Homeland Security
Policy Institute
THE GEORGE WASHINGTON UNIVERSITY

Cyber Threats from China, Russia and Iran: Protecting American Critical Infrastructure

U.S. House of Representatives, Committee on Homeland Security

Subcommittee on Cybersecurity, Infrastructure Protection, and Security Technologies

March 20, 2013

Frank J. Cilluffo
Director. Homeland Security Policy Institute,
Co-Director, Cyber Center for National and Economic Security
The George Washington University

Chairman Meehan, Ranking Member Clarke, and distinguished Members of the Subcommittee, thank you for this opportunity to testify before you today. The Subcommittee has demonstrated real leadership in this issue area with hearings and other work undertaken long before the cyber domain and its challenges were front and center on the national agenda as is now the case. For example, your hearing last April on the Iranian cyber threat to the United States was quite prescient.[1] That challenge, and the broader one under study today, remains crucial to explore, understand, and respond to, because of all that is at stake—namely U.S. national and economic security.

My statement below is designed to help frame how the U.S. can and should assess and respond to cyber threats, especially those posed by nation-states. A great deal of excellent, deep dive analysis is already being performed on specific threats, including the work of my fellow witnesses. For example, the recent Mandiant report tracing extensive hacking activity against the United States (and other countries and corporations) back to the doorstep of China's Army, the PLA, was a significant contribution to the discourse, in that it provided both forensic and empirical data, which are in short supply in the open-source literature, yet sorely needed.[2] What is also needed, however, is a broader typology of the cyber threat, structured to help us rack and stack the challenges that we face, and prioritize our efforts to meet them. I will propose such a typology today to assess the relative severity of cyber threats, and also suggest how the United States might re-focus its cyber efforts accordingly.

The cyber threat comes in various shapes, sizes, and forms. The bar to entry is low to launch a relatively rudimentary, but still potentially damaging, cyber-attack. The threat spectrum ranges from nation-states plus their proxies, to foreign terrorist organizations, criminal syndicates and information brokers, to hacktivists, to ankle-biters operating out of their parents' home. Each of these categories, in turn, also breaks down into a number of sub-categories. Regarding nation-states, for example, they vary widely in their sophistication, capability, intent, motivation, and so on. Taking a topline perspective, however, it is nation-states (and their proxies) that the U.S. should be most concerned about when it comes to threat. This finding is supported by a recent Homeland Security Policy Institute (HSPI) Flash Poll

[1] "The Iranian Cyber Threat to the United States", Testimony of Frank J. Cilluffo before the House Subcommittee on Cybersecurity, Infrastructure Protection, and Security Technologies; and the House Subcommittee on Counterrorism and Intelligence (April 26, 2012). http://www.gwumc.edu/hspi/policy/Iran%20Cyber%20Testimony%204.26.12%20Frank%20Cilluffo.pdf

[2] Mandiant Report, "APT-1: Exposing one of China's Cyber Espionage Units" (February 2013). http://intelreport.mandiant.com/, and https://www.mandiant.com/blog/mandiant-exposes-apt1-chinas-cyber-espionage-units-releases-3000-indicators/

conducted right after the President issued an Executive Order, "Improving Critical Infrastructure Cybersecurity"[3], this February. According to our poll, to which over one hundred HSPI stakeholders responded: nearly 70% of respondents indicated that nation-states posed the greatest threat to cybersecurity, by comparison to other categories of actors. The remainder of responses were split between foreign terrorist organizations, "hacktivists", organized crime, and "other".[4]

For too long, though, we have assessed and appreciated the nation-state threat in overly general terms. The volume and nature of activity directed against us, and our allies, should serve as a wakeup call to raise our game. Now is the time to focus on the high end threat, and to rack and stack our priorities. We simply cannot afford to do otherwise—not in the current economic climate, and not in light of the critical U.S. assets and infrastructure that are still vulnerable and at risk.

Every day, new news of cyber intrusions, exploits, and attacks comes to light. The nation's most sensitive sectors, from defense to energy to finance, are often the targets. Our adversaries have engaged in brazen activity, from computer network exploitation (CNE) to computer network attack (CNA). Foreign militaries are, increasingly, integrating CNE and CNA capabilities into their warfighting and military planning and doctrine. These efforts may allow our adversaries to enhance their own weapon systems and platforms, as well as stymie those of others. CNE may also support intelligence preparation of the battlefield, to include the mapping of critical infrastructures that could be targeted in a more strategic campaign or attack plan. CNAs may occur simultaneously with other forms of attack (kinetic, insider threats, etc).

Last month, against this background, the President issued an Executive Order intended to improve critical infrastructure cybersecurity.[5] The goal is closer collaboration between government and the private sector to protect critical networks. The Executive Order is a good start, but it is no substitute for legislation—which can introduce a range of incentives (such as tax provisions, liability protections, and procurement preferences which factor security requirements into federal acquisitions) plus sticks to accompany

[3] http://www.whitehouse.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity

[4] http://www.gwumc.edu/hspi/frontincludes/Cyber%20EO%20Flash%20Poll%20Press%20Release%202-15-2013.pdf

[5] http://www.whitehouse.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity

those carrots, and thereby raise the bar higher when it comes to critical infrastructure standards and practices.[6]

To refine and reinforce its stance in relation to the threat, the U.S. must focus upon actors and their particular behaviors, rather than upon technology per se, or upon means and modalities of attack. Doing so means digging deeper into specifics, and factoring those case-by-case (actor- and country-specific) details about our adversaries into a tailored U.S. response that is also designed to dissuade, deter, and compel our adversaries accordingly. Our response must be calibrated to address and thwart (among other things) the adversary's motivation—be it to steal money, intellectual property, or military secrets, etc. U.S. response must also be calibrated to address and thwart the adversary's intent—be it commercial gain, military advantage, criminal activity, etc. To complicate matters, both motivation and intent are multidimensional, and thus may consist of some combination of these factors. Motivation and intent may also change over time, and the various factors that comprise each may shift at a given moment. Nation-states and their proxies may also differ in their motivation and intent.

Parsing our understanding of U.S. adversaries down to (and beyond) this level of granularity will yield insights upon which more effective strategies and tactics may be built and implemented. At first glance, such a task may seem overwhelming, given the number and complexity of the potential variables. The good news is that a robust but general posture should help us deal with the signal to noise ratio and suffice to handle 80% of the nefarious activity that comes our way. The other 20% is where we need to keep a closer eye on the ball. I turn now to those harder cases, to offer a snapshot of who they are, what they have done, why they have done it, and what they might do in future.

Naming and shaming is an approach that has been invoked with varying degrees of success across a range of contexts. Until recently, however, only a few of the boldest of U.S. officials (current and former) had walked out on that limb in the context under examination today. Lately, however, the number of U.S. government and private sector voices has become more of a chorus. The President's National Security Advisor Thomas Donilon publicly cited and elaborated upon U.S. cybersecurity concerns in connection with

[6] Frank J. Cilluffo and Andrew Robinson, "While Congress dithers, cyber threats grow greater" Nextgov.com (July 24, 2012). http://www.nextgov.com/cybersecurity/2012/07/while-congress-dithers-cyber-threats-grow-greater/56968/

China, in a speech earlier this month.[7] Before that, and among other developments, the New York Times published an account of intrusions against its own networks[8] by Chinese hackers—which in turn seems to have prompted a cascade of similar revelations, including in relation to the Washington Post and the Wall Street Journal. In this context, as in others, there is power in numbers.

Capabilities do matter, of course. Our most challenging adversaries in the cyber domain are commonly known as Advanced Persistent Threats (APT). China and Russia indisputably fall in this category although the two can and should be characterized and understood somewhat differently (see below). Iran is another difficult case, though a bit different in kind, as it makes up in intent what it may lack in capability—though its capabilities are noteworthy, especially when proxies are factored in. To the list of truly concerning nation-state actors one could and should also add North Korea. 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(s).

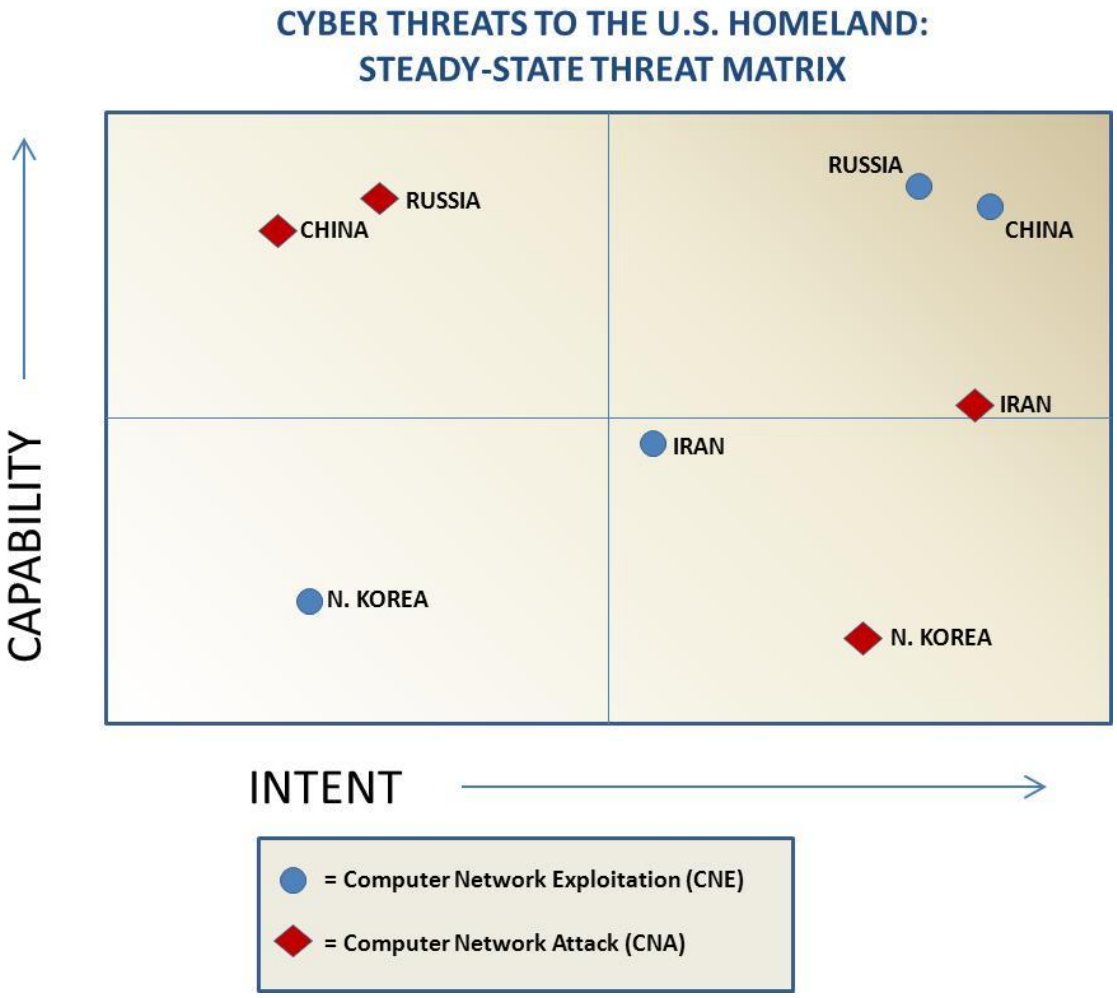
Though I will focus exclusively on China, Russia, and Iran in the limited space that remains, North Korea is a troubling case as well as an unusual one. Ordinarily, it is organized crime that seeks to penetrate the state. In this case, however, it is the other way around, with the state trying to penetrate organized crime in order to ensure the survival of the regime/dynasty. Like Iran, the DPRK is more likely to turn to CNA to achieve its objectives. In this regard, Iran and North Korea stand in contrast to China and Russia which operate under greater constraints. Precisely because North Korea has fewer constraints, I would underscore that it poses an important "wildcard" threat, not only to the United States but also to the region and broader international stability.

Since a picture is often worth a thousand words, I have tried to encapsulate findings and cross-country comparisons in the two charts that follow. The graphics are a rough attempt to rank each of the countries at issue according to capability and intent, as well as in terms of the CNE and CNA threat that they each pose, including in relative terms to one another. For the purposes of the matrices below, CNE is defined as traditional, economic, and industrial

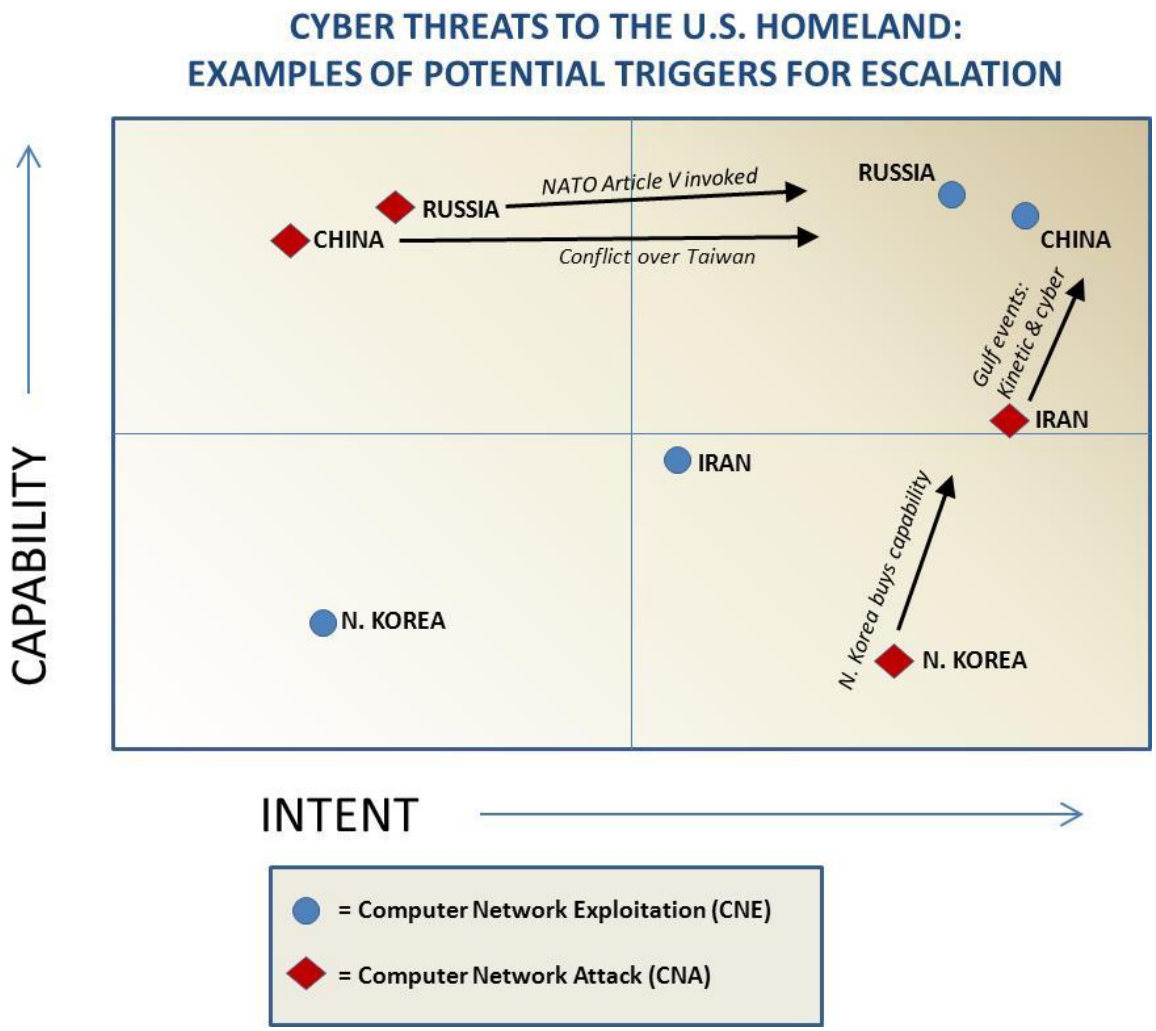
[7] "The United States and the Asia-Pacific in 2013", before The Asia Society (March 11, 2013). http://www.whitehouse.gov/the-press-office/2013/03/11/remarks-tom-donilon-national-security-advisory-president-united-states-a

[8] Nicole Perlroth, "Hackers in China Attacked the Times for Last 4 Months", New York Times (January 30, 2013). http://www.nytimes.com/2013/01/31/technology/chinese-hackers-infiltrate-new-york-times-computers.html?pagewanted=all&_r=0

espionage, as well as intelligence preparation of the battlefield (IPB). However, IPB is also included in the definition of CNA used here, as it may well be a precursor, such as surveillance and reconnaissance of targets to be attacked. Bear in mind that if one can exploit, one can also attack if the intent exists to do so. Note also that, for present purposes, CNA is defined as activities that alter (disrupt, destroy, etc.) the targeted data/information.



The second chart reflects the shifts in position that may occur if triggering or unforeseen events lead to potential escalation:



Unless and until we wrap our heads around the challenge posed by each of these cases, and do so in a way that appreciates both the similarities and differences between and among them, our national and economic security (including our critical infrastructure) will remain at risk. Not all actors, nor capabilities, nor intentions, are the same. Tradecraft and its application may also differ widely. So too motivations, which may include blackmail, coercion, fraud, and theft. Heightening our understandings of each of these elements as they apply to key actors is all the more important, as countries

continue to integrate CNA/CNE into war-fighting and military planning, and interweave the cyber domain into the activities of their foreign intelligence services, to include intelligence derived from human sources (HUMINT).

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] 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.

China denies the various charges leveled against it, and has raised its own hacking allegations, in which the country claims to have been victimized. The latter claim is difficult to accept completely, especially since China appears to take its own cybersecurity efforts seriously. According to Microsoft's security blog, "China had the lowest malware infection rate…of any of the 105 locations included in volume 13 of the [Microsoft] Security Intelligence Report", which refers back to 2012.[11] Perhaps China is as focused on self-inoculation as it is on hacking others? And perhaps this posture derives from an attempt to protect against precisely the points of vulnerabilities that China saw in others? Consider also the Mandiant report

[9] "Foreign Spies Stealing U.S. Economic Secrets in Cyberspace", Report to Congress on Foreign Economic Collection and Industrial Espionage, 2009-2011 (October 2011). http://www.ncix.gov/publications/reports/fecie_all/Foreign_Economic_Collection_2011.pdf [referred to hereafter as NCIX Report]. See also Frank J. Cilluffo, "Chinese Telecom Firms Pose a Threat to U.S. National Security", U.S. News & World Report (November 19, 2012). http://www.usnews.com/opinion/articles/2012/11/19/chinese-telecom-firms-pose-a-threat-to-us-national-security

[10] Patton Adams, George Bakos and Bryan Krekel, "Occupying the Information High Ground: Chinese Capabilities for Computer Network Operations and Cyber Espionage," Report prepared for the U.S.-China Economic and Security Review Commission by Northrop Grumman Corp. (March 3, 2012). http://www.uscc.gov/RFP/2012/USCC%20 Report_Chinese_CapabilitiesforComputer_Net-workOperationsandCyberEspionage.pdf.

[11] Tim Rains, "The Threat Landscape in China: A Paradox" (March 11, 2013). http://blogs.technet.com/b/security/

referenced earlier, which identifies Chinese PLA Unit 61398 as the most likely culprit behind the theft of "hundreds of terabytes of data from at least 141 organizations across a diverse set of industries, beginning as early as 2006."

As a domain, cyberspace is made for plausible deniability. Attribution remains a challenge, because smoking keyboards can be hard to find; and in the case of China, the PLA may also outsource certain activities and operations to skilled hackers, to distance the PLA from any smoking keyboards.[12] The attribution challenge is just one reason the Mandiant report is significant. Separate and apart from attempts to mask involvement in activity targeting the U.S., there may also be powerful reasons for China to restrict itself from acting against the U.S. in certain ways, at least at a particular moment in time. Director of National Intelligence James Clapper testified last week that China and Russia are "advanced" cyber actors, but that he did not foresee "devastating" cyber-attacks by these two actors against the U.S. in the near future[13]—"outside of a military conflict or crisis that they believe threatens their vital interests."[14] The vital interests caveat is important, since it is fairly easy to identify potential triggers in this category, such as Taiwan.

The Administration's public pronouncements on China have taken on a tougher tone this month, which represents a good step forward—but this is only a first step down a path that, for far too long, we have been traveling too slowly and too weakly. National Security Advisor Thomas Donilon emphasized "the urgency and scope of this problem"—meaning "sophisticated, targeted theft of confidential business information and proprietary technologies through cyber intrusions emanating from China on an unprecedented scale". Donilon then called on China "to investigate and put a stop to these activities" as well as "engage with us in a constructive direct dialogue to establish acceptable norms of behavior in cyberspace".[15] Days later, President Obama himself raised U.S. cyber concerns (of volume, scale, and scope) in a phone call with China's President, Xi Jinping.[16]

---

[12] Perlroth, http://www.nytimes.com/2013/01/31/technology/chinese-hackers-infiltrate-new-york-times-computers.html?pagewanted=all&_r=0

[13] Mark Mazetti and David E. Sanger, "Security Leader Says U.S. Would Retaliate Against Cyberattacks", New York Times (March 12, 2013). http://www.nytimes.com/2013/03/13/us/intelligence-official-warns-congress-that-cyberattacks-pose-threat-to-us.html?src=twr&_r=0

[14] Tom Gjelten, "Is All The Talk About Cyberwarfare Just Hype?" NPR.org (March 13, 2013). http://www.npr.org/2013/03/15/174352914/is-all-the-talk-about-cyberwarfare-just-hype

[15] Donilon, supra.

[16] Steve Holland, "Obama, China's Xi discuss cybersecurity dispute in phone call", Reuters (March 14, 2013). http://www.reuters.com/article/2013/03/14/us-usa-china-obama-call-idUSBRE92D11G20130314

Sustained U.S. leadership and engagement, at the highest levels, will be required, moving forward.

Since the line between CNE and CNA is thin, with the distinction between the two turning largely on intent, it is crucial that there be consequences for the actor that engages in sophisticated and persistent CNE. The principle applies regardless of the perpetrator. Indeed, one could argue that the only difference between China and Russia in this regard is that China got caught. It is a numbers game, after all. And China may not even be that concerned about getting caught, since the country may have taken a conscious decision to throw as much as possible at us, in terms of human resources dedicated to CNE—in the hope that some, even if not all, of their efforts would yield fruit. Unless and until there are consequences for such behavior, China (and others) have no real reason to care if they are caught in the act of CNE. To date, there have been no significant consequences for China's massive intrusions into critical U.S. networks. By failing to call attention to their CNE campaign (much less retaliating in any way at all) earlier on, we have encouraged it. Last month's White House report announcing a new strategy to mitigate the theft of U.S. trade secrets is at least a step in the right direction.[17]

Russia

Russia's cyber capabilities are, arguably, even more sophisticated than those of China. The Office of the U.S. National Counterintelligence Executive (NCIX) observes: "Moscow's highly capable intelligence services are using HUMINT [human intelligence], cyber, and other operations to collect economic information and technology to support Russia's economic development and security.[18] Russia's extensive attacks on 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.

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

[17] Executive Office of the President of the United States, "Administration Strategy on Mitigating the Theft of U.S. Trade Secrets" (February 2013) http://www.whitehouse.gov/sites/default/files/omb/IPEC/admin_strategy_on_mitigating_the_theft_of_u.s._trade_secrets.pdf

[18] NCIX Report, supra, at p. 5. http://www.ncix.gov/publications/reports/fecie_all/Foreign_Economic_Collection_2011.pdf

or an act of aggression? What purpose could the mapping of critical U.S. infrastructure serve, other than intelligence preparation of the battlefield?

Ambassador David Smith notes: "Russia has integrated cyber operations into its military doctrine; though not fully successful…Russia's 2008 combined cyber and kinetic attack on Georgia was the first practical test of this doctrine…[and] we must assume that the Russian military has studied the lessons learned". [19] Russia was also behind the 2007 distributed denial of service (DDoS) attacks on Estonia (its government, banks, etc.) although Russia denies official involvement. Relying upon "patriotic hackers" guided by government handlers plus a little help from the Russian intelligence service, however, does not alter the reality that activity undertaken by those hackers is state-sponsored and directly implicates Russia.

Hackers and criminals based in Russia have also made their mark. 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. Russia's slice of the 2011 global cybercrime market has been pegged at $2.3 billion, and there are indications that the forces of Russian organized crime have begun to join up "by sharing data and tools" to increase their take.[20] Just last week, moreover, hackers based in Russia posted what seemed to be personal financial information about the Vice President, the Director of the FBI, and a number of other current and former senior U.S. officials.[21] Russia's history has demonstrated a toxic blend of crime, business, and politics—and there are few, if any, signs that things are changing today. Indeed, as the former ranking member of the KGB in London said recently, Moscow has as many spies in the UK now as it did in the Cold War.[22] Similarly, former CIA officer Hank Crumpton has said: "I would hazard to guess there are more foreign intelligence officers inside the U.S. working against U.S. interests now than even at the height of the Cold War."[23]

---

[19] "How Russia Harnesses Cyberwarfare", American Foreign Policy Council *Defense Dossier* (August 2012) http://www.afpc.org/files/august2012.pdf

[20] Group IB, State and Trends of the Russian Digital Crime Market 2011, p. 6, http://group-ib.com/images/media/Group-IB_Report_2011_ENG.pdf; see also http://group-ib.com/images/media/Group-IB_Cybercrime_Inforgraph_ENG.jpg (graphics).

[21] Ken Dilanian and Jessica Guynn, "Obama meets with CEOs to push cyber-security legislation", L.A. Times (March 13, 2013) http://www.latimes.com/business/la-fi-obama-hacking-20130314,0,2583428.story

[22] Luke Harding, "Gordievsky: Russia has as many spies in Britain now as the USSR ever did", The Guardian (March 11, 2013). http://www.guardian.co.uk/world/2013/mar/11/russian-spies-britain-oleg-gordievsky

[23] "More spies in U.S. than ever, says ex-CIA officer." 60 Minutes (May 10, 2012). http://www.cbsnews.com/8301-18560_162-57431837/more-spies-in-u.s-than-ever-says-ex-cia-officer/

Iran

In April 2012, as mentioned earlier, I testified before a joint hearing of this Subcommittee and the Subcommittee on Counterterrorism and Intelligence, on the subject "The Iranian Cyber Threat to the United States."[24] What follows is an attempt to distill the essence of that nine-page statement into just a few paragraphs here.[25]

Iran is investing heavily to deepen and expand its cyber warfare capacity.[26] A range of proxies for indigenous cyber capability also 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. Iran has also long relied on proxies such as Hezbollah—which now has a companion organization called Cyber Hezbollah—to strike at perceived adversaries. Elements of Iran's Revolutionary Guard Corps (IRGC) have also openly sought to pull hackers into the fold. There is evidence that at the heart of IRGC cyber efforts one will find the Iranian political/criminal hacker group Ashiyane[27]; and the Basij, who are paid to do cyber work on behalf of the regime, provide much of the manpower for Iran's cyber operations.[28]

In January 2013, the Wall Street Journal reported 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.[29] In the latest chapter in this story, six leading U.S. banks—including J.P. Morgan Chase—were targeted just last week, in "the most disruptive" wave of this campaign, characterized by DDoS attacks.[30] The Izz ad-Din al-Qassam Cyber Fighters claim responsibility for all of these incidents.

---

[24] http://www.gwumc.edu/hspi/policy/Iran%20Cyber%20Testimony%204.26.12%20Frank%20Cilluffo.pdf

[25] For an in-depth treatment of Iran, see Gabi Siboni and Sami Kronenfeld, "Iran and Cyberspace Warfare" in Military and Strategic Affairs, Vol. 4, No. 3 (Dec. 2012) at 77-99. http://www.gwumc.edu/hspi/policy/INSS.pdf

[26] Yaakov Katz, "Iran Embarks on $1b. Cyber-Warfare Program," Jerusalem Post (December 18, 2011). http://www.jpost.com/Defense/Article.aspx?id=249864.

[27] Iftach Ian Amit, "Cyber [Crime/War]," paper presented at DEFCON 18 conference (July 31, 2010).

[28] "The Role of the Basij in Iranian Cyber Operations", Internet Haganah (March 24, 2011). http://internet-haganah.com/harchives/007223.html.

[29] Siobhan Gorman and Danny Yadron, "Banks Seek U.S. Help on Iran Cyberattacks", Wall Street Journal (January 15, 2013). http://online.wsj.com/article/SB10001424127887324734904578244302923178548.html

[30] Tracy Kitten, "DDoS: 6 Banks Hit on Same Day" (March 14, 2013). http://www.bankinfosecurity.com/ddos-6-banks-hit-on-same-day-a-5607

There has also been considerable speculation about Government of Iran involvement in a number of hacking incidents including against Voice of America, and Dutch firm DigiNotar which issues security certificates. Fallout from the latter case was significant, and affected a range of entities including western intelligence and security services, Yahoo, Facebook, Twitter, and Microsoft.[31] The DigiNotar case, moreover, reflected a new and concerning level of sophistication on the part of Iran and its capabilities. Iran and Hezbollah are also suspected in connection with the August 2012 cyber-attacks on the state-owned oil company Saudi Aramco and on Qatari producer RasGas, which resulted in the compromise of approximately 30,000 computers.[32]

On the kinetic side, from Bulgaria to Bangkok, we have seen an uptick in attacks and assassinations (attempted and actual) targeting Israeli, Jewish, U.S., and Western interests. Iranian agents and proxies (Hezbollah) have been implicated, although Iran has tried to distance itself from these incidents and denied responsibility. Also recall the recently thwarted Iranian plot to assassinate Saudi Arabia's Ambassador to the United States on U.S. soil. Based on recent activity, the Los Angeles Police Department has elevated the Government of Iran and its proxies to a Tier One threat.

Conclusion

Looking ahead, with the described threat spectrum in mind, the US must strike a careful and powerful balance between offense and defense, to include a well-developed and well-articulated cyber deterrence strategy.[33] Historically, that balance has tilted heavily toward defense.[34] More recently, however, we have seen and heard evidence that the pendulum has shifted significantly. These indicators include General Alexander's testimony before the Senate Armed Services Committee last week (in his capacity as head of US Cyber Command and director of the National Security Agency), in which he referenced and detailed a series of cyber teams attached to Cyber Command—and underscored the role of these teams in contributing to and

[31] Kevin Kwang, "Spy agencies hit by CA hack; Iran suspected," ZDNet Asia (September 5, 2011) http://www.zdnetasia.com/spy-agencies-hit-by-ca-hack-iran-suspected-62301930.htm. See also Bill Gertz, "Iranians hack into VOA website," The Washington Times (February 21, 2011).
[32] Adam Schreck, "Virus origin in Gulf computer attacks questioned", Associated Press. http://www.nbcnews.com/technology/technolog/virus-origin-gulf-computer-attacks-questioned-978717. See also Siboni and Kronenfeld, supra, at pp. 90-91.
[33] Frank J. Cilluffo, Sharon L. Cardash, and George C. Salmoiraghi, "A Blueprint for Cyber Deterrence: Building Stability through Strength", in Military and Strategic Affairs, Vol. 4, No. 3 (Dec. 2012) at 3-23. http://www.gwumc.edu/hspi/policy/INSS.pdf
[34] Frank Cilluffo and Sharon Cardash, "Defense Cyber Strategy Avoids Tackling the Most Critical Issues" in Nextgov.com (July 28, 2011) http://www.nextgov.com/cybersecurity/2011/07/commentary-defense-cyber-strategy-avoids-tackling-the-most-critical-issues/49494/

supporting offensive capabilities.[35] As for U.S. cyber deterrence strategy, it must reflect the best ways and means of raising the (actual and perceived) costs and risks of action, to our adversaries, so as to prevent them from taking steps that would harm U.S. interests.

An "active defense" capability, meaning the ability to immediately attribute and counter attacks, is needed to address future threats in real-time. U.S. companies cannot be expected to go it alone, unassisted, against foreign intelligence services. If a thief robs a bank, the police will not stand idly by as the robber races away with his take. Similarly, the public and private sectors must partner together to prevent major heists online—and when private defenses are breached, the U.S. government must work closely with companies to ensure that there are consequences for the perpetrator(s). Active defense is a complex undertaking however, as it requires meeting the adversary closer to their territory, which in turn demands the merger of our foreign intelligence capabilities with U.S. defensive and offensive cyber capabilities (and potentially may require updating relevant authorities).[36] At the end of the day, however, perhaps the best deterrent—irrespective of the threat/actor—is the ability to recover, reconstitute, and bounce back quickly.

In conclusion, the threat is clear, but it is not monolithic. It will also continue to evolve over time. We may see nation-states intertwine increasingly with proxy actors, to include skilled hackers for hire.[37] Now is the time to examine and deconstruct the high end threat in its many permutations and combinations, so as to devise nuanced and effective counterstrategies and tactics. Thank you again, to the Subcommittee and its staff, for the opportunity to testify today. I would be pleased to try to answer any questions that you may have.

##

[35] Ellen Nakashima, "Pentagon creating teams to launch cyberattacks as threat grows", Washington Post (March 12, 2013). http://www.washingtonpost.com/world/national-security/pentagon-creating-teams-to-launch-cyberattacks-as-threat-grows/2013/03/12/35aa94da-8b3c-11e2-9838-d62f083ba93f_print.html

[36] Testimony of Frank J. Cilluffo before the Senate Committee on Homeland Security & Governmental Affairs, "The Future of Homeland Security: Evolving and Emerging Threats" (July 11, 2012). http://www.gwumc.edu/hspi/policy/Testimony%20-%20SHSGAC%20Hearing%20-%2011%20July%202012.pdf. See also: Testimony of Frank J. Cilluffo before the House of Representatives' Homeland Security Committee, "The Department of Homeland Security: An Assessment of the Department and a Roadmap for its Future" (September 2012).

[37] Frank J. Cilluffo and Joseph R. Clark, "Thinking About Strategic Hybrid Threats: In Theory and in Practice", PRISM 4, no. 1 (December 2012). http://www.ndu.edu/press/strategic-hybrid-threats.html