June 13, 2017

State-Sponsored Cyberspace Threats: Recent Incidents and U.S. Policy Response

Subcommittee on East Asia, the Pacific and International Cybersecurity, Committee on Foreign Relations, United States Senate, One Hundred Fifteenth Congress, First Session

---

Hearing Contents:

Witnesses

Samantha Ravich
Senior Advisor
Foundation for Defense of Democracies
View Testimony

Eric Rosenbach
Co-Director
Belfer Center for Science and International Affairs, Harvard University
View Testimony

Available Webcast(s)*:

- [Full Hearing]

Compiled From*:

- https://www.foreign.senate.gov/hearings/state-sponsored-cyberspace-threats-recent-incidents-and-us-policy-response-061317p

** Please Note: External links included in this compilation were functional at the time of its creation but are not maintained thereafter.*

CONGRESSIONAL TESTIMONY: FOUNDATION FOR DEFENSE OF DEMOCRACIES

Senate Foreign Relations Committee
Subcommittee on East Asia, the Pacific, and International Cybersecurity

State-Sponsored Cyberspace Threats:

Recent Incidents and U.S. Policy Response

SAMANTHA F. RAVICH, PH.D.

Senior Advisor
Foundation for Defense of Democracies

Board of Advisors
Center on Sanctions and Illicit Finance, Foundation for Defense of Democracies

Former Deputy National Security Advisor
Vice President Dick Cheney

Former Co-Chair
National Commission for the Review of Research and Development Programs in the United States Intelligence Community

Washington, DC
June 13, 2017

FDD
FOUNDATION FOR DEFENSE OF DEMOCRACIES

www.defenddemocracy.org

Chairman Gardner, Ranking Member Markey, distinguished members of the subcommittee, thank you for inviting me to participate in this important hearing on state-sponsored cyber threats. My testimony today focuses on an area that I believe is woefully underappreciated yet cannot be more important for our country. And that is the use of cyber means by adversarial states to purposefully undermine our economy in order to weaken us military and politically.

Both traditional economic warfare and, more recently, cyber warfare have been extensively studied. What is much less understood, however, is the *intersection* between these two subjects: The contemporary evolution of economic warfare within the new realities of cyberspace has not received the focused, comprehensive scrutiny and policy attention that it warrants. The questions we must be asking and answering are: Within the escalating cyber attacks on U.S. public and private organizations, is there lurking a new type of action – some form of *concerted adversarial strategy* – to undermine the U.S. economically? Are some adversaries' strategies designed to cause economic harm that would weaken or significantly debilitate U.S. security capabilities? To what extent, and when, are they sponsoring proxies to achieve these nefarious goals? Is the U.S. prepared to identify and address such hostile strategies effectively? Does the U.S. government need new collection and analysis platforms to perform this critical function?

It is my contention that the threats are real, the warfare is ongoing, and that the U.S. government is **inadequately structured to properly and comprehensively** detect, evaluate, and address cyber-enabled economic threats. The U.S. government has made great strides in organizing itself to protect and defend the .gov and .mil realms.[1] But our nation's greatest vulnerability may lie with adversarial attacks on the U.S. private sector. And in this regard, the private sector believes it is on its own, a position that is untenable when the adversary is a state actor such as China or North Korea.

Background of the Evolving Battlespace

As we think through our ability as a nation to protect ourselves and our allies, and advance our core interests overseas, the greatest strength we have is our economy. It is our free market, with its ability to efficiently move capital, protect intellectual property, distribute goods, and provide the running room for new ideas and technology to flourish, that creates the most powerful and fearsome military the world has ever known. It is the confidence of the American people that our $18.5-trillion GDP will continue to thrive that provides our leaders the confidence to fund our defense budget. And it is not just the defense industrial base but the broader national security industrial base that underpins it all. Specifically, it is not just the big defense contractors and the big telecommunication companies but everything from the technology startups; to the banks and investment houses that supply capital; to the cars, trucks, trains, and planes that move men and materiel; to the pharmaceuticals and food supplies that care and feed those who protect the free world. Moreover, an April report from the Defense Science Board Task Force on the Cyber Supply Chain warned that the Pentagon can be crippled through maliciously inserted

[1] Vicki Michetti, "DoD's Defense Industrial Base Cybersecurity (DIB CS) Program," *U.S. Department of Defense*, August 24, 2016. (https://www.fbcinc.com/e/cybertexas/presentations/Room_302_Wed_1-145PM_Vicki_Michetti_DIB_101_Cyber_Texas_Aug15.pdf)

vulnerabilities into the weapons and goods that power the U.S. military through entry points in private sector companies.[2]

It is true that the business of America is business. And the business of America is at risk of being hollowed out from the inside by everything from theft of intellectual property to the malicious infection of the supply chain to the degradation of confidence in our commerce, banking, and transportation sectors. The papers are filled with articles about cyber attacks against the private sector to gain profit. No doubt, this is a serious and growing problem. British insurance company Lloyds estimated that cyber attacks cost global businesses as much as $400 billion per year.[3] The internet and its related networked systems provide overwhelming advantages that help an economy to learn, share, and grow, but as we increase our reliance on the electronic movement of data, money, goods, and services, we also increase our vulnerability.[4]

What the $400 billion amount, large as it seems, ignores is the corrosive effect cyber attacks against the private sector can have on a country's military readiness or political sovereignty. The theft of defense-related intellectual property and the corruption of the defense supply chain has been widely reported, and the possible damage these hostile actions could inflict upon our weapons systems has raised alarms throughout the Pentagon and on Capitol Hill.[5] The more pernicious, and less recognized, effect is the degrading of the entrepreneurial motivation that occurs with the systematic and wholesale theft of intellectual property from its creators and owners. As a result of sustained cyber attacks, startups may not get financing because their IP is stolen and established companies may be forced to shut down for days because of malware incidents, projects may get cancelled, and people may get laid off. And it is the small- and medium-sized enterprises – the very companies where the most innovative work is being done that eventually finds its way into our military – that are often hit hardest by cyber attacks.[6] A 2012 U.S. Patent and Trademark Office report aptly summed it up this way: "Every job in some way produces, supplies, consumes, or relies on innovation, creativity, and commercial distinctiveness. Protecting our ideas and intellectual property (IP) promotes innovative, open, and competitive markets."[7] With estimates of the annual costs of trade secret theft in the U.S. ranging from $180 billion to $540 billion, the long-tailed drag on the economy must be recognized for the crisis it is, with a disproportionate burden falling on the very startups and

[2] U.S. Department of Defense, Defense Science Board, "Cyber Supply Chain," April 2017. (http://www.acq.osd.mil/dsb/reports/2010s/DSBCyberSupplyChain_ExecSummary_Distribution_A.PDF)
[3] Stephen Gandel, "Lloyd's CEO: Cyber attacks cost companies $400 billion every year," *Fortune*, January 23, 2015. (http://fortune.com/2015/01/23/cyber-attack-insurance-lloyds/)
[4] Steve Morgan, "IBM's CEO On Hackers: 'Cyber Crime Is The Greatest Threat To Every Company In The World,'" *Forbes*, November 24, 2015. (https://www.forbes.com/sites/stevemorgan/2015/11/24/ibms-ceo-on-hackers-cyber-crime-is-the-greatest-threat-to-every-company-in-the-world/#1db8a3473f07)
[5] Ellen Nakashima, "Confidential report lists U.S. weapons system designs compromised by Chinese cyberspies," *The Washington Post*, May 27, 2013. (https://www.washingtonpost.com/world/national-security/confidential-report-lists-us-weapons-system-designs-compromised-by-chinese-cyberspies/2013/05/27/a42c3e1c-c2dd-11e2-8c3b-0b5e9247e8ca_story.html?utm_term=.afe441d46dc3)
[6] According to the 2012 Verizon Breach report, 71 percent of companies with less than 100 employees have suffered a cyber attack. "2012 Data Breach Investigations Report," *Verizon*, 2012, page 11. (http://www.verizonenterprise.com/resources/reports/rp_data-breach-investigations-report-2012_en_xg.pdf)
[7] "Economics and Statistics Administration and U.S. Patent and Trademark Office, "Intellectual Property and the U.S. Economy: Industries in Focus," March 2012. (https://www.uspto.gov/sites/default/files/news/publications/IP_Report_March_2012.pdf)

innovation leaders that the U.S. and other developed nations credit with building the future economy, enhancing military readiness, and safeguarding sovereignty.[8] As the U.S. government better develops systems to cooperate with and defend the private sector, protecting these types of startups and innovative companies should be a priority given the disproportionate role they play in determining future national power.

The very well-researched IP Commission Report from the National Bureau of Asian Research discusses at length the follow-on effects from IP theft, including advantaging our adversaries both in the market and on the battlefield as well as chilling the innovative spirit that creates the technological breakthroughs upon which our economy and military rely.[9] Therefore, it is not the pure cyber criminal that should keep this committee up at night. Rather, it is the hostile state actor who recognizes that while it may not be able to compete directly with America's strength of arms, it holds a significant asymmetric advantage in attacking our economic wherewithal and, by so doing, weaken us militarily or politically.

We call this purposeful strategy Cyber-Enabled Economic Warfare (CEEW).

Cyber-enabled economic warfare is distinct from cyber crime and cyber terrorism – although both may be part of a larger CEEW campaign. What distinguishes CEEW attacks from other types of cyber attacks is the motivation and strategy. A CEEW campaign is driven by strategic intent to degrade the military and political capabilities of an adversary. States can now use cyber means as just one more part of their economic warfare toolbox.

Economic warfare goes back as far as the Bible and was used throughout history in the form of blockades, trade embargoes, blacklists, sanctions, tariff and/or quota discrimination, sabotage of economic targets, preclusive purchase of scarce critical resources, and expropriation. During World War II, Britain created the Ministry of Economic Warfare "to so disorganize the enemy's economy as to prevent him from carrying on the war."[10] In more recent times, economic warfare has also encompassed the freezing of capital assets, counterfeiting, suspending foreign aid, and restricting foreign investment and capital flows. Over the last few decades, the U.S. has relied heavily on economic sanctions (a form of economic warfare) to curtail the illicit, illegal, and dangerous actions and behaviors of rogue countries such as Saddam Hussein's Iraq, the Islamic Republic of Iran, and, of course, the Kim family's DPRK.

---

[8] "Update to the IP Commission Report: the Theft of American Intellectual Property: Reassessments of the Challenge and United States Policy," *National Bureau of Asian Research* on behalf of the *Commission on the Theft of American Intellectual Property*, 2017. (http://www.ipcommission.org/report/IP_Commission_Report_Update_2017.pdf); "Economic Impact of Trade Secret Theft: A Framework for Companies to Safeguard Trade Secrets and Mitigate Potential Threats," *Center for Responsible Enterprise and Trade* and *PricewaterhouseCoopers*, 2014. (https://create.org/resource/economic-impact-oftrade-secret-theft)

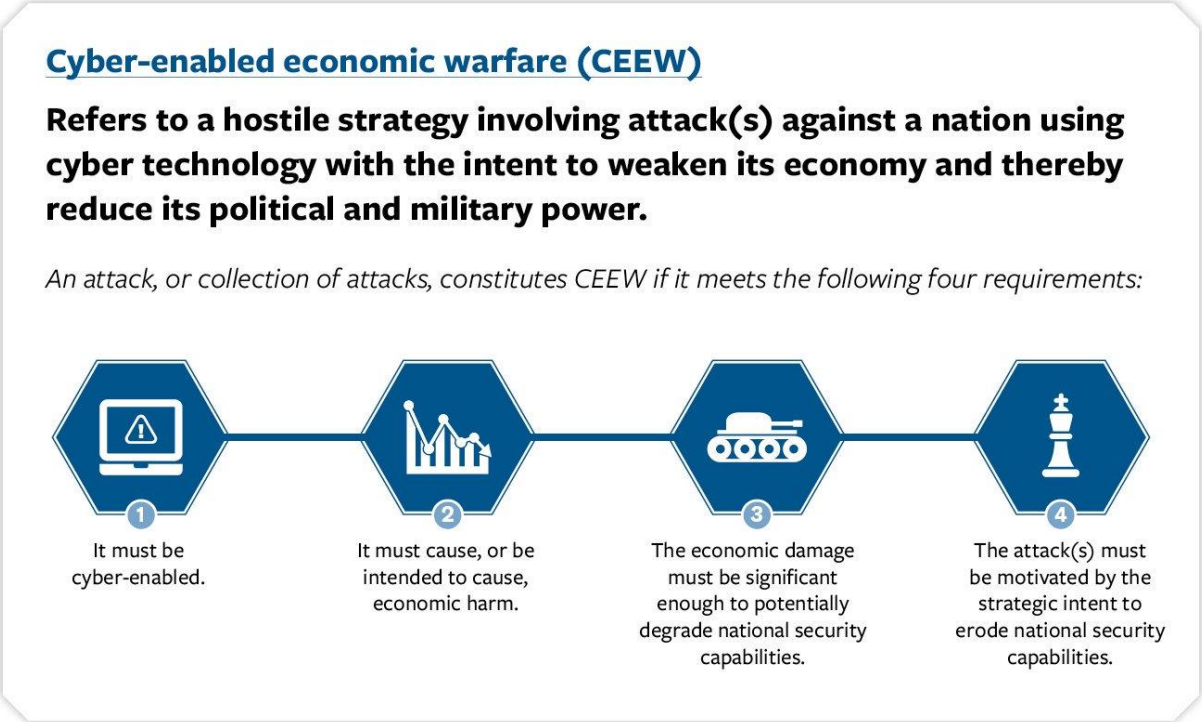
[9] "Update to the IP Commission Report: the Theft of American Intellectual Property: Reassessments of the Challenge and United States Policy," *National Bureau of Asian Research* on behalf of the *Commission on the Theft of American Intellectual Property*, 2017. (http://www.ipcommission.org/report/IP_Commission_Report_Update_2017.pdf)

[10] W.N. Medlicott, *The Economic Blockade (Volume I)*, (London: His Majesty's Stationery Office, 1952). (https://archive.org/stream/economicblockade012328mbp/economicblockade012328mbp_djvu.txt)

But in the past quarter century, there has emerged a vitally important new potential form of economic warfare. The advent of the Information Age and its accompanying "virtual" world of cyberspace has produced the potential for the use of cyber-enabled attack methods to cause an adversary economic harm that is far disproportionate to the size, resources, or efforts of the attacker.

To rise to the level of Cyber-Enabled Economic Warfare, the attack must:

- Be cyber-enabled.
- Cause, or be intended to cause, economic harm.
- Be significant enough to potentially degrade national security capabilities.
- Be motivated by the strategic intent to erode national security capabilities.[11]



State Adversaries

Ten years ago this past April, the small country of Estonia suffered a Russia-supported cyber invasion.[12] The ostensible cause of the invasion was the anger of ethnic Russians and their

[11] For a more fulsome discussion of what constitutes a cyber-enabled economic warfare attack, see Samantha F. Ravich and Annie Fixler, "Framework and Terminology for Understanding Cyber-Enabled Economic Warfare," *Foundation for Defense of Democracies*, February 22, 2017. (http://www.defenddemocracy.org/content/uploads/documents/MEMO_CyberDefinitions_07.pdf)

[12] Emily Tamkin, "10 Years After the Landmark Attack on Estonia, Is the World Better Prepared for Cyber Threats?" *Foreign Policy*, April 27, 2017 (http://foreignpolicy.com/2017/04/27/10-years-after-the-landmark-attack-on-estonia-is-the-world-better-prepared-for-cyber-threats/); Joshua Davis, "Hackers Take Down The Most Wired Country In Europe," *Wired*, August 21, 2007. (https://www.wired.com/2007/08/ff-estonia/); Christian Lowe,

Moscow backers over the relocation of a World War II memorial in the Estonian capital. The larger setting was that Vladimir Putin deeply resented Estonia's accession to NATO and decided to inflict great harm on that country's economy and public sector by cyber means. The first round began on April 26, 2007 when the initial attacks brought down the Estonian government's websites. The prime minister's office as well as the offices of the minister of defense, political parties, and the parliament were all crippled by distributed denial of service (DDoS) attacks. The attack undermined the ability of the government to communicate with the people. The next round of attacks brought down press outlets covering the crisis, making it harder to inform both the Estonian citizenry and the outside world about what was happening. Waves and waves of denial of service and malware attacks on all aspects of Estonian life, culture, civil society occurred over the next two weeks.

What made this cyber attack even more alarming was that, on May 9, the financial system was figuratively brought to its knees. Hansabank, Estonia's largest bank, experienced a sustained attack and had to cease operations, cutting off nearly all Estonians from accessing their capital. ATMs would not dispense money. People panicked. The citizenry lost faith in its banking sector. Apparently having gotten their message across that they could attack where and when they chose and then recede into the darkness, the aggressors stopped the attacks on May 19 as quickly as they had begun.

It is important to recognize the likely effect of similar actions if taken against the United States, where nearly 50 percent of Americans live paycheck to paycheck. If those Americans could not access their ATMs or get their paycheck in time, a hundred million of our citizens would quickly have no money to buy food for their families, diapers for their babies, or their much-needed medicine.

Estonia suffered a large-scale but relatively unsophisticated Russian cyber attack. While most Russian cyber attacks seem aimed at political institutions and more direct military targets, it is not a stretch to envision Russia retaliating for any new sanctions against it by going after our own economic wherewithal. It was only five years ago, we should recall, when an Iranian cyber attack brought down the state-owned Saudi Arabian oil company Aramco's network, destroying 35,000 computers and putting 10 percent of the world's oil at risk. In one day, Aramco bought 50,000 new hard drives – a cost that would have bankrupted most companies.[13]

While it is important to understand the strategies of all U.S. adversaries and competitors, two of the most active players in the field of cyber-enabled economic warfare are the Chinese and North Koreans. Often the discussion focuses on how China steals trade secrets to advantage its own industries and Pyongyang steals money because North Korea has no real economy. While these motivations may explain part of what is occurring, it appears that both of these actors may have a much broader strategy in play.

"Kremlin loyalist says launched Estonia cyber-attack," *Reuters*, March 13, 2009. (http://www.reuters.com/article/us-russia-estonia-cyberspace-idUSTRE52B4D820090313)

[13] Nicole Perlroth, "In Cyberattack on Saudi Firm, U.S. Sees Iran Firing Back," *The New York Times*, October 23, 2012. (http://www.nytimes.com/2012/10/24/business/global/cyberattack-on-saudi-oil-firm-disquiets-us.html?_r=0); Jose Pagliery, "The inside story of the biggest hack in history," *CNN*, August 5, 2015. (http://money.cnn.com/2015/08/05/technology/aramco-hack/)

***China*:** Beginning as early as the 1970s, China has been engaged in a massive, prolonged campaign of intellectual property theft against U.S. firms.[14] Over time, China has increasingly been conducting this campaign via cyber-enabled technologies, targeting nearly every sector of the U.S. economy. While the exact amount such theft has cost U.S. companies in dollars and American citizens in jobs is unknown, it has been estimated to be as high as hundreds of billions of dollars and more than two million jobs.[15] In the aggregate, the effects on the U.S. private sector include, according to the IP Commission: "Lost sales; lost brand value; reduced scope of operations; lost jobs and reduced ability to provide employee benefits; reduced ability to conduct R&D; increased IP protection expenses for prevention, remediation, and enforcement; increased costs from dealing with malware acquired from unlicensed software; [and] reduced incentive to innovate."[16]

China's IP theft campaign constitutes a large, if not the largest, part of what appears to be Beijing's overall cyber-enabled economic warfare strategy against the U.S. and the West more generally. Illustrative of this intention are the words by PLA Colonels Qiao Liang and Wang Xiangsui in their book *Unrestricted Warfare*, where they describe CEEW as "a form of non-military warfare which is just as terribly destructive as a bloody war, but in which no blood is actually shed."[17]

However, Washington and its allies have been slow to comprehend the threat, primarily because they view each attack individually as a separate incident instead of collectively as elements in an overall coordinated campaign. For example, in May 2014, the Department of Justice charged five Chinese hackers who targeted American companies in the nuclear power, metals, and solar industries with only computer crimes and espionage.[18] Similarly, accusations against China for theft of U.S. Steel's proprietary information claim only that Beijing is focused on market share,[19] without understanding how this fits into the larger collective pattern.

---

[14] Christopher Cox, "Report of the Select Committee on U.S. National Security and Military/Commercial Concerns with the People's Republic of China," *U.S. House of Representatives*, May 1999. (https://www.congress.gov/105/crpt/hrpt851/CRPT-105hrpt851.pdf)

[15] Lesley Stahl, "The Great Brain Robbery," *CBS News*, January 17, 2016. (http://www.cbsnews.com/news/60-minutes-great-brain-robbery-china-cyber-espionage/); "The IP Commission Report: The Report of the Commission on the Theft of American Intellectual Property," *The National Bureau of Asian Research* on behalf of the *Commission on the Theft of American Intellectual Property*, 2013. (http://www.ipcommission.org/report/ip_commission_report_052213.pdf)

[16] "The IP Commission Report: The Report of the Commission on the Theft of American Intellectual Property," *The National Bureau of Asian Research* on behalf of the *Commission on the Theft of American Intellectual Property*, 2013, page 29. (http://www.ipcommission.org/report/ip_commission_report_052213.pdf)

[17] Qiao Liang and Wang Xiangsui, *Unrestricted Warfare*, Trans. Foreign Broadcast Information Service (Beijing, China: PLA Literature and Arts Publishing House, February 1999), page 51. (http://www.terrorism.com/documents/unrestricted.pdf)

[18] U.S. Department of Justice, Press Release, "U.S. Charges Five Chinese Military Hackers for Cyber Espionage Against U.S. Corporations and a Labor Organization for Commercial Advantage," May 19, 2014. (https://www.justice.gov/opa/pr/us-charges-five-chinese-military-hackers-cyber-espionage-against-us-corporations-and-labor)

[19] John W. Miller, "U.S. Steel Accuses China of Hacking," *The Wall Street Journal*, April 28, 2016. (http://www.wsj.com/articles/u-s-steel-accuses-china-of-hacking-1461859201)

Of late, Beijing has flexed its cyber-enabled economic powers of coercion and intimidation more overtly. In July 2016, loudspeakers and screens of Vietnam Airlines in that country's two largest airports were hacked, and flight and safety information was overridden by offensive messages about Vietnam's claims to the South China Sea. Although there is some debate regarding the ultimate culprit, the cyber attack did come on the heels of the Hague's Permanent Court of Arbitration's ruling against China and in favor of the Philippines in their territorial dispute. The Vietnam Security Information Association said that the attacks were "deliberate" and "well-planned" and appeared to be part of an escalating pattern by China that took a more formal shape in the immediate aftermath of China's placement of an oil rig in Vietnam's exclusive economic zone.[20] The particular attack did little damage aside from inconveniencing passengers who had to wait for the analog system to kick in, but if replicated and expanded, it could shake the trust in the airline and transportation system of that country. Already, Vietnamese companies are worried about the toll Chinese cyber-enabled economic warfare will take on their own businesses. A 2014 survey found that "20 percent of respondent firms expressed concerns that the East Sea/South China Sea tensions could threaten their information security."[21]

South Korean firms have also begun to feel China's cyber-enabled economic wrath. When Beijing was informed that the United States was accelerating the deployment of its Terminal High Altitude Area Defense (THAAD) system to South Korea as a response to North Korea's latest missile tests, the PRC immediately began to bring pressure on South Korean private firms operating in China. Lotte, a South Korean conglomerate that sold its government a golf course to be used for THAAD, felt the pain almost immediately. Chinese authorities shuttered nearly two-dozen Lotte stores on the mainland,[22] using the flimsy excuse that the government only just discovered that the stores did not comply with existing fire regulations.[23] Additionally, the website for the Lotte Group was brought down by a denial-of-service (DDoS) attack originating from Chinese internet addresses,[24] and a number of Chinese e-commerce sites halted sales of Lotte goods. Estimates of lost business and damage are in the hundreds of thousands of dollars.[25] Although the damage is a small dollar figure compared to Lotte's total income from 150 chemical plants, supermarkets, and other facilities operating in China, the move has prompted deep concern in Seoul. South Korea exported over $120 billion to China last year, about a quarter of the country's total exports, and is particularly vulnerable to Chinese coercion.

---

[20] Helen Clark, "The Alleged Chinese Hacking at Vietnam's Airports Shows That the South China Sea Battle Isn't Just in the Water," *The Huffington Post*, accessed June 7, 2017. (http://www.huffingtonpost.com/helen-clark1/china-hack-vietnam-south-china-sea_b_11357330.html)

[21] "Vietnam vulnerable to cyber attacks but agencies poorly equipped," *Than Nien News* (Vietnam), December 10, 2014. (http://www.thanhniennews.com/tech/vietnam-vulnerable-to-cyber-attacks-but-agencies-poorly-equipped-34980.html)

[22] Javier Hernandez, Owen Guo, and Ryan McMorrow, "South Korean Stores Feel China's Wrath as U.S. Missile System Is Deployed," *The New York Times*, March 9, 2017. (https://www.nytimes.com/2017/03/09/world/asia/china-lotte-thaad-south-korea.html?_r=2)

[23] Jethro Mullen and Sol Han, "One company is bearing the brunt of China's anger over U.S. missile system," *CNN*, March 7, 2017. (http://money.cnn.com/2017/03/07/news/china-lotte-thaad-south-korea-tensions/)

[24] Joyce Lee and Heekyong Yang, "South Korea's Lotte Duty Free says website crashed after attack from Chinese IPs," *Reuters*, March 2, 2017. (http://www.reuters.com/article/us-lotte-china-idUSKBN1690HR)

[25] Shin Ji-hye, "Cyberattacks open new front in Korea, China THAAD spat," *The Korea Herald* (South Korea), March 9, 2017. (http://www.koreaherald.com/view.php?ud=20170309000792)

In one of his first issues taken up upon entering office, the new South Korean president, Moon Jae-in, sent an emissary to meet with Chinese President Xi. In the aftermath of the meeting, Lotte's website was unblocked. Days later, President Moon suspended the deployment of THAAD.[26]

***North Korea*:** As early as 2009, North Korea was already initiating malicious cyber attacks on its adversaries. That summer there was a wave of destructive denial of service attacks perpetrated against "websites of the Departments of Homeland Security, Treasury, Transportation, the Secret Service, the FTC, the New York Stock Exchange, and NASDAQ, as well as dozens of South Korean banks, affecting at least 60,000, and possibly as many as 160,000 computers."[27]

In March 2013, North Korean hackers attacked South Korean banks and media companies using malware dubbed "DarkSeoul," destroying tens of thousands of computers, deleting data from hard drives and overwriting Master Book Records, and rendering many banking services inoperable.[28] North Korea's intentions in the March 2013 attacks were not purely economic or commercial – that is, Pyongyang was not interested in advantaging its own media companies and financial institutions within the South Korean market by taking out their competitors. Rather, North Korea attacked South Korea's economic resources in order to threaten its economy and affect Seoul's national security decision-making. North Korea engaged in a systematic operation, which continues today, to disrupt elements of the South Korean economy in order to sap the strength of the country – financially and militarily. Indeed, South Korean police cyber investigators stated in 2016 that North Korea had operationalized a long-term plan involving the seeding of malicious code in more than 140,000 computers at over 160 South Korean firms and government agencies.[29] The police concluded that the DPRK likely "aimed to cause confusion on a national scale by launching a simultaneous attack after securing many targets of cyber terror, or intended to continuously steal industrial and military secrets."

More recently, it was reported that North Korean hackers most likely initiated the WannaCry ransomware attack that spread to hundreds of thousands of computers worldwide.[30] The monetary haul from the scheme was minimal, leading some analysts to question if the effort was a test for a larger attack. Similar assessments have been made about the 2016 cyber bank heist

---

[26] Paul Mcleary, "In Nod to China, South Korea Halts Deployment of THAAD Missile Defense," *Foreign Policy*, June 7, 2017. (http://foreignpolicy.com/2017/06/07/in-nod-to-china-south-korea-halts-deployment-of-thaad-missile-defense/)

[27] Fred Kaplan, *Dark Territory: The Secret History of Cyber War* (New York: Simon & Schuster, 2016), page 213.

[28] Choe Sang-Hun, "Computer Networks in South Korea Are Paralyzed in Cyberattacks," *The New York Times*, March 20, 2013. (http://www.nytimes.com/2013/03/21/world/asia/south-korea-computer-network-crashes.html); K.J. Kwon, "Smoking Gun: South Korea uncovers northern rival's hacking codes," *CNN*, April 22, 2015. (http://www.cnn.com/2015/04/22/asia/koreas-cyber-hacking/); "Four Years of DarkSeoul Cyberattacks Against South Korea Continue on Anniversary of Korean War," Semantec Security Response, June 26, 2013. (https://www.symantec.com/connect/blogs/four-years-darkseoul-cyberattacks-against-south-korea-continue-anniversary-korean-war)

[29] Jack Kim, "North Korea mounts long-running hack of South Korea computers, says Seoul," *Reuters*, June 13, 2016. (http://www.reuters.com/article/us-northkorea-southkorea-cyber-idUSKCN0YZ0BE)

[30] Choe Sang-hun, paul Mozur, Nicole Perlroth, and David Sanger, "Focus Turns to North Korea Sleeper Cells as Possible Culprits in Cyberattack," *The New York Times*, May 16, 2017. (https://www.nytimes.com/2017/05/16/world/asia/north-korea-cyber-sleeper-cells-ransomware.html?smid=tw-nytimes&smtyp=cur&_r=2)

that attempted to withdraw $1 billion from Bangladesh's account at the New York Federal Reserve. Assessments now tie this attack back to the North Korean cyber group Lazarus. While some in the U.S. government have remarked that, if true, it appears that the North Koreans are now robbing banks, it is more chilling to consider that, if true, the North Koreans are now targeting our banking sector.[31]

With a GDP per capita of barely $1,000 and its single largest source of foreign currency coming from sales of coal to China, North Korea has an obvious need to rob foreign banks. But Kim Jong Un is not simply a Korean Willie Sutton. In a military confrontation with the U.S. and South Korea, Kim would look to any capability that could help even out the overwhelming military advantage of the allies. Attacking our economies, which he has already proven he can and will do, may be the quickest way to gain battlefield advantage since it could potentially cause panic in our markets and on our streets.

Policy Recommendations: Without a concerted effort, the United States economy will become increasingly vulnerable to hostile adversaries seeking to undermine our military and political strength. The U.S. government, both the Congress and the executive branch, need to immediately undertake a number of actions to prevail in this new battlespace, including:

- **Understanding the Adversary:** There should be sustained attention within the U.S. intelligence community to understanding the capabilities and intentions of adversarial leadership to engage in cyber-enabled economic warfare. This effort should focus both on staying one step ahead of what cyber tools the enemy is creating and fielding (by using U.S intelligence collection platforms to target adversarial science and technology), but also on mapping the command-and-control hierarchy of the enemy's leadership which directs such campaigns, recognizing any internal frictions or vulnerabilities that can be exploited. It is critical to know as much as possible about the man *behind* the man *behind* the computer – because decisions are made by decision-makers, not bots and bits. At least not yet. In the same vein that the U.S. intelligence community studied Soviet leadership through Kremlinology, so too is it time to map the organizational leadership charts for CEEW within the most dangerous enemy states.

- **International Cyber Co-op:** The U.S. cannot go it alone in its endeavor to safeguard the networks and systems upon which our economy depends. We must take steps to formalize the cyber partnerships that already exist with the other free-market democracies that are leaders in cyber science and technology. Such a "co-op" should begin with the U.S., the UK, and Israel, building on the fact that the UK and Israel are world leaders in cyber and already have cyber attachés stationed in Washington. There is growing evidence that the "bad guys" (China, Russia, Iran, and North Korea) cooperate,[32] and the

[31] Jim Finkle, "Cyber security firm: more evidence North Korea linked to Bangladesh heist," *Reuters*, April 3, 2017. (http://www.reuters.com/article/us-cyber-heist-bangladesh-northkorea-idUSKBN1752I4)

[32] Alex Grigsby, "The Next Level For Russia-China Cyberspace Cooperation?" *Council on Foreign Relations*, August 20, 2015. (https://www.cfr.org/blog/next-level-russia-china-cyberspace-cooperation); Riley Waggaman, "Iran and Russia announce plans for cyber security cooperation," *Press TV* (Iran), March 14, 2017. (http://www.presstv.ir/Detail/2017/03/14/514354/Iran-Russia-cyber-security-cooperation); Yeganeh Torbati and Roger Atwood, "Iran, North Korea agree to cooperate in science, technology," *Reuters*, September 1, 2012. (http://www.reuters.com/article/us-korea-north-iran-idUSBRE88005H20120901)

"good guys" must also build better cooperation not only at the declaratory level, but on the strategic and tactical level.

- **Cyber R&D:** While the private sector plays a key role in the creation of new technologies for the ultimate securing of the systems and networks upon which our economic livelihood rests, government R&D is needed to supply certain types of research which the private sector is not likely to advance. As then-Federal Reserve Chair Ben Bernanke commented, the "argument [for government funding of R&D] which applies particularly strongly to basic or fundamental research, is that the full economic value of a scientific advance is unlikely to accrue to its discoverer, especially if the new knowledge can be replicated or disseminated at low cost. For example, James Watson and Francis Crick received a minute fraction of the economic benefits that have flowed from their discovery of the structure of DNA. If many people are able to exploit, or otherwise benefit from, research done by others, then the total or social return to research may be higher on average than the private return to those who bear the costs and risks of innovation. As a result, market forces will lead to underinvestment in R&D from society's perspective, providing a rationale for government intervention."[33] Initial candidates for government CEEW R&D could include everything from protections for legacy supervisory control and data acquisition systems (SCADA) to assessing if and how a new internet protocol needs to be built. Optimally, the "cyber co-op" discussed above could be established with its first task being to create a cyber R&D agenda, with partner countries leveraging their comparative advantage in certain fields while not duplicating the work likely to be produced in the private sector.

- **Understanding the Scale, Scope, and Evolution of the Threat:** As we better understand the strategies of our adversaries and build better cooperation with our allies, we must also understand the evolution of the threats. An open-source database, searchable by tags such as targeted industry and type of attack, should be funded and made available to the government, researchers, and the private sector. While both the Cyber Threat Intelligence Integration Center, housed in the Office of Director of National Intelligence, and the National Cybersecurity and Communications Integration Center (NCCIC) of the Department of Homeland Security exist in some form or fashion to increase the sharing of cyber security-related information within federal and, in the case of NCCIC, non-federal entities, neither funds a comprehensive database of cyber attacks and incidents across the private sector. Consequently, most of U.S. policy and operations are built on anecdotal observations from single cases, which are then used to speculate about attack patterns and potential. We are virtually blind to the context and setting of cyber conflict unless we have a macro-level data source that provides this key information.[34] Such a database could shed much needed light on the scale, scope, and evolution of the threat against our economic foundation as well as serve as a way to gauge whether actions taken against the adversary are succeeding in deterring malicious behavior.

[33] Federal Reserve Chairman Ben Bernanke, "Promoting Research and Development: The Government's Role," *Speech at the Conference on "New Building Blocks for Jobs and Economic Growth,"* May 16, 2011. (https://www.federalreserve.gov/newsevents/speech/bernanke20110516a.htm)

[34] From a research proposal submitted to the author by Brandon Valeriano and Christopher Whyte.

- **Creating a Whole of Government CEEW OODA Loop.** Using the platforms above, the U.S. government should create a whole of government OODA (observe, orient, decide, and act) loop so that it can properly assess the enemy's escalatory ladder and better recognize if our defensive and offensive actions are actually minimizing and deterring hostile activity. Without such an informed assessment, we run the risk of being too timid to use our capabilities against the enemy on the one hand or potentially exacerbating a fraught situation on the other. In practice, this would mean more coordination across the government on everything from the tasking of the collection of the relevant CEEW intelligence to a better understanding of how the threat is evolving to the sharing of hard data on what is being attacked to the analysis of theories and practice for deterring and responding to the enemy.

While the analogies to the dawn of the nuclear age can be overdrawn when laid over the challenges we now face in cyber-enabled economic warfare, today's legislators, decisionmakers, and operators can learn a lot from the rigorous thought that went into assessing the types of intelligence collection platforms, targeting processes, and analytic methods created to deal with that challenge. In this new threat environment, we are akin to the late 1940s or early 1950s in how to organize ourselves as a government. We have much work to do.

Thank you for the opportunity to testify. I look forward to your questions.

"Living in a Glass House: The United States Must Better Defend Against Cyber and Information Attacks"

Prepared Statement
by
Honorable Eric Rosenbach
Co-Director of Belfer Center at Harvard Kennedy School; former Assistant Secretary of Defense for Homeland Defense and Global Security

Before the
United States Senate Foreign Relations Committee
Subcommittee on East Asia, the Pacific, and International Cybersecurity Policy

Hearing on

State-Sponsored Cyberspace Threats: Recent Incidents and U.S. Policy Response
June 12, 2017

Chairman Gardner, Ranking Member Markey and other distinguished members of the Committee, thank you for calling today's hearing on cybersecurity and for the invitation to testify.

As technology advances and we become more connected, we increasingly live in a digital "glass house" that must be much better protected. I like to use the glass house analogy because it helps illustrate two important points.

First, that cyber warfare is truly asymmetric: a small nation with an offensive cyber capability can have an outsized effect on a larger power. For example, the US—a technological and economic powerhouse—is significantly more vulnerable to cyberattack than North Korea, a nation where most citizens do not even have an internet connection. We should therefore think very carefully about the implications of a possible North Korean cyberattack on the United States, something that I believe is likely to happen within the next year if current trends continue.

Second, that democracies' transparent, open societies also make them vulnerable to foreign information operations. This vulnerability is exacerbated by high levels of internet accessibility and the rapid pace and breadth of information sharing. In contrast, authoritarian societies like China, Russia and North Korea often control the media, censor domestic online activity and shield

their nations (to some degree) from outside information and cyber operations through the use of national-level firewalls, such as the Great Firewall of China.

Unfortunately, no nation, including the United States, has responded to Russia's recent potent hybrid of cyber and information attacks in a way that is visible and forceful enough to deter future attacks. The fragility of our national cybersecurity posture, combined with our adversaries' perception that Russia's recent actions achieved unprecedented success, increases the likelihood that the US and our allies will experience more serious attacks in the coming years.

Thus, the US needs to bolster its deterrence posture by both raising the costs and decreasing the benefits to hostile actors of engaging in this conduct.

In 2015, the Department of Defense articulated for the first time our strategy on deterrence in cyberspace. In sum, the strategy articulated that deterrence is partially a function of perception. As the DoD strategy explains, deterrence works by "convincing a potential adversary that it will suffer unacceptable costs if it conducts an attack on the United States, and by decreasing the likelihood that a potential adversary's attack will succeed."[1]

In terms of increasing the costs of an attack, the US and international community should be less circumspect about employing all available foreign policy tools, particularly those outside of the cyber domain. Given the "glass house effect" that I previously described, we should be careful about responding to cyberattacks with military options since the US has more to lose from an escalation in cyber-initiated conflict. We should, however, be prepared to use our superior cyber capability strategically and creatively in order demonstrate our willingness to act in the face of serious provocations.

Additionally, the US must increase the costs of cyber and information operations by using foreign policy tools outside the military domain, such as: 1) attributing publicly cyber and information attacks as soon as we have confidence the origins; 2) pushing for sustained multi-lateral economic sanctions against states that use cyber and information weapons; 3) reinventing our capabilities with respect to information operations and our strategy for countering them; and 4) taking a leading role in building international capacity to disrupt the proliferation of black-market destructive malware.[2]

As I mentioned, reducing the benefits that adversaries derive from cyber and information operations is a key aspect of bolstering our deterrence posture. To do this, the Administration, Congress and private sector should work together to: 1) pass legislation that improves the ability

---

[1]The Department of Defense Cyber Strategy, April 2015, p.11.

[2] By disrupting the black market for destructive malware and other exploits, the international community would increase the costs associated with conducting? cyber and information attacks. This is a difficult challenge, but the Proliferation Security Initiative for weapons of mass destruction—a global initiative supported by over 100 countries—provides an analogous model for action.

for the government and private sector to share cyber threat information, including with state election bodies and campaigns; 2) legislate mandatory compliance with the NIST's Cybersecurity Framework for critical infrastructure providers; 3) pursue more aggressive steps to mitigate the effect of information operations on the platforms of leading tech companies, including Facebook, Twitter and Google; and 4) incentivize investment in cloud-based security, blockchain-enabled transactions and quantum computing.

Developing and employing operational cyber capabilities is an important way to advance US national interests. That said, we simply must keep sensitive vulnerabilities and exploits secure. Allowing this type of sensitive knowledge to get into the public domain damages American tech firms and increases the likelihood that hostile actors will conduct malicious actions against the US.

In sum, the strength of the tech sector and the internet has driven American economic growth and strengthened our democracy for the past two decades. The corollary of this success, though, is that the US is increasingly vulnerable to cyber and information attacks. In order to maintain the "center of gravity" for the United States, we must bolster America's cybersecurity posture and rethink our strategy for countering foreign information operations.