Center for Cyber
& Homeland Security
THE GEORGE WASHINGTON UNIVERSITY

Emerging Cyber Threats to the United States

Testimony of Frank J. Cilluffo
Director, Center for Cyber & Homeland Security

Before the U.S. House of Representatives
Committee on Homeland Security
Subcommittee on Cybersecurity, Infrastructure Protection,
and Security Technologies

February 25, 2016

GW Center for Cyber and Homeland Security
2000 Pennsylvania Avenue, NW, Suite 2210 • Washington, DC 20052
Tel: 202-994-2437 • E-Mail: cchs@gwu.edu
http://cchs.gwu.edu

Chairman Ratcliffe, Ranking Member Richmond, and distinguished Subcommittee Members, thank you for this opportunity to testify before you today. The United States currently faces an almost dizzying array of cyber threats from many and varied actors. Virtually every day there is a new incident in the headlines and the initiative clearly remains with the attacker. Critical infrastructure, such as the U.S. financial services sector, is in the crosshairs as a primary target; but our banks are not alone—"lifeline" sectors such as energy & electricity, telecommunications, transportation, and water are similarly situated. According to the Department of Homeland Security, cyber-attacks on U.S. industrial control systems rose 20 percent last year as compared to the year before, with the energy sector among those hardest hit.[1] Just days ago, hackers took a Los Angeles hospital offline, demanding ransom in bitcoins to restore systems and operations.[2] And no one is immune from digital targeting of crucial infrastructure: earlier this month for instance, it was reported that hackers "used malware to infiltrate a Russian regional bank and manipulate the ruble-dollar exchange rate by more than 15 percent in minutes."[3]

The threat tempo is magnified by the speed at which technologies continue to evolve and by the fact that our adversaries continue to adapt their tactics, techniques and procedures in order to evade and defeat our prevention and response measures. While breaches to date have largely exemplified data theft, the next step that hostile actors take may go further—such as data manipulation. Just imagine the havoc that a creative adversary could wreak this way, by changing our most sensitive and private information, with everything from medical records to stock exchanges potentially at risk. Against this background, a strong detection and mitigation program is just as necessary as a strong defense. While it is important to continue to invest in technologies and procedures to prevent attacks, the reality is that nobody can prevent all attacks; but significant steps can be taken to minimize the impact and consequences of an attack. This posture, one of substantial resilience, must also extend to our partners in the private sector, which own and operate 85 percent of U.S. critical infrastructure.

At the national level, the challenge is to understand as best we can the threat as it manifests in so many different incarnations; and to prioritize it so that our limited resources for preventing and containing the challenge are directed as efficiently and effectively as possible. This includes supporting the private sector which now finds itself on the front lines, so as to allow U.S. businesses to engage in active defense of their "crown jewels"—from trade secrets to R&D-related intellectual property and so on.

---

[1] U.S. Department of Homeland Security, *ICS CERT Monitor*, November/December 2015. *https://ics-cert.us-cert.gov/sites/default/files/Monitors/ICS-CERT%20Monitor_Nov-Dec2015_S508C.pdf*

[2] Brian Barrett, "Hack Brief: Hackers Are Holding an L.A. Hospital's Computers Hostage," *Wired*, Feb. 2, 2016. *http://www.wired.com/2016/02/hack-brief-hackers-are-holding-an-la-hospitals-computers-hostage/*

[3] Katie Bo Williams, "Report: Hackers use Malware to Manipulate Russian Currency Value," *The Hill*, Feb. 8, 2016. *http://thehill.com/policy/cybersecurity/268588-report-hackers-use-malware-to-manipulate-russian-currency-value*

Taking a global perspective on cyber threats, the bottom line up front is as follows:

- The threat spectrum includes a wide array of actors with different intentions, motivations, and capabilities.

- Nation-states and their proxies continue to present the greatest—meaning most advanced and persistent—threat in the cyber domain. This testimony will focus on four key threat actors, but it is important to keep in mind the broader context: every country that has a modern military and intelligence service also has a computer network attack capability.[4] Importantly, nation-states vary in terms of both their capability and intent, with some being more willing to exercise their cyber capabilities than others.

- Nation-states often use proxies to conceal state involvement. In turn, there are different grades of proxies: they may be state-sanctioned, state-sponsored, or state-supported.

- Foreign terrorist organizations certainly possess the motivation and intent but fortunately, they have yet to fully develop a sustained cyber-attack capability. Recent "doxing" tactics against US military and law enforcement personnel by the Islamic State in Iraq and Syria (ISIS) is troubling and indicative of an emerging threat. It is likely that ISIS, or their sympathizers, will increasingly turn to disruptive cyber-attacks.

- By contrast, criminal organizations possess substantial capabilities, but their motivation and intent differs from terrorists. Rather than being motivated by ideology or political concerns, criminal organizations are driven by the profit motive. However criminals are increasingly working with or for nation-states such as Russia; and this convergence of forces heightens the dangers posed by both groups.

- Yet other entities such as "hacktivists" may also possess considerable skills and abilities; and when their special interests or core concerns are perceived to be in play, these individuals can be a significant disruptive force whether acting alone or loosely in tandem, essentially as a leaderless movement.

[4] Over 100 governments have stood up military entities to engage in cyberwarfare, according to Peter Singer and Allan Friedman ("Cybersecurity and Cyberwar: What Everyone Needs to Know," *Oxford University Press*, Jan. 3, 2014). The Wall Street Journal recently reported that "29 countries have formal military or intelligence units dedicated to offensive hacking," out of 60 that are developing tools for computer-enabled espionage or attacks (Damian Paletta, Danny Yadron, and Jennifer Valentino-Devries, "Cyberwar Ignites a New Arms Race," *Wall Street Journal*, Oct. 11, 2015*)*. Discrepancies in these numbers are due to varying definitions of cyber warfare units, but the underlying point that there are a number of cyber capable state actors is clear.

Their motive is often to cause maximum embarrassment to their targets and to bring attention to their cause.

- Regardless of actor, there are many different modalities of attack. Tactics, techniques, and procedures include malware, exploitation of zero day vulnerabilities, distributed denial of service (DDoS) attacks, and the use of botnets. Data may be stolen or manipulated. The use of ransomware and crypto-ransomware is also on the rise: hospitals, police departments, and schools have been hit. For a good overview of these trends, see Symantec's 2015 Internet Security Threat Report.[5]

- In reference to any threat vector, a worst-case scenario would combine kinetic and cyber-attacks; and the cyber component would serve as a force multiplier to increase the lethality or impact of the physical attack.

- The insider threat also cuts across vectors and can materialize within any actor, from the nation-state on down.

- Finally, critical infrastructure such as U.S. banks and the energy sector (oil & gas) are primary targets for cyber-attacks and cybercrimes. A concerted campaign against these crucial infrastructures holds the potential to undermine trust and confidence in the system itself, irrespective of the perpetrator.

  Below the various categories of actors are examined in greater detail in terms of the nature of the threat they pose and how they function.

Nation-States

The most advanced and persistent cyber threats to the United States today remain nation-states and their proxies, and in particular China and Russia. In addition, Iran has increased its cyber capabilities exponentially in recent years. And with the hack of Sony Corporation—which made use of more than half a dozen exploits lest the target be patched against one or more of these vulnerabilities, North Korea too has demonstrated itself to be a significant adversary.

Against the growing abilities of these key threat actors for "online espionage, disinformation, theft, propaganda and data-destruction,"[6] the Director of National Intelligence James Clapper recently observed (during the annual worldwide threat assessment offered to Congress earlier this month) that, "improving offensive tradecraft, the use of proxies, and the creation of cover organizations will hinder

---

[5] "Internet Security Threat Report, Volume 20," *Symantec*, April 2015.

[6] Spencer Ackerman and Sam Thielman, "US Intelligence Chief: We Might Use the Internet of Things to Spy on You," *The Guardian*, Feb. 9, 2016.
http://www.theguardian.com/technology/2016/feb/09/internet-of-things-smart-home-devices-government-surveillance-james-clapper

timely, high-confidence attribution of responsibility for state-sponsored cyber operations."[7] This is significant because the harder it is to attribute activity, the harder it is to deter and punish the perpetrator.

How do these actors function?

Our adversaries have engaged in brazen activity, from computer network exploitation (CNE) to computer network attack (CNA). CNE includes traditional, economic, and industrial espionage, as well as intelligence preparation of the battlefield (IPB)—such as surveillance and reconnaissance of attack targets, and the mapping of critical infrastructures for potential future targeting in a strategic campaign. In turn, CNA encompasses activities that alter (disrupt, destroy, etc.) the targeted data/information. The line between CNE and CNA is thin, however: if one can exploit, one can also attack if the intent exists to do so.

Foreign militaries are, increasingly, integrating CNE and CNA capabilities into their warfighting and military planning and doctrine, as well as their grand strategy. These efforts may allow our adversaries to enhance their own weapon systems and platforms, as well as stymie those of others. Moreover, CNAs may occur simultaneously with other forms of attack (kinetic, insider threats, etc.).

Our adversaries are also interweaving the cyber domain into the activities of their foreign intelligence services, to include intelligence derived from human sources (HUMINT).

This said our adversaries are certainly not all of a piece. Rather, nation-states may differ from one another, or from their proxies, in their motivation and intent. Tradecraft and its application may also differ widely. From a U.S. perspective, the challenge is to parse our understanding of key actors and their particular behaviors, factoring details about each threat vector into a tailored U.S. response that is designed to dissuade, deter, and compel.[8]

China

China possesses sophisticated cyber capabilities and has demonstrated a striking level of perseverance, evidenced by the sheer number of attacks and acts of espionage that the country commits. Reports of the Office of the U.S. National Counterintelligence Executive have called out China and its cyber espionage, characterizing these activities as rising to the level of strategic threat to the U.S. national interest.[9]

---

[7] James R. Clapper, Director of National Intelligence, *Statement for the Record*, "Worldwide Threat Assessment of the U.S. Intelligence Community," Senate Armed Services Committee, Feb. 9, 2016.

[8] Frank J. Cilluffo and Rhea D. Siers, "Cyber Deterrence is a Strategic Imperative," *Wall Street Journal*, Apr. 28, 2015. *http://blogs.wsj.com/cio/2015/04/28/cyber-deterrence-is-a-strategic-imperative/*

[9] Foreign Spies Stealing US Economic Secrets in Cyberspace, *Report to Congress on Foreign Economic Collection and Industrial Espionage*, 2009-2011, Oct. 2011. *http://www.ncix.gov/publications/reports/fecie_all/Foreign_Economic_Collection_2011.pdf*

The U.S.-China Economic and Security Review Commission notes further: "Computer network operations have become fundamental to the PLA's strategic campaign goals for seizing information dominance early in a military operation."[10]

China's aggressive collection efforts appear to be intended to amass data and secrets (military, commercial / proprietary, etc.) that will support and further the country's economic growth, scientific and technological capacities, military power, etc.—all with an eye to securing strategic advantage in relation to (perceived or actual) competitor countries and adversaries.

In May 2015, data theft on a massive scale, affecting virtually all U.S. government employees, was traced back to China. Whether the hack was state-sponsored, state-supported, or simply tolerated through a blind eye by the government of China, is not yet clear. But military officers in China are increasingly known to moonlight as hackers for hire when off the clock; and countries are increasingly turning to proxies do their bidding in order to provide plausible deniability.[11] The extent to which China may benefit from the massive data breach such as by using the information to blackmail and recruit Americans thus remains to be seen.

In September 2015, China and the United States reached an agreement on refraining from conducting economic cyber-espionage. Earlier this month, DNI Clapper noted that there is evidence of "limited ongoing cyber activity from China", but as yet it has not been confirmed to be state-sponsored. Meantime however, China appears to be giving "security and intelligence agencies a larger role in helping Beijing hack foreign companies."[12]

Russia

Russia's cyber capabilities are, arguably, even more sophisticated than those of China, and Russia has been particularly adept at integrating cyber into its strategic plans and operations[13]. The Office of the U.S. National Counterintelligence Executive (NCIX) observes: "Moscow's highly capable intelligence services are using HUMINT, cyber, and other operations to collect economic information and technology to support Russia's economic development and security. Russia's extensive attacks on

---

[10] *http://www.uscc.gov/RFP/2012/USCC%20 Report_Chinese_CapabilitiesforComputer_NetworkOperationsandCyberEspionage.pdf*

[11] Sharon L. Cardash and Frank J. Cilluffo, "Massive Government Employee Data Theft Further Complicates US-China Relations," *The Conversation*, June 8, 2015. *https://theconversation.com/massive-government-employee-data-theft-further-complicates-us-china-relations-42941*; and Kelly Jackson Higgins, "State-Owned Chinese Firms Hired Military hackers for IT Services," *Dark Reading*, May 21, 2014. *http://www.darkreading.com/attacks-breaches/state-owned-chinese-firms-hired-military-hackers-for-it-services/d/d-id/1269102*

[12] Jack Detsch, "Report: China Bolsters State Hacking Powers," *Christian Science Monitor - Passcode*, Feb. 4, 2016. *http://www.csmonitor.com/World/Passcode/2016/0204/Report-China-bolsters-state-hacking-powers*

[13] Jason Wirtz, "Cyber War and Strategic Culture: The Russian Integration of Cyber Power into Grand Strategy," NATO Cooperative Cyber Defence Center of Excellence, 2015.

U.S. research and development have resulted in Russia being deemed (along with China), "a national long-term strategic threat to the United States," by the NCIX.[14] Also concerning, Russia and China recently signed a cybersecurity agreement pursuant to which they pledge not to hack one another and to share both information and technology.[15]

In 2009, the Wall Street Journal reported that cyber-spies from Russia and China had penetrated the U.S. electrical grid, leaving behind software programs. The intruders did not cause damage to U.S. infrastructure, but sought to navigate the systems and their controls. Was this reconnaissance or an act of aggression? What purpose could the mapping of critical U.S. infrastructure serve, other than intelligence preparation of the battlefield? The NASDAQ exchange, too, has allegedly been the target of a "complex hack" by a nation-state. Again, one questions the motivation.[16]

More recently, Russian hackers believed to be doing their government's bidding breached the White House, the State Department, and the Defense Department.[17] Similar forces were also poised to cyber-attack US banks against the backdrop of economic sanctions levied against Russia for its repeated and brazen incursions into Ukraine.[18]

Russia has also engaged in cyber operations against Ukraine (2014/15), Georgia (2008), and Estonia (2007); in the first two instances combining them with kinetic operations. Notably, in December 2015, western Ukraine experienced a power outage that is believed to have been caused by cyberattack perpetrated by Russia. Though one power company reported the incident, "similar malware was found in the networks of at least two other utilities."[19] More than four dozen substations were affected, as were more than a quarter of a million customers for up to six hours. In addition, a simultaneous attack on call centers (a telephony denial of

---

[14] *http://www.ncix.gov/publications/reports/fecie_ all/Foreign_Economic_Collection_2011.pdf*

[15] Cory Bennett, "Russia, China Unite with Major Cyber Pact," *The Hill*, May 8, 2015. *http://thehill.com/policy/cybersecurity/241453-russia-china-unit-with-major-cyber-pact*

[16] http://www.bloomberg.com/bw/articles/2014-07-17/how-russian-hackers-stole-the-nasdaq

[17] Evan Perez and Shimon Prokupecz, "How the U.S. Thinks Russians Hacked the White House," *CNN*, Apr. 8, 2015*, http://www.cnn.com/2015/04/07/politics/how-russians-hacked-the-wh/*; and Cory Bennett, "Defense chief: Russian goals in Pentagon hack 'not clear'," *The Hill*, May 15, 2015, *http://thehill.com/policy/cybersecurity/242213-pentagon-head-russian-goals-not-clear-in-dod-hack*

[18] Cory Bennett, "Russian Hacking Group was Set to hit U.S. Banks," *The Hill*, May 13, 2015 *http://thehill.com/policy/cybersecurity/241965-russian-hacking-group-was-set-to-hit-us-banks*; and "APT28: A Window into Russia's Cyber Espionage Operations?" *FireEye*, October 27, 2015 *https://www.fireeye.com/blog/threat-research/2014/10/apt28-a-window-into-russias-cyber-espionage-operations.html*; and Frank J. Cilluffo and Sharon L. Cardash, "How to Stop Putin Hacking the White House," *Newsweek*, April 13, 2015 *http://www.newsweek.com/how-stop-putin-hacking-white-house-321857;* and http://www.cnbc.com/id/102025262

[19] Eric Auchard and Jim Finkle, "Experts: Ukraine Utility Cyberattack Wider than Reported," *Reuters*, January 4, 2016. *http://m.voanews.com/a/reu-experts-ukraine-utility-cyberattack-wider-than-reported/3131554.html*

service attack) hindered communication and customer reporting of difficulties. The case is truly significant: it is believed to represent the first time that a blackout was caused by computer network attack.

Over time, Russia's history has also demonstrated a toxic blend of crime, business, and politics—and there are few, if any, signs that things are changing today. To the contrary, a convergence between the Russian intelligence community and cyber-criminals has been observed as relations between Russia and the West have deteriorated as the conflict over Ukraine has unfolded.[20] Evidence of the complicity between the Russian government and its cyber-criminals and hackers became even starker when the Russian Foreign Ministry issued "a public notice advising `citizens to refrain from traveling abroad, especially to countries that have signed agreements with the U.S. on mutual extradition, if there is reasonable suspicion that U.S. law enforcement agencies' have a case pending against them."[21]

Notably the DNI stated to Congress this month that Russia is "assuming a more assertive cyber posture based on its willingness to target critical infrastructure systems and conduct espionage operations even when detected."[22] It has also been reported that Russia's Defense Ministry is standing up a cyber command which will "be responsible for conducting offensive cyber activities, including propaganda operations and inserting malware into enemy command and control systems."[23]

Iran

Iran has invested heavily in recent years to deepen and expand its cyber warfare capacity. Under President Rouhani, the country's cybersecurity budget has increased "twelvefold"; and the country may now be considered "a top-five world cyber power."[24]

This concerted effort and the associated rapid rise through the ranks comes in the wake of the Stuxnet worm, which targeted Iran's nuclear weapons development program. How the recently concluded international agreement on containing that program will affect Iran's behavior in the cyber domain over the long run remains to be seen—although early reports indicate that Iran "has ramped up its cyber espionage, targeting…the emails and social media accounts of State Department

---

[20] John Leyden, "Ukraine Conflict Spilling Over into Cyber-crime, Warns Former Spy Boss," *The Register*, April 16, 2015. *http://www.theregister.co.uk/2015/04/16/cyber_war_keynote_infiltrate/*

[21] Kevin Poulsen, "Russia Issues International Travel Advisory to its Hackers," *Wired*, September 3, 2013. *http://www.wired.com/2013/09/dont-leave-home/*

[22] James R. Clapper, Director of National Intelligence, "Worldwide Threat Assessment of the US Intelligence Community," *Statement for the Record before the U.S. Senate, Armed Services Committee*, February 9, 2016. *http://www.dni.gov/files/documents/SASC_Unclassified_2016_ATA_SFR_FINAL.pdf*

[23] James R. Clapper, Director of National Intelligence, "Worldwide Cyber Threats," *Statement for the Record before The U.S. House of Representatives, Permanent Select Committee on Intelligence*, September 10, 2015. *http://docs.house.gov/meetings/IG/IG00/20150910/103797/HHRG-114-IG00-Wstate-ClapperJ-20150910.PDF*

[24] Cory Bennett, "Iran has Boosted Cyber Spending Twelvefold," *The Hill*, March 23, 2015. *http://thehill.com/policy/cybersecurity/236627-iranian-leader-has-boosted-cyber-spending-12-fold*

officials whose work is related to Iran and the Middle East."[25] Another important but open question is whether and how recent reports that the United States had formulated plans to disable Iran's nuclear program by cyber means, in the event that nuclear negotiations failed and military conflict ensued, may affect Iran's cyber-behavior moving forward.[26]

We also know that Iran has engaged in a concerted cyber campaign against U.S. banks.[27] In January 2013, the Wall Street Journal reported[28] on "an intensifying Iranian campaign of cyberattacks [thought to have begun months earlier] against American financial institutions" including Bank of America, PNC Financial Services Group, Sun Trust Banks Inc., and BB&T Corp. Six leading U.S. banks—including J.P. Morgan Chase—were targeted in "the most disruptive" wave of this campaign, characterized by DDoS attacks. The Izz ad-Din al-Qassam Cyber Fighters claim responsibility for all of these incidents.

U.S. officials also believe Iran to be responsible for a cyber-attack against the Sands Casino in Las Vegas owned by politically active billionaire Sheldon Adelson. The incident appears to be a first: "a foreign player simply sought to destroy American corporate infrastructure on such a scale… PCs and servers were shut…down in a cascading IT catastrophe, with many of their hard drives wiped clean."[29]

Iran has also long relied on proxies such as Hezbollah—which now has a companion organization called Cyber Hezbollah—to strike at perceived adversaries. Iran and Hezbollah are suspected in connection with the August 2012 cyberattacks on the state-owned oil company Saudi Aramco and on Qatari producer RasGas, which resulted in the compromise of approximately 30,000 computers.[30]

---

[25] Cory Bennett, "Iran Launches Cyber Offensive after Nuclear Deal," *The Hill*, November 24, 2015. *http://thehill.com/policy/cybersecurity/261190-iran-switches-to-cyber-espionage-after-nuclear-deal*

[26] David Sanger and Mark Mazetti, "U.S. Had Cyberattack Plan if Iran Nuclear Dispute Led to Conflict," *The New York Times*, February 16th, 2016. *http://www.nytimes.com/2016/02/17/world/middleeast/us-had-cyberattack-planned-if-iran-nuclear-negotiations-failed.html?smid=nytcore-iphone-share&smprod=nytcore-iphone*

[27] Shane Harris, "Forget China: Iran's Hackers are America's Newest Cyber Threat," *Foreign Policy*, February 18, 2014. *http://foreignpolicy.com/2014/02/18/forget-china-irans-hackers-are-americas-newest-cyber-threat/*

[28] Siobhan Gorman and Danny Yadron, "Banks Seek U.S. Help on Iran Cyberattacks," *The Wall Street Journal*, January 16, 2013. *http://www.wsj.com/articles/SB10001424127887324734904578244302923178548*

[29] Ben Elgin and Michael Riley, "Now at the Sands Casino: An Iranian hacker in Every Server," *Bloomberg Business*, December 11, 2015. *http://www.bloomberg.com/bw/articles/2014-12-11/iranian-hackers-hit-sheldon-adelsons-sands-casino-in-las-vegas*

[30] Kim Zetter, "The NSA Acknowledges What we all Feared: Iran Learns from US Cyberattacks," *Wired*, February 10, 2015. *http://www.wired.com/2015/02/nsa-acknowledges-feared-iran-learns-us-cyberattacks/*

In addition, elements of Iran's Revolutionary Guard Corps (IRGC) have also openly sought to pull hackers into the fold, including the political/criminal hacker group Ashiyane; and the Basij, who are paid to do cyber work on behalf of the regime.[31]

North Korea (DPRK)

As perhaps the world's most isolated state-actor in the international system, North Korea operates under fewer constraints. For this reason, the country poses an important "wildcard" threat, not only to the United States but also to the region and to broader international stability.

South Korea's Defense Ministry estimates that North Korea possesses a force of "about 6,000 cyber agents."[32] A frequent DPRK target, South Korea has attributed a series of cyber-attacks—upon its Hydro & Nuclear Power Company (2014) and upon its banks and broadcasting companies (2013), for example—to North Korea.[33]

From a U.S. standpoint, it is the North Korean attack on Sony Pictures Entertainment late last year that looms large: "`There was disruption. There was destruction of data. There was an intent to hurt the company. And it succeeded, bringing a major U.S. entertainment company to its knees'."[34]

Where will the DPRK go from here? In the words of an Australian expert, "There's growing concern amongst analysts, and government officials alike that North Korea has begun to rapidly accelerate its development of advanced offensive cyber capabilities'."[35] This concern is compounded by the fact that, potentially, "cyber operations…could be integrated in the future with a military strategy designed to disrupt U.S. systems."[36]

These developments are all the more disturbing when considered in tandem with the following trenchant question raised by one of my CCHS colleagues: "`Given North Korea's proclivity to provide other destructive technologies and military

---

[31] Frank J. Cilluffo, "The Iranian Cyber Threat to the United States," *Testimony before the U.S. House of Representatives, Committee on Homeland Security, Subcommittee on Counterterrorism and Intelligence and Subcommittee on Cybersecurity, Infrastructure Protection, and Security Technologies*, April 26, 2012. *http://cchs.gwu.edu/sites/cchs.gwu.edu/files/downloads/Testimony_Cilluffo_April_26_2012.pdf*

[32] Leo Byrne, "N. Korean Hacking Threat Leads to Blue House Cyber-security Office," *NK News*, March 31, 2015. *http://www.nknews.org/2015/03/n-korean-hacking-threat-leads-to-blue-house-cyber-security-office/*

[33] Tae-jun Kang, "South Korea Beefs up Cyber Security with an Eye on North Korea," *The Diplomat*, April 1, 2015. *http://thediplomat.com/2015/04/south-korea-beefs-up-cyber-security-with-an-eye-on-north-korea/*

[34] James Lewis, "The Attack on Sony," *CBS News 60 Minutes*, April 12, 2015. *http://www.cbsnews.com/news/north-korean-cyberattack-on-sony-60-minutes/*

[35] Leo Byrne, "N. Korean Hacking Threat Leads to Blue House Cyber-security Office," *NK News*, March 31, 2015. *http://www.nknews.org/2015/03/n-korean-hacking-threat-leads-to-blue-house-cyber-security-office/*

[36] Harper Neidig, "GOP Senator: North Korea Cyber Threat Growing," *The Hill*, October 7, 2015. *http://thehill.com/policy/cybersecurity/256274-gop-senator-north-korean-cyber-threat-growing*

assistance to rogue states and non-state actors, would the DPRK also assist them with destructive cyber capabilities'?"[37]

In addition, reports that the United States targeted the DPRK's nuclear program with a version of Stuxnet, but without success, may—if true—further complicate the challenge posed by North Korea.[38]

On many levels, North Korea is both a troubling and unusual case. Ordinarily, it is organized crime that seeks to penetrate the state. In this case, however, it is the other way around—with the state trying to penetrate organized crime in order to ensure the survival of the regime/dynasty.

Foreign Terrorist Organizations

To date, terrorist organizations have not demonstrated the advanced level of cyber-attack capabilities that would be commensurate with these groups' stated ambitions. Undoubtedly, though, these organizations will persist in their efforts to augment their in-house cyber skills and capacities. Of particular concern are foreign terrorist organizations that benefit from state sponsorship and support, as well as the Islamic State in Iraq and Syria (ISIS/ISIL). Given ISIS' savvy use of social media and how it has built and maintained a sophisticated propaganda machine, it is likely that the group—and their sympathizers—will turn their efforts towards developing a more robust cyber-attack capability.

The current level of cyber expertise possessed by terrorist groups should bring us little comfort, however, because a range of proxies for indigenous cyber capability exist: there is an arms bazaar of cyber weapons, and our adversaries need only intent and cash to access it. Capabilities, malware, weapons, etc.—all can be bought or rented.[39]

In terms of what we have seen recently, ISIS has invoked a new tactic against members of the U.S. military and law enforcement: "doxing"—which involves gathering personal information from sources online and then publishing that data online, which puts the victim at risk of further attack in both the physical and virtual worlds. [40] A prevalent theme in the drumbeat of ISIS propaganda videos has been repeated calls for "lone wolf" attacks against Western law enforcement and military personnel.

---

[37] Rhea Siers, "North Korea: The Cyber Wild Card," *Journal of Law & Cyber Warfare*, 2014.

[38] Joseph Menn, "Exclusive: U.S. Tried Stuxnet-style Campaign against North Korea but Failed – Sources," *Reuters*, May 29, 2015. *http://www.reuters.com/article/2015/05/29/us-usa-northkorea-stuxnet-idUSKBN0OE2DM20150529*

[39] Frank Cilluffo, "Cyber Threats from China, Russia and Iran: Protecting American Critical Infrastructure," *Testimony before the U.S. House of Representatives, Committee on Homeland Security Subcommittee on Cybersecurity, Infrastructure Protection, and Security Technologies*, March 20, 2013. *http://cchs.gwu.edu/sites/cchs.gwu.edu/files/downloads/Testimony_Cilluffo_March_20_2013.pdf*

[40] Kate Knibbs, "ISIS Has a New Terrorism Tactic: Doxing US Soldiers," *Gizmodo*, March 23, 2015. *http://gizmodo.com/isis-has-a-new-terrorism-tactic-doxing-us-soldiers-1693078782*

Terrorist organizations also use the internet in a host of ways that serve to further their ends and put the United States and its allies, and the interests of both, in danger. By way of illustration, the internet helps terrorists plan and plot, radicalize and recruit, and train and fundraise. To help protect and facilitate these online activities, ISIS in particular has created "a new technical 'help desk'" that unifies its various tech support efforts, including for encryption.[41]

As terrorist cyber capabilities grow more sophisticated, one especially concerning scenario would involve terrorist targeting of U.S. critical infrastructure, using a mix of kinetic and cyber-attacks. In this scenario, the cyber component could serve as a force multiplier to increase the lethality or impact of the physical attack.

Criminal Organizations

Cyberspace has proven to be a gold mine for criminals, who have moved ever more deeply into the domain as opportunities to profit there continue to multiply. These criminal groups operate in layered organizations that share networks and tools. Despite reaping 30 cents on the dollar, there is a low chance that these criminals will be held accountable for their actions because they benefit from safe havens in Eastern Europe—which is, according to European Police Office (EUROPOL) Director Robert Wainwright, the source of 80 percent of all cybercrime.

The illicit activities of criminal groups in the virtual world are typically associated with the "Dark Web," a sub-set of the Internet where the IP addresses of websites are concealed. Here, "the sale of drugs, weapons, counterfeit documents and child pornography" constitute "vibrant industries."[42] Cybercriminals have also demonstrated substantial creativity, such as extortion schemes demanding payment via cryptocurrencies, such as Bitcoin. For example, most criminals demand payment for "ransomware" attacks (such as GameOver Zeus or CryptoLocker) to be made via cryptocurrencies, which are attractive to criminal organizations due to their anonymity or pseudonymity. Increasingly, more traditional organized crime groups, such as drug trafficking organizations, are also turning to virtual currencies for payment and to move their money in the black market.

According to EUROPOL whose focus is serious international organized crime, "cybercrime has been expanding to affect virtually all other criminal activities":

> The emergence of crime-as-a-service online has made cybercrime horizontal in nature, akin to activities such as money laundering or document fraud. The changing nature of cybercrime directly impacts on how other criminal activities, such as drug trafficking, the facilitation of illegal immigration, or the distribution

[41] Cory Bennett, "New ISIS 'Help Desk' to Aid Hiding From Authorities," *The Hill*, February 10, 2016. *http://thehill.com/policy/cybersecurity/268940-new-isis-help-desk-unifies-encryption-support*

[42] Andy Greenberg, "Hacker Lexicon: What is the Dark Web?" *Wired*, November 19, 2014. *http://www.wired.com/2014/11/hacker-lexicon-whats-dark-web/*

> of counterfeit goods are carried out. … General trends for cybercrime suggest considerable increases in scope, sophistication, number and types of attacks, number of victims and economic damage. … This allows traditional OCGs [organized criminal groups] to carry out more sophisticated crimes, buying access to the technical skills and expertise they require.[43]

Cybercriminals possess substantial cyber capabilities and, increasingly, are working with or for nation-states such as Russia. This convergence of forces heightens the dangers posed by both groups (e.g., criminal organizations and nation-states). And from a monetary standpoint alone, the amounts at stake are staggering. Consider: Russia's slice of the 2011 global cybercrime market has been pegged at $2.3 billion.[44]

"Hacktivists" and Other Entities

Cyberspace largely levels the playing field, allowing individuals and small groups to have disproportionate impact. While some "hacktivists" may possess considerable abilities, the bar here is relatively low, and virtually anyone with a measure of skills and a special interest can cause harm.

Though great sophistication may not be needed to achieve disruption and draw attention to a particular concern, individuals and entities in this category can be a significant force, whether acting alone or loosely in tandem, essentially as a leaderless movement.

U.S. Response Measures

This varied threat landscape has a direct impact on a wide variety of cybersecurity policy questions facing the Congress and the executive branch, including on current issues such as federal spending on cybersecurity, the implementation of the new information sharing law, federal support for our critical infrastructure sectors, and the "going dark" debate over encryption in our electronic devices. In the remainder of my testimony, I will briefly highlight two important cyber issues that the GW Center for Cyber & Homeland Security is currently focusing on: deterrence and active defense.

First, I will discuss deterrence. Having just racked and stacked the wide range of cyber threats that presently exist, and that may evolve and emerge in the future, the next step is to confront, contain, and thwart them by imposing significant costs on our adversaries for engaging in unacceptable behaviors.[45] Unless our adversaries

---

[43] Massive Changes in the Criminal Landscape," *Europol*, 2015; and "Counterterrorism & Cybersecurity: Insights from Europol Director Rob Wainwright," *Center for Cyber and Homeland Security*, April 30, 2014. *https://www.europol.europa.eu/newsletter/massive-changes-criminal-landscape*; and *http://cchs.gwu.edu/counterterrorism-cybersecurity-insights-europol-director-rob-wainwright*

[44] "Leading Russian Security Firm Group-IB Releases 2011 Report on Russian Cybercrime," *Group-IB*, April 24, 2012. *http://www.group-ib.com/?view=article&id=705*

[45] Frank Cilluffo and Rhea Siers, "Cyber Deterrence is a Strategic Imperative," *The Wall Street Journal*, April 28, 2015; *http://blogs.wsj.com/cio/2015/04/28/cyber-deterrence-is-a-strategic-imperative/*; and

experience such consequences, there will be little incentive for them to cease the actions and attacks in question. Changing their incentive structure requires signaling to hostile actors that the United States is both capable and willing to play offense. In turn, this means being more transparent about U.S. abilities and demonstrating the will to invoke them as required.

As things now stand however, our adversaries are acting largely without penalty and thus continue to transgress. Moreover when an incident occurs, our tendency is to blame the victim. This is a deeply flawed state of affairs that must be reversed. In fact, we should go further than simple reversal by working not only to deter our adversaries but to dissuade and compel them as well. Further elaborating U.S. policy and position in such a manner would be complementary to ongoing U.S. and international efforts to enumerate and flesh out global norms of conduct for cyberspace.

The second crucial shortcoming in current U.S. strategy and posture regards active defense, meaning the use of proactive measures by U.S. companies to defend themselves and their most critical assets against sophisticated and determined cyber adversaries. These adversaries include nation-states and their proxies. Although America's business community never asked to face off against foreign intelligence and security services (or those who would do their bidding), this is the position in which our companies find themselves. Accordingly, at minimum it is the responsibility of the U.S. government to delineate and offer our private sector partners an operating framework—that provides the parameters and supports that they need—in order to engage in active defense. The Center has formed a task force to examine these issues that is co-chaired by Admiral Dennis Blair, Secretary Michael Chertoff, Nuala O'Connor of the Center for Democracy & Technology, and me. We will be releasing a major report addressing these questions later this year.[46]

Concluding Thoughts

Looking ahead, many crucial questions on the threat side remain open, including: Will the nuclear weapons agreement concluded with Iran curb or embolden Iranian cyber operations against the United States and its allies over the longer term? Will the December 2015 cyberattack on Ukraine's electric grid, that caused a power outage in the western portion of the country, become a more commonplace tactic? Will hackers engage increasingly in data manipulation, as distinct from data theft? Equally important will be the attack vectors that, for whatever reason, we fail to anticipate. While we cannot know in advance every threat that may lurk around every virtual corner, we can certainly take the steps necessary to maximize our ability to detect, prevent, protect, and respond. In some instances, it may be that our

---

https://cchs.gwu.edu/sites/cchs.gwu.edu/files/downloads/INSS%20Blueprint%20for%20Cyber%20Deterrence.pdf

[46] "Center Announces New Project on Active Defense against Cyber Threats," *GW Center for Cyber and Homeland Security*, February 4, 2016. http://cchs.gwu.edu/center-announces-new-project-active-defense-against-cyber-threats

ability to bounce back—our resilience—proves to be a valuable deterrent to our adversaries. At present however, there is still much work to be done before we can say that we have done all that we can. That work will be all the more crucial to accomplish as the Internet of Things expands exponentially the potential attack surface and leads the cyber domain to converge ever-further with the physical world. Secure design, architected from the get-go, will be crucial to resilience.[47]

Thank you again for this opportunity to testify on this important topic. [48] I look forward to trying to answer any questions that you may have.

[47] Michael Papay, Frank Cilluffo, Sharon Cardash, "Opinion: Fortifying the Internet of Things means baking in security at the beginning," *The Christian Science Monitor*, March 6, 2015. *http://www.csmonitor.com/World/Passcode/Passcode-Voices/2015/0306/Opinion-Fortifying-the-Internet-of-Things-means-baking-in-security-at-the-beginning*

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