Center for Cyber
& Homeland Security

THE GEORGE WASHINGTON UNIVERSITY

"A Global Perspective on Cyber Threats"

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

Before the U.S. House of Representatives, Committee on Financial Services, Subcommittee on Oversight and Investigations

Tuesday June 16, 2015

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

Introduction

Thank you, Chairman Duffy, Ranking Member Green, and distinguished Subcommittee Members 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.

The U.S. financial services sector in particular is in the crosshairs as a primary target. To give you a sense of the magnitude of the problem, consider the following figures which were provided to me recently by a major U.S. bank on a not-for-attribution basis: just last week, they faced 30,000 cyber- attacks. This amounts to an attack every 34 seconds, each and every day. And these are just the attacks that the bank actually knows about, by virtue of a known malicious signature or IP address. As for the source of the known attacks, approximately 22,000 came from criminal organizations; and 400 from nation-states.

This pace 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. 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. The financial services sector understands this well and should therefore serve as a model for other sectors which are simply not as far along on the learning curve. Indeed, up until recently, even the financial sector invested overwhelmingly (85%) in prevention .

While Wall Street has made significant strides and is investing heavily in shoring up their cybersecurity, Main Street—meaning small and medium sized businesses, including the regional banks—lags far behind. This issue will

become increasingly salient as the threat continues to migrate along the spectrum, shifting its focus from harder targets like big business to encompass medium-sized and smaller enterprises.

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.

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.

- 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.

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

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

- 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.

- Finally, banking and financial services are primary targets for cyber-attacks and cybercrimes. Directed against this truly critical infrastructure, cyber-attacks or a concerted campaign against U.S. banks, exchanges, clearinghouses, and markets—hold 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.

How do these actors function?

Our adversaries have engaged in brazen activity, from computer network exploitation (CNE) to computer network attack (CNA). CNE includes

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

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. 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.[1]

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

[1] http://blogs.wsj.com/cio/2015/04/28/cyber-deterrence-is-a-strategic-imperative/

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

espionage, characterizing these activities as rising to the level of strategic threat to the U.S. national interest.[2]

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."[3]

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.

Just this month, 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.[4]

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, cyber, and other operations to collect economic information and technology to support Russia's economic development and security. Russia's extensive

[2]http://www.ncix.gov/publications/reports/fecie_all/Foreign_Economic_Collection_2011.pdf
[3] http://www.uscc.gov/RFP/2012/USCC%20 Report_Chinese_CapabilitiesforComputer_NetworkOperationsandCyberEspionage.pdf
[4] https://theconversation.com/massive-government-employee-data-theft-further-complicates-us-china-relations-42941; and http://www.darkreading.com/attacks-breaches/state-owned-chinese-firms-hired-military-hackers-for-it-services/d/d-id/1269102

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

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.[5]

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.[6]

More recently, Russian hackers believed to be doing their government's bidding breached the White House, the State Department, and the Defense Department.[7] 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.[8]

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. Equally concerning, if not more so, Russia and China

[5] http://www.ncix.gov/publications/reports/fecie_ all/Foreign_Economic_Collection_2011.pdf
[6] http://www.bloomberg.com/bw/articles/2014-07-17/how-russian-hackers-stole-the-nasdaq
[7] http://www.cnn.com/2015/04/07/politics/how-russians-hacked-the-wh/; and http://thehill.com/policy/cybersecurity/242213-pentagon-head-russian-goals-not-clear-in-dod-hack
[8] http://thehill.com/policy/cybersecurity/241965-russian-hacking-group-was-set-to-hit-us-banks; https://www.fireeye.com/blog/threat-research/2014/10/apt28-a-window-into-russias-cyber-espionage-operations.html; http://www.newsweek.com/how-stop-putin-hacking-white-house-321857; and http://www.cnbc.com/id/102025262

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

recently signed a cybersecurity agreement pursuant to which they pledge not to hack one another and to share both information and technology.[9]

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.[10] 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."[11]

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."[12]

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 current international negotiations on containing that program will affect Iran's behavior in the cyber domain, moving forward, remains to be seen.

---

[9] http://www.afpc.org/files/august2012.pdf; and http://thehill.com/policy/cybersecurity/241453-russia-china-unit-with-major-cyber-pact
[10] http://www.theregister.co.uk/2015/04/16/cyber_war_keynote_infiltrate/
[11] http://www.wired.com/2013/09/dont-leave-home/
[12] http://thehill.com/policy/cybersecurity/236627-iranian-leader-has-boosted-cyber-spending-12-fold

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

What we do know is that Iran has engaged in a concerted cyber campaign against U.S. banks.[13] In January 2013, the Wall Street Journal reported[14] 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."[15]

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.[16]

In addition, elements of Iran's Revolutionary Guard Corps (IRGC) have also openly sought to pull hackers into the fold, including the political/criminal

[13] http://foreignpolicy.com/2014/02/18/forget-china-irans-hackers-are-americas-newest-cyber-threat/
[14] http://www.wsj.com/articles/SB10001424127887324734904578244302923178548
[15] http://www.bloomberg.com/bw/articles/2014-12-11/iranian-hackers-hit-sheldon-adelsons-sands-casino-in-las-vegas
[16] http://www.wired.com/2015/02/nsa-acknowledges-feared-iran-learns-us-cyberattacks/

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

hacker group Ashiyane; and the Basij, who are paid to do cyber work on behalf of the regime.[17]

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."[18] 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.[19]

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'."[20]

Where will the DPRK go from here? In the words of an Australian expert, "There's growing concern amongst analysts, and government officials alike

[17]http://cchs.gwu.edu/sites/cchs.gwu.edu/files/downloads/Testimony_Cilluffo_April_26_2012.pdf
[18] http://www.nknews.org/2015/03/n-korean-hacking-threat-leads-to-blue-house-cyber-security-office/
[19] http://thediplomat.com/2015/04/south-korea-beefs-up-cyber-security-with-an-eye-on-north-korea/
[20] http://www.cbsnews.com/news/north-korean-cyberattack-on-sony-60-minutes/

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

that North Korea has begun to rapidly accelerate its development of advanced offensive cyber capabilities'."[21]

The latter development is 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 assistance to rogue states and non-state actors, would the DPRK also assist them with destructive cyber capabilities'?"[22]

In addition, recent 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.[23]

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

[21] http://www.nknews.org/2015/03/n-korean-hacking-threat-leads-to-blue-house-cyber-security-office/

[22]https://books.google.com/books?id=oG51CAAAQBAJ&pg=PA1&lpg=PA1&dq=north+korea:+the+cyber+wild+card&source=bl&ots=i9IDOgGLS6&sig=xXyFSVkL4LslwPoO6EjWyQc77pI&hl=en&sa=X&ved=0CCYQ6AEwAWoVChMI0eet7fuHxgIVKE2MCh0L_gAv#v=onepage&q=north%20korea%3A%20the%20cyber%20wild%20card&f=false

[23] http://www.reuters.com/article/2015/05/29/us-usa-northkorea-stuxnet-idUSKBN0OE2DM20150529

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

(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.[24]

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. [25] 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.

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.

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

[24]http://cchs.gwu.edu/sites/cchs.gwu.edu/files/downloads/Testimony_Cilluffo_March_20_2013.pdf

[25] http://gizmodo.com/isis-has-a-new-terrorism-tactic-doxing-us-soldiers-1693078782

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

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."[26] 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 of counterfeit goods are carried out. … General trends for cybercrime suggest

[26] http://www.wired.com/2014/11/hacker-lexicon-whats-dark-web/

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

> 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.[27]

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.[28]

While the focus of this hearing is on threat rather than response, it bears mention that it is a relatively small, core group of "kingpins" that constitute the heart of the cybercrime problem. If these key figures could be extradited for prosecution, it would go a long way toward combating the problem—and would represent a much more efficient way of tackling the challenge.

"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. Recall, for example, the activities of

[27] https://www.europol.europa.eu/newsletter/massive-changes-criminal-landscape; and http://cchs.gwu.edu/counterterrorism-cybersecurity-insights-europol-director-rob-wainwright
[28] http://www.group-ib.com/?view=article&id=705

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

"Anonymous," whose significant impact has been felt by targets as diverse as the private intelligence firm Stratfor and opponents of the "Arab Spring."[29]

Conclusion

From the standpoint of banking and financial services in particular—a critical U.S. infrastructure sector, cyber-attacks hold the potential to undermine trust and confidence in the system itself, irrespective of the perpetrator. This is just one of many reasons that it is imperative to bolster U.S. prevention, resilience, and response efforts—in partnership with the private sector.

Moving forward, and in connection with this last point, the U.S. government must give companies who now find themselves at the tip of the spear, the framework, parameters, and tools that they need in order to engage in active defense to protect themselves.

Thank you again for this opportunity to testify on this important topic. [30] I look forward to trying to answer any questions that you may have.

[29] http://www.wired.com/2012/07/ff_anonymous/

[30] I would like to thank CCHS Associate Director, Sharon Cardash, for her help in drafting my prepared testimony.

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