Center for Cyber
& Homeland Security
THE GEORGE WASHINGTON UNIVERSITY

Empty Threat or Serious Danger?
Assessing North Korea's Risk to the Homeland

Testimony before the House Homeland Security Committee
Oversight and Management Efficiency Subcommittee

October 12, 2017

Frank J. Cilluffo
Director of the Center for Cyber and Homeland Security
The George Washington University

Center for Cyber
& Homeland Security
THE GEORGE WASHINGTON UNIVERSITY

Chairman Perry, Ranking Member Correa, and distinguished Members of the Subcommittee, thank you for the opportunity to testify before you today on this subject of national importance. North Korea poses an increasingly complex and multidimensional threat to the U.S. homeland. The many facets of the challenge include the nuclear threat, the missile threat, and the proliferation threat—which encompasses North Korea's role in the global arms trade of conventional and non-conventional weapons. Other experts testifying before you today will focus on these and other aspects of the problem. My own remarks will focus on the cyber threat, though I will also touch on the issue of electromagnetic pulse (EMP). As regards the cyber aspect, it should be flagged upfront that it is not unidimensional. To the contrary, it may manifest in at least three ways: as a stand-alone cyber threat; as a cyber component of a broader campaign that makes use of other means (e.g., military); or as an indicator of an attack or campaign that is yet to come (cyber intelligence preparation (IPB) of the battlefield or mapping of critical infrastructure). After assessing the threat, I will turn to the role that DHS can and should play in countering that threat.

The Cyber Threat that North Korea Poses to the U.S. Homeland

At the Central Intelligence Agency (CIA)'s fourth annual public conference on the Ethos and Profession of Intelligence (co-hosted by the George Washington University Center for Cyber & Homeland Security), a senior CIA official described North Korea as between "bookends"—the fear of Chinese abandonment on the one hand, and the fear of a U.S. strike on the other. The official stated further that North Korea "exists to oppose the United States," and that Kim Jong Un "defines winning as staying in the game."[1] It is against this background, the overriding survival of the Kim regime and the "Songun" or military first policy, that the North Korean cyber threat must be considered and evaluated.

In prepared testimony before the full Committee[2] and one of your counterpart Subcommittees[3], I have set out in some detail the nature of the cyber threat that North Korea poses to the U.S. homeland. Today I will build further upon that baseline. At the high end of the cyber threat spectrum are nation-states whose military and intelligence services are both determined and sophisticated in the cyber domain and are integrating computer network attack (CNA) and computer network exploit (CNE) into their warfighting strategy and doctrine—North Korea is one of a small handful of countries that top that list from a U.S. national security

[1] https://www.youtube.com/watch?v=a-N_NqVe_uc&list=PL-bQ6_vfcE05kAK-AX3uGxjLk0bVDhE3O&index=2
[2] https://cchs.gwu.edu/sites/cchs.gwu.edu/files/Cilluffo%20Testimony%20for%20HHSC%203-22-2017.pdf
[3] https://cchs.gwu.edu/sites/cchs.gwu.edu/files/downloads/HHSC_Testimony_Feb%2025-2016_Final.pdf

perspective. While many of the details about North Korea's cyberwarfare capabilities are shrouded in secrecy (the same is true of their military capabilities writ large), we do know that North Korea has invested heavily in building cyber capabilities. A 2015 report by the South Korean Defense Ministry estimates that the North Korean "cyber army" employs an elite squad of 6,000 hackers,[4] many of whom operate abroad in northeast China and throughout South East Asia. And, what North Korea may lack in capability, it makes up for with intent.

North Korea has engaged in both disruptive and destructive activity in the cyber domain—meaning both computer network exploitation (CNE) and computer network attack (CNA; as distinct from espionage). North Korea operates without compunction, targeting U.S. companies; the most notorious case being the attack on Sony Pictures Entertainment. North Korea is just as aggressive within its region: in 2017, there has been a major increase in North Korean cyber-attacks (attempted and successful) targeting South Korean companies and government.[5] Senior Japanese cybersecurity officials confirmed this in recent meetings, and expressed significant concern about the increase in volume and the level of boldness of North Korean cyber activity. Recent news articles revealing alleged U.S. cyber activities aimed at stymieing North Korea's ballistic missile program will likely serve to increase the likelihood of additional North Korean cyber-attacks.

In order to raise revenue—and under particular pressure from sanctions imposed recently by the international community (including key trading partner China), following North Korean nuclear and missile testing—North Korea has turned to cybercrime, and is the prime suspect in a string of bank heists throughout Asia (SWIFT hack), as well as reportedly targeting "bitcoin and other virtual currencies" for theft (FireEye report).[6] It has also been reported that the country is "widely believed to be behind the WannaCry [ransomware] cyberattack which spread to more than 300,000 computers across 150 countries."

---

[4] Martin Anderson, "North Korea's Internet Tundra Breeds Specialised "Cyber Forces" Numbering 6,000," The Stack, January 7, 2015. https://thestack.com/security/2015/01/07/north-koreas-internet-tundra-breeds-specialisedcyber-forces-numbering-6000

[5] Charlie Campbell, "The World Can Expect More Cybercrime from North Korea Now that China has Banned its Coal," Time, February 19, 2017. http://time.com/4676204/north-korea-cyber-crime-hacking-china-coal/

[6] Luke McNamara, "Why is North Korea So Interested in Bitcoin?" (September 11, 2017), https://www.fireeye.com/blog/threat-research/2017/09/north-korea-interested-in-bitcoin.html. See also Ryan Browne, "North Korea appears to be trying to get around sanctions by using hackers to steal bitcoin," (September 12, 2017), https://www.cnbc.com/2017/09/12/north-korea-hackers-trying-to-steal-bitcoin-evade-sanctions.html

State Sponsor of Cybercrime

If past is prologue, we ought to be prepared for a further spike in North Korean state-sponsored and/or state-supported cybercrime. The former head of the United Kingdom's Government Communications Headquarters (GCHQ) reinforced this point the other day, stating bluntly, "They're after our money."[7] While the cyber twist may be relatively new, such behavior is not: North Korea has long turned to criminal activity, such as counterfeiting (of currency including so-called super-notes, pharmaceuticals, and cigarettes), to fill its coffers. In this way, the regime engages criminal proxies and their cyber prowess to help achieve the ends that will perpetuate the regime's survival. This convergence of nation-state and criminal forces heightens the dangers posed by both. Whereas, traditionally, it has been the forces of crime that seek to penetrate the state; in the case of North Korea, the opposite is true, with the country often using diplomatic cover to pursue illegal activities.

North Korea's cyber strategy and tactics must be understood in broader context, as part and parcel of other geopolitical tools and goals (military, political, economic). The country's cyber capabilities are just one weapon in their arsenal, to be used in conjunction with other elements and for the purpose of achieving a wide range of goals and objectives. When assessed and appreciated in this way, North Korea's cyber activity may portend a broader campaign (including military operations), and thereby serve as an indicator or early warning of the intent to strike in other domains. And, cybercrime is undoubtedly helping fund North Korea's nuclear and missile programs. At the same time, from a cyber standpoint, North Korea is less vulnerable (relative to the countries it targets) to retaliation in-kind, since North Korea is not "wired" like most other nation-states. To the extent that the country is connected to the Internet—for military and intelligence purposes, for example—it appears that efforts have been made to protect and maintain that cyber capability and resilience, by diversifying connectivity: just days ago, it was reported that a Russian firm will provide North Korea with a second Internet connection, thereby decreasing reliance on the previously single connection that a Chinese firm had provided; and expanding North Korea's cyber-attack capability.[8] There has also been chatter about Russian criminal support of North Korea's cyber activities.

A further risk for the United States is electromagnetic pulse (EMP), which includes the threat posed by directed energy weapons. As defined by the Department of

---

[7] Harvey Gavin, "Hacking warning: Kim Jong-Un's henchmen to step up cyber attacks and target City of London," Express (October 1, 2017), http://www.express.co.uk/news/uk/861007/north-korea-hackers-target-uk-banks

[8] Reuters Staff, "Russian firm provides new internet connection to North Korea," Reuters (Oct. 2, 2017), http://www.reuters.com/article/us-nkorea-internet/russian-firm-provides-new-internet-connection-to-north-korea-idUSKCN1C70D2?il=0

Energy, EMPs "are intense pulses of electromagnetic energy resulting from solar-caused effects or man-made nuclear and pulse-power devices."[9] Nuclear EMP in particular—generated by detonating a nuclear device at a high altitude—would have catastrophic effects for the electricity, communications, transportation, fuel, and water sectors (including others). EMP is a threat that the United States must address from both a strategic and operational perspective. In connection with North Korea, it may be tempting to think in binary terms; but we do so at our peril, for cyber tools/attacks, EMPs, missiles, kinetic actions, and so on, are not "either/or" propositions. To the contrary—and, especially, if North Korea does not have the requisite launch capacity for its missiles (be they nuclear-tipped or conventional)—the country may turn to some combination of the foregoing (i.e., cyber plus…). Significantly, just last month North Korea publicly stated, for the first time, that they have developed a hydrogen bomb that can be detonated at high altitudes thereby signaling "interest and ability in an EMP attack."[10] While the probability of first use may currently be relatively low, the potential consequences and impact could be catastrophic and, therefore, the possibility must be taken seriously and treated accordingly.

The chart on the following page captures, at a glance, the multidimensional nature of the North Korean cyber threat; and contextualizes it with selected examples.

---

9 https://energy.gov/sites/prod/files/2017/01/f34/DOE%20EMP%20Resilience%20Action%20Plan%20January%202017.pdf (at page 1)

10 Anthony Furey, "North Korea openly threatens EMP attack for the first time, changing the game," Toronto Sun (September 3, 2017), http://m.torontosun.com/2017/09/03/north-korea-openly-threatens-emp-attack-for-the-first-time-changing-the-game

North Korea - Cyber Threat Actor

Strategy	Descriptor	Example
Computer Network Attack (CNA)	Disruptive or destructive in nature, cyber specific/exclusive or in combination with kinetic military operations	Hack of SONY Pictures Entertainment Inc.
Computer Network Exploitation (CNE)	Espionage (military, economic, and diplomatic), cyber IPB of critical infrastructure can provide important indicators & warning of a broader campaign and attack plans (order of battle)	Persistent, ongoing, across a range of sectors and targets
Cybercrime	Theft, ransomware, etc.	SWIFT hack, bank and bitcoin theft, Wanna Cry ransomware

The Role of the Department of Homeland Security

Preparing for cyber threats from state actors such as North Korea requires a multidimensional response. Accordingly, all elements of statecraft—diplomatic, economic, law enforcement, intelligence, military, emergency preparedness, and so on—should be considered and integrated, as appropriate (including in contingency plans). Whatever the Department of Homeland Security (DHS) does, it must be undertaken with the preparatory efforts of its various partners in mind— including, in particular, the Department of Defense and the private sector. Actions to protect and enhance the resilience of critical infrastructure, moreover, should be undertaken in a manner that recognizes, addresses, and integrates the full spectrum of threats, from cyber to EMP and beyond. There is a need to begin planning and exercising in earnest for various scenarios including EMP—which would have impact beyond DHS and U.S. utilities, given the importance of the electric grid and its interdependencies with all other "lifeline" critical infrastructures.

Policy and programs must not only cohere at the strategic and operational levels within DHS, within the interagency, and across the public/private sector (to ensure that public and private sector efforts and initiatives are pulling in the same direction). Policy and programs must also complement and leverage those of our international allies and partners, in order to be maximally effective. Others, beyond the United States, could and should do more to contain and crack down on North Korea. The United States is already working with South Korea and Japan, for example; but, geopolitical complexities must be navigated skillfully in order to further pull in other key actors constructively, so as to better deal with the challenges at hand. Keep in mind, for instance, that as pressure increases on China to pull back from North Korea, Russia is stepping into the breach as backstop for Kim Jong Un's regime.

The Department of Homeland Security (DHS) must strategically plan, resource, and prepare for the cyber threat posed by North Korea, and it must do so in the context of the broader threat posed by that country, and as part of the Department's mission writ large, which includes but is not limited to the ".gov" environment. DHS must also do all of this at a time when resources are limited and threats are expanding. The challenge, therefore, is to develop and implement programs that are not only effective but efficient. The Quadrennial Homeland Security Review (QHSR) is one instrument that helps to align strategy imperatives with spending parameters, so that both programming and underwriting are undertaken wisely. However, in the present ecosystem where risks are intensifying, it bears asking (immediately) if the current status of DHS programs and plans is sufficient—or whether there are things that the Department can and should do differently.

The National Protection and Programs Directorate (NPPD) of DHS provides a range of valuable services to support and protect entities directly within its remit (federal civilian networks) and partners with whom the Department collaborates (state, local, tribal, and territorial governments, and the private sector). These services range from vulnerability scanning and mitigation guidance, to information sharing and malware analysis, to technical assistance and intrusion-/incident-specific "hunt" teams. Importantly, efforts are underway to "streamline and elevate" the NPPD's cybersecurity and critical infrastructure mission. These activities, together with the multidisciplinary experience and expertise of the Department as a whole (e.g., in law enforcement, risk mitigation, and emergency management, to name a few), allow DHS to help further national resilience, and deter threat actors.[11]

[11] For additional details, see the written testimony of Acting Secretary of Homeland Security Elaine C. Duke, tendered to the Senate Committee on Homeland Security and Governmental Affairs (September 27, 2017), https://www.hsgac.senate.gov/hearings/09/18/2017/threats-to-the-homeland (see especially pages 9-11)

The Department's work on "Hidden Cobra" is a case in point. This attack effort by North Korean government actors targeted U.S. businesses (including critical infrastructure sectors, financial and aerospace companies) using malware and botnet attacks.[12] Working together with the Federal Bureau of Investigation (FBI), DHS provided critical infrastructure owners and operators (85% are in the private sector) with crucial situational awareness in the form an alert, attribution, and malware analysis.[13] In its outreach to stakeholders, DHS specified the vulnerabilities that the North Korean perpetrators were using, as well as signatures that could be used for/integrated into response strategies. Importantly, these types of network-defense activities can be very effective in countering North Korea in particular, which has a massive botnet infrastructure. From the standpoint of industry, furthermore, the sort of granular and timely information that DHS provided—including the identity of the attacker and the tactics, techniques, and procedures (TTPs) used—was valuable, as it allowed alerted entities to inoculate themselves against certain vulnerabilities (or, at least, to mitigate the consequences of breach). In addition to identifying TTPs, DHS and FBI in conjunction with the intelligence community could also provide indications & warning (I&W) of potential North Korean target lists/selection and potential order of battle.

Hidden Cobra is thus illustrative of the interagency process working as it should, with DHS partnering with the federal community for information exchange, in order for DHS to provide real added-value to its stakeholders. The case also ties together the information sharing component with deterrence, in that the DHS alert and subsequent prevention/mitigation activity on the part of targeted businesses (and the government) demonstrates to the attacker that the United States is both ready and able to take anticipatory (defensive) action against adversaries or, if need be, to rebound and show resilience post-attack. This evidence of "a virtuous cycle" is what DHS can and should build upon, so as to generate additional positive momentum that in turn will help further fuel its own success. Interagency partners like the Cyber Threat Intelligence Integration Center (CTIIC) have already proven to be willing and capable partners in upping the U.S. game against cyber adversaries: as events unfold, CTIIC brings together information from across the federal cyber community to form a shared picture of the U.S. government's information (both classified and unclassified), gaps, and actions to inform decision-makers who have a role in the response. But still, we need to do more, and we need to do better. In this respect, we should strive for the DHS equivalent to military planning and execution, where all relevant players have a seat at the table pre-incident and where all

[12] Tom Spring "DHS, FBI warn of North Korea 'Hidden Cobra' strikes against US assets," Threatpost (June 14, 2017), https://threatpost.com/dhs-fbi-warn-of-north-korea-hidden-cobra-strikes-against-us-assets/126263/
[13] US-CERT Alert (TA 17-164A), "HIDDEN COBRA – North Korea's DDoS Botnet Infrastructure" (June 13, 2017), https://www.us-cert.gov/ncas/alerts/TA17-164A

concerned are well-positioned to thwart attacks and attackers when an incident is underway.

Conclusion

Thank you again for this opportunity to testify on this important topic.[14] I look forward to trying to answer any questions that you may have.

[14] I would like to thank the Center's Associate Director Sharon Cardash for her help in drafting my prepared testimony.