largest newspaper. In May, the Defense Ministry disclosed that the South Korean military's intranet had been hacked by people "presumed to be North Koreans." But the military said that only 53 gigabytes of information were stolen, and it did not reveal what was included. The previous month, reports emerged that North Korean hackers had broken into the Defense Ministry network and infected more than 3,000 computers, including the defense minister's, with malware. At the time, South Korean newspapers, quoting unnamed government officials, reported that parts of one operational plan, OPLAN

5027, which outlines troop deployment plans and key North Korean targets, were stolen.

Information War

North Korea was potentially behind phony evacuation messages sent via cell phones and social media to military families and defense personnel in South Korea last month. That incident opens the possibility that last year's breach may have led to the harvest of personal information used for the notifications.

This is hardly the first time that Kim's regime has been accused of cyber attacks. The country's spy agency, the Reconnaissance General Bureau, is thought to have assembled a large cyber army, assumed to be based in China, to launch such hacks.

North Korea Hacks South Korean Warship Blueprints

North Korea stole blueprints of missile-equipped ships and unspecified submarines in a heist last year of classified documents from the world's biggest shipbuilder. About 60 classified military documents were among the 40,000 hacked from South Korea's Daewoo Shipbuilding and Marine Engineering Co in April 2016. They included information on construction technology, blueprints, weapons systems and evaluations of the ships and submarines. South Korea's Aegis-equipped ships and submarines are key to plans for a preemptive strike against North Korea should it send a submarine equipped with ballistic missiles to target key facilities in the South.

Information War

North Korea is emerging as a significant actor in cyberspace with both its clandestine and military organizations gaining the ability to conduct cyber operations. These attacks have shown that the country is capable of conducting damaging and disruptive cyber attacks during peacetime. North Korea seems heavily invested in growing and developing its cyber capabilities for both political and military purposes

North Korea was potentially behind phony evacuation messages sent via cell phones and social media to military families and defense personnel in South Korea last month. That incident opens the possibility that last year's breach may have led to the harvest of personal information used for the notifications.

Financial Domain

The attacks on the Bangladesh Central Bank, additional banks around the world, and the WannaCry ransomware campaign represent a new phase in North Korean cyber operations, one that mirrors the phases of violence and criminality North Korea has passed through over the past 50 years. Unlike its weapons tests, which have led to international sanctions, the North's cyber strikes have faced almost no pushback or punishment, even as the regime is already using its hacking capabilities for actual attacks against its adversaries in the West. Soon the digital bank heists began — an attack in the Philippines in October 2015; then the Tien Phong Bank in Vietnam at the end of the same year; and then the Bangladesh Central Bank. Researchers at

Symantec said it was the first time a state had used a cyber attack not for espionage or war, but to finance the country's operations.

Now, the attacks are increasingly cunning. Security experts noticed in February that the website of Poland's financial regulator was unintentionally infecting visitors with malware. It turned out that visitors to the Polish regulator's website — employees from Polish banks, from the central banks of Brazil, Chile, Estonia, Mexico, Venezuela, and even from prominent Western banks like Bank of America — had been targeted with a so-called watering hole attack, in which North Korean hackers waited for their victims to visit the site, then installed malware in their machines. Forensics showed that the hackers had put together a list of internet addresses from 103 organizations, most of them banks, and designed their malware to specifically infect visitors from those banks, in what researchers said appeared to be an effort to move around stolen currency.

Bangladesh Central Bank. In early 2016, a new pattern of activity began to emerge in an unusual operation against the Bangladesh Central Bank. Actors obtained the legitimate Bangladesh Central Bank credentials for the SWIFT interbank messaging system and used them to attempt to transfer $951 million of the bank's funds to accounts around the world. A few simple errors by the actors about a withdrawal request that had misspelled "foundation" as "fandation." (and some pure luck) allowed central bankers to prevent the transfer of or recover most of the funds, but the attackers ended up getting away with nearly $81 million. The National Security Agency (NSA) has attributed this attack on the Bangladesh Central Bank to the North Korean state, however, the investigation within the U.S. government is still ongoing. Threat analysts from numerous companies have attributed this attack and subsequent attacks on banks around the world through early 2017 to the Lazarus Group (which DHS, FBI, and NSA have all linked to the North Korean government over the past three days).

RANSOMWARE. The most widespread hack was WannaCry, a global ransomware attack that used a program that cripples a computer and demands a ransom payment in exchange for unlocking the computer, or its data. The hackers based the attack on a secret tool, called "Eternal Blue," stolen from the National Security Agency. In the late afternoon of May 12, panicked phone calls flooded in from around Britain and the world. The computer systems of several major British hospital systems were shut down, forcing diversions of ambulances and the deferral of nonemergency surgeries. Banks and transportation systems across dozens of countries were affected.

Then only sheer luck enabled a 22-year-old British hacker to defuse, the ransomware attack. It ended thanks to Marcus Hutchins, a college dropout and self-taught hacker living with his parents in the southwest of England. He spotted a web address somewhere in the software and, on a lark, paid $10.69 to register it as a domain name. The activation of the domain name turned out to act as a kill switch causing the malware to stop spreading.

Britain's National Cyber Security Center had picked up no warning of the attack, said Paul Chichester, its director of operations. "This was part of an evolving effort to find ways to disable key industries," said Brian Lord, a former deputy director for

intelligence and cyber operations at the Government Communications Headquarters in Britain. “All I have to do is create a moderately disabling attack on a key part of the social infrastructure, and then watch the media sensationalize it and panic the public.”

According to a Washington Post report published on June 14, the NSA has compiled an intelligence assessment on the WannaCry campaign and has attributed the creation of the WannaCry worm to “cyber actors sponsored by” the RGB. This assessment, ascribed the April campaign as an “attempt to raise revenue for the regime.” British officials privately acknowledge that they know North Korea perpetrated the attack, but the government has taken no retaliatory action, uncertain what they can do. It is assessed that use of ransomware to raise funds for the state would fall under both North Korea’s asymmetric military strategy and ”self-financing” policy, and be within the broad operational remit of their intelligence services.

BITCOIN. North Korea is drenched in chronic economic problems, due to a one-sided focus on military spending and decades of economic sanctions from the international community. Under the U.N. sanctions imposed in August, China has banned imports on North Korea's iron, coal and seafood, which accounts for about 35 percent of North Korea's trading income. North Korea may be "mining" bitcoin as a way to get around the tighter sanctions. It also helps that bitcoin is an open and decentralized network, making "mining" a legal and relatively easy activity for anyone who has access to the internet. Ultimately, it's up to the international community and the bitcoin community to decide whether they're comfortable trading bitcoin with North Korea.

Recently, North Korean hackers’ fingerprints showed up in a series of attempted attacks on so-called crypto currency exchanges in South Korea, and were successful in at least one case, according to researchers at FireEye. The attacks on Bitcoin exchanges, which see hundreds of millions of dollars worth of Bitcoin exchanged a day, offered Pyongyang a potentially very lucrative source of new funds. Researchers say, there is evidence they have been exchanging Bitcoin gathered from their heists for Monero, a highly anonymous version of crypto currency that is far harder for global authorities to trace.

Any North Korean activity in bitcoin is likely a tiny fraction of global trade activity. The total trade volume of bitcoin was nearly $2 billion, according to CryptoCurrency Market Capitalizations. Bitcoin in itself is not criminal by any means; it's not a suspect activity. But the timing of that activity was an interesting correlation with the WannaCry [cyber]attack," The "mining" started five days after the cyber attack, which locked tens of thousands of computer and data files for ransom payments in bitcoin. The attack has also been attributed to North Korea by the U.S. National Security Agency.

"Mining" is a process of earning bitcoins. Miners use high-performance computers to solve complex mathematical problems and verify bitcoin transactions online. In return they are rewarded with bitcoins.

But who would be capable of pulling off such activity in the autocratic country? After all, most North Koreans have no access to the internet. Only a small minority of

users — university students, scientists and select government officials — have access to Kwangmyong, a domestic intranet "that offers email and websites but is totally shut off from the rest of the world," according to a Slate article.

"Only the most senior leaders and ruling elite are granted access to worldwide internet directly North Korean elites access internet primarily through three IP ranges, one of which is assigned by China Netcom.

[https://www.cnbc.com/2017/09/13/bitcoin-mining-a-new-way-for-north-korea-to-generate-funds-for-the-regime.html]

CASH. Once North Korea counterfeited crude $100 bills to try to generate hard cash. Now intelligence officials estimate that North Korea reaps hundreds of millions of dollars a year from ransomware, digital bank heists, online video game cracking, and more recently, hacks of South Korean Bitcoin exchanges.

One former British intelligence chief estimates the take from its cyber heists may bring the North as much as $1 billion a year, or a third of the value of the nation's exports.

Learning From Iran, Growing Bolder

For decades Iran and North Korea have shared missile technology, and American intelligence agencies have long sought evidence of secret cooperation in the nuclear arena. In cyber, the Iranians taught the North Koreans something important: When confronting an enemy that has internet-connected banks, trading systems, oil and water pipelines, dams, hospitals, and entire cities, the opportunities to wreak havoc are endless.

By midsummer 2012, Iran's hackers, still recovering from an American and Israeli-led cyber attack on Iran's nuclear enrichment operations, found an easy target in Saudi Aramco, Saudi Arabia's state owned oil company and the world's most valuable company.

Mar 13 Seven months later, during joint military exercises between American and South Korean forces, North Korean hackers, operating from computers inside China, deployed a very similar cyber weapon against computer networks at three major South Korean banks and South Korea's two largest broadcasters. Like Iran's Aramco attacks, the North Korean attacks on South Korean targets used wiping malware to eradicate data and paralyze their business operations. It may have been a copycat operation, but Mr. Hannigan, the former British official, said recently: "We have to assume they are getting help from the Iranians."

[https://www.nytimes.com/2017/10/15/world/asia/north-korea-hacking-cyber-sony.html]

Attribution. Attribution of specific cyber activity to the North Korean state or intelligence organizations is difficult, and up until recently, circumstantial. On June 12, US-CERT released a joint technical alert that summarized analysis conducted by the U.S. Department of Homeland Security (DHS) and FBI on the "tools and

infrastructure used by cyber actors of the North Korean government to target the media, aerospace, financial, and critical infrastructure sectors in the United States and globally."

This alert marked the first time the U.S. government linked threat actor groups and malware long-suspected to be utilized by North Korean state-sponsored actors with the with North Korean government itself. DHS and FBI explicitly identified two threat actor groups, Lazarus Group and Guardians of Peace, and three tools, Destover, Wild Positron/Duuzer, and Hangman, as used by the North Korean government. While the FBI and DHS identified many indicators of compromise, Yara rules, and network signatures, the report did not provide any evidence supporting the attribution to the North Korean government or details on which organization or unit might be responsible.

A recent analysis by the cyber security firm Recorded Future found heavy North Korean internet activity in India, Malaysia, New Zealand, Nepal, Kenya, Mozambique, and Indonesia. In some cases, like that of New Zealand, North Korean hackers were simply routing their attacks through the country's computers from abroad. In others, researchers believe they are now physically stationed in countries like India, where nearly one-fifth of Pyongyang's cyber attacks now originate.

North Korean Cyber Infrastructure

The North Koreans are getting the hang of "cyber operations". They're not as skilled yet as the Chinese and the Russians (not to mention the Americans), but they're making real progress. Who thought that a country with only about 1,000 internet addresses could inflict serious damage on a nuclear-tipped superpower would have been regarded as preposterous, nobody in Washington (or London) is laughing any longer.

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

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

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

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

American Publication Recorded Future Report

India has been second largest trading partner of North Korea after China As per the Directorate General of Foreign Trade, India's export to North Korea was $76.52 million and import stood at $132.53 million in 2014-15. While India largely exported oilmeals, cotton yarn and machinery, Pyongyang exported iron and steel. From $209.05 million, the bilateral came down $130.38 million in 2016-17.

India has been under pressure from USA to cut off all relations with North Korea. India has obliged halting all trade, except for food and medicine. However, India's embassy in Pyongyang with two diplomats will continue to function.

The USA has its own way of putting pressure. In a stunning report from the New York Times claimed that India serves as a base for North Korea's cyber warfare.

Citing a report by the Recorded Future, the American publication said nearly a fifth of the Pyongang's attacks originate from India. The report claims that most of North Korean cyber operations are carried out from foreign countries like India, Malaysia,

New Zealand, Nepal, Kenya, Mozambique, and Indonesia. While in some cases, the North Korean hackers route their attacks through their computers from abroad, in cases like that in India, hackers are physically stationed to carry out attacks. The report by Recorded Future also indicates that India, despite serving as a base for North Korea's cyberwar, also remains at a potential threat from similar attacks.

It is interesting to see what the report from Recorded Future, a CIA Funded organization, says. In the open domain there has not been much rebuttal from the Government of India side. You can view the report here.

[https://www.recordedfuture.com/north-korea-internet-activity/]

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

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

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

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

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

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

It has been widely reported that North Korea has a physical presence to conduct cyber operations in China, including co-owning a hotel in Shenyang with the Chinese from which North Korea conduct malicious cyber activity. Nearly 10 percent of all activity observed during this timeframe involved China, not including the internet access points provided by Chinese telecommunications companies.

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

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

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

Bitcoin mining — a new way for North Korea to make money.

North Korea appears to be funding itself with bitcoin, according to a recent report. Recorded Future, an intelligence research firm backed by Google Venture and In-Q-Tel (a venture capital firm funded by the CIA), reported that North Korea began "mining" bitcoin on May 17 and could be using the digital currency to generate income for the regime.

The United Nations Security Council on Monday unanimously approved new sanctions against North Korea, the harshest yet — capping North Korea's oil imports, banning textile exports, ending additional overseas labor contracts. Bitcoin "mining" could become a viable income source for this further-isolated nation that's craving nuclear weapons.

"We weren't able to determine the volumes, like how many bitcoin they can generate per certain time period. We could just see activity," said Priscilla Moriuchi, the director of strategic threat development at Recorded Future.

Future Threat Trends from North Korean Cyber Operations

Evidence is mounting that sanctions, international pressure, and possibly increased enforcement by China are beginning to take their toll on the North Korean economy and in particular, North Korea intelligence agent's ability to procure goods for regime leadership. A May 2017 report from the Korea Development Institute concluded that North Korea's black market had helped the nation endure the impacts of the international sanctions last year.

Left unchecked and barring any unpredictable power shift, North Korea is likely to continue to place strategic value in its cyber capabilities. Future North Korean cyber attacks are likely to fall along a spectrum, with one end being continued low-intensity attacks and the other end characterized by high-intensity attacks from an emboldened North Korea. Concurrently, the DPRK will likely deepen the integration of its cyber elements into its conventional military forces. Although North Korea's history of low-intensity provocations makes it more likely that it will continue on the lower end of the spectrum, the Specific policy recommendations for the United States and the U.S.-ROK alliance are :

- Prepare a graduated series of direct responses targeting North Korea's cyber organizations.

- Curb North Korea's operational freedom in cyberspace.

- Identify and leverage North Korea's vulnerabilities to maintain strategic balance.

- A dopt damage mitigation and resiliency measures to ensure that critical systems and networks maintain operational continuity during and after an attack.

CONCLUSION

In international relations one does not assume that your adversary is nuts and do not underestimate his capacity to inflict serious damage on you. West has made both the mistakes with regard to North Korea. Our reasons for doing so are, at one level, understandable. In economic terms, the country is a basket case. According to the CIA's world factbook, its per-capita GDP is $1,800 or less, compared with nearly $40,000 for the UK and $53,000 for the US. Its industrial infrastructure is clapped out and nearly beyond repair; the country suffers from chronic food, energy and electricity shortages and many of its people are malnourished. International sanctions are squeezing it almost to asphyxiation.

And yet this impoverished basket case has apparently been able to develop nuclear weapons, plus the rocketry needed to deliver them to Los Angeles and its environs. Kim's priority is to avoid regime change. He knows that if you have nukes, then no one – not even Trump – is going to try any funny business, especially when it's clear that a seriously aggressive move by the US would mean the death of hundreds of thousands of South Koreans. The North Korean leader's rationale for developing nuclear weapons that are ready for deployment is identical to Britain's rationale for renewing Trident: deterrence.

While American and South Korean officials often express outrage about North Korea's cyber activities, they rarely talk about their own — and whether that helps fuel the cyber arms race. Yet both Seoul and Washington target the North's Reconnaissance General Bureau, its nuclear program and its missile program. Hundreds, if not thousands, of American cyber warriors spend each day mapping the North's few networks, looking for vulnerabilities that could be activated in time of crisis. Both the United States and South Korea have also placed digital "implants" in the Reconnaissance General Bureau, the North Korean equivalent of the Central Intelligence Agency, according to documents that Edward J. Snowden released several years ago. American created cyber and electronic warfare weapons were deployed to disable North Korean missiles, an attack that was, at best, only partially successful.

At a recent meeting of American strategists to evaluate North Korea's capabilities, some participants expressed concerns that the escalating cyber war could actually tempt the North to use its weapons — both nuclear and cyber — very quickly in any conflict, for fear that the United States has secret ways to shut the country down.

North Korea has understood how digital technology can convert industrial and economic weakness into a strength. The reason why major industrialised countries hold back from responding in kind to one another's cyber attacks is because their societies are all desperately dependent on complex, fragile and insecure network infrastructures. So all fear the unfathomable consequences of retaliation. And, accordingly, a new doctrine of mutually assured destruction keeps an uneasy peace in cyberspace.

North Korea, however, doesn't have much of a digital infrastructure and so has less to fear. Which is why Kim may be smarter than we like to think.

[https://www.theguardian.com/commentisfree/2017/oct/22/north-korea-deadliest-weapon-cyber-operations-sony-pictures]

Indeed, both sides see cyber as the way to gain tactical advantage in their nuclear and missile standoff.

There is evidence Pyongyang has planted so-called digital sleeper cells in the South's critical infrastructure, and its Defense Ministry, that could be activated to paralyze power supplies and military command and control networks. The North Korean cyber threat "crept up on us," said Robert Hannigan, the former director of Britain's Government Communications Headquarters, which handles electronic surveillance and cyber security."Because they are such a mix of the weird and absurd and medieval and highly sophisticated, people didn't take it seriously," he said. "How can such an isolated, backward country have this capability? Well, how can such an isolated backward country have this nuclear ability?"