THE GEORGE WASHINGTON UNIVERSITY
HOMELAND SECURITY POLICY INSTITUTE

"The Iranian Cyber Threat to the United States"

The U.S. House of Representatives

Committee on Homeland Security

Subcommittee on Counterterrorism and Intelligence; and

Subcommittee on Cybersecurity, Infrastructure Protection and Security Technologies

April 26, 2012

Statement of Frank J. Cilluffo

Director, Homeland Security Policy Institute

The George Washington University

Chairman Meehan, Chairman Lungren, Ranking Members Higgins and Clarke, and distinguished Members of the Subcommittees, thank you for the opportunity to testify before you today. The subject is one of national importance — we, as a country, still have work to do in order to best respond to, and get ahead of, threats on the cybersecurity front. Indeed, with regard to cyber, the United States is in a position akin to where the homeland security community was shortly after 9/11. This is problematic in terms of both cybersecurity and infrastructure protection, as well as counterterrorism and intelligence. There are many points of intersection and overlap between these two "lenses"; and if recent history has taught us anything, it is that bureaucratic stovepiping can have fatal consequences. Your demonstrated commitment to tackle the subject under study jointly is therefore all the more commendable, and indeed a model for moving the nation forward on the truly difficult interdisciplinary challenges that characterize the current national security ecosystem.

Iran (its Islamic Revolutionary Guard Corps, and associated Quds Force; the Ministry of Intelligence and Security; etc.) and proxies have long had the United States in their crosshairs. Up until 9/11, in fact, it was Iran's chief proxy, Hezbollah, that held the mantle of deadliest terrorist organization, having killed more Americans up to that point than any other terrorist group. The October 23, 1983 bombing of the U.S. Marine Barracks in Beirut, Lebanon, cost the lives of 241 Soldiers, Marines and Sailors.

The current climate is particularly concerning however, because the level of tension appears to be rising. We have seen an uptick in attempted and actual attacks on and assassinations of Israeli, Jewish, U.S. and Western interests. This past February saw apparently coordinated bomb attacks against the embassies of one ally, Israel, in the capitals of two others—India and Georgia. February also saw Iranian agents in Bangkok prematurely detonate explosives, while preparing devices, resulting in injuries only to the perpetrators. Consider also the recently thwarted Iranian plot to assassinate Saudi Arabia's ambassador to the United States.

While Iran has sought to distance itself from the incidents described above and denied responsibility for them (not credibly mind you), the reach of Iran's proxies has gone global. Hezbollah's activities now stretch from West Africa to the Tri-Border Area of Argentina, Brazil, and Paraguay. Within the United States, there were 16 arrests of Hezbollah activists in 2010 based on Joint Terrorism Task Force investigations in Philadelphia, New York, and Detroit; and the organization has attempted to obtain equipment in the U.S., including Stinger missiles, M-4 rifles, and night vision equipment.[1] Based on recent activity, the Los Angeles Police Department has elevated the Government of Iran and its proxies to a Tier One threat. Notably, the city of Los Angeles contains the most active Hezbollah presence in this country (Detroit is their "traditional" U.S. base of operations). L.A. also happens to be home to the largest ethnic Iranian population outside of Iran itself.

---

[1] Immigration and Customs Enforcement, DHS. "Indictment charges 4 with conspiracy to support Hezbollah 6 others charged with related crimes," press release, November 24, 2009. Accessed 4/23/12 <http://www.ice.gov/news/releases/0911/091124philadelphia.htm>; Mike Newall, "Road to terrorism arrests began at Deptford Mall, Moussa Ali Hamdan's meeting in 2007 with an undercover FBI informant led to the indictment of 26 with alleged Hezbollah ties," *The Philadelphia Inquirer*, January 25, 2010. Accessed 4/23/12 <http://articles.philly.com/2010-01-25/news/25210171_1_hezbollah-fbi-informant-indictment>; and Anti-Defamation League, "Four Men Indicted in Philadelphia for Attempting to Support Hezbollah," modified 6/16/2010. Accessed 4/23/12 <http://www.adl.org/main_Terrorism/philadelphia_hezbollah_indictment.htm>

Law enforcement officials have observed a striking convergence of crime and terror. Hezbollah's nexus with criminal activity is greater than that of any other terrorist group. These links, including with gangs and cartels, generate new possibilities for outsourcing, and new networks that can facilitate terrorist travel, logistics, recruitment, and operations. Authorities have noted significant terrorist interest in tactics, techniques, and procedures used to smuggle people and drugs into the United States from Mexico. According to Texas State Homeland Security Director, Steve McCraw, Hezbollah operatives were captured trying to cross the border in September 2007.[2]

Law enforcement officials also confirm that Shia and Sunni forces are cooperating to an extent. For instance, Shia members of Lebanese Hezbollah and Sunni (Saudi/Iraqi) militant forces are drawing on each other's skills. That said, competition persists even within Shia circles, including between Lebanese Hezbollah and Iran's Quds Force.

These developments suggest that our longstanding frames of reference and the "redlines" they incorporated have shifted. First and foremost: whereas previously Iran and its proxies targeted U.S. interests and personnel abroad, the cleave between here (the homeland) and overseas is wearing away, as the two fronts merge. The Director of National Intelligence recently stated that Iran is "now more willing to conduct an attack in the United States."[3] His assessment does not stand alone. In a recent hearing before the House Committee on Homeland Security, the NYPD's Director of Intelligence Analysis asserted that "New York City and its plethora of Jewish and Israeli targets could be targeted by Iran or Hezbollah in the event that hostilities break out in the Persian Gulf."[4] At the same hearing, the Committee heard from a former Assistant Director of the FBI that Hezbollah's fundraising infrastructure in the United States could serve as a "platform" for launching attacks against the homeland.[5]

With Iran's nuclear program under scrutiny and sanctions, the potential for escalation is heightened. As a result of his policy choices, President Ahmadinejad is under increasing pressure both internationally and domestically.[6] The complexity of the situation is increased by the tendency of Iran and its allies to conflate the United States and our ally Israel in the

---

[2] "Terrorists have been arrested on the border, security chief says," Associated Press, September 13, 2007

[3] Testimony of James R. Clapper before the Senate Select Committee on Intelligence, *Worldwide Threat Assessment of the US Intelligence Community,* January 31, 2012, Washington, D.C., Accessed 4/18/2012 <http://www.dni.gov/testimonies/20120131_testimony_ata.pdf>

[4] Testimony of Mitchell D. Silber before the U.S. House of Representatives Committee on Homeland Security, *Iran, Hezbollah, and the Threat to the Homeland*, March 21, 2012, Washington, D.C.,. Accessed 4/16/2012 <http://homeland.house.gov/sites/homeland.house.gov/files/Testimony-Silber.pdf>

[5] Testimony of Chris Swecker before the U.S. House of Representatives Committee on Homeland Security, *Iran, Hezbollah, and the Threat to the Homeland*, March 21, 2012, Washington, D.C.,. Accessed 4/22/2012 <http://homeland.house.gov/sites/homeland.house.gov/files/Testimony-Swecker.pdf>

[6] Rick Gladstone and Alan Cowell, "Iran's President Unfazed in Parliamentary Grilling," *The New York Times*, March 14, 2012. Accessed 4/18/12 <http://www.nytimes.com/2012/03/15/world/middleeast/iran-ahmadinejad-questioned-before-parliament-majlis.html?_r=1&pagewanted=all>

context of Israeli contingency and attack plans. Events from Baku to Bangkok (referenced above) have been characterized by some analysts as a "shadow war".[7]

The conflict is not limited to the kinetic or to the physical world. In 2010, the Stuxnet worm disabled Iranian centrifuges used to enrich uranium. Attribution for this attack remains unresolved, although speculation has centered on Israel and the United States. The possibility that Iran may feel aggrieved and seek to retaliate, even in the absence of proof of attribution, is not to be dismissed — particularly against the backdrop of ever-tougher U.S. and global sanctions, and historically turbulent (at least as measured in decades) bilateral relations with the United States. The recent SWIFT sanctions have proven particularly effective in crippling Iran's financial system, adding further pressure.[8] Iran is also grappling with Duqu, a worm which seems "designed to gather data to make it easier to launch future cyber attacks."[9]

With Stuxnet, the virtual and real worlds collided, as the worm caused physical damage to infrastructure. Former head of the CIA and the NSA, General Michael Hayden, has (rightly I would suggest) characterized Stuxnet as both "`a good idea'" and "`a big idea'" — suggesting also that it represents a crossing of the Rubicon in that "`someone has legitimated this type of activity as acceptable'."[10] The vulnerability to cyber attack of critical systems, including nuclear facilities and supervisory control & data acquisition (SCADA) / industrial control systems — with concomitant possibility of loss of life, and less than fatal but still serious and widespread consequences — raises a host of implications for U.S. national and homeland security. Potential targets are many and varied, and extend to critical sectors such as finance and telecommunications. Assistant to the President for Homeland Security and Counterterrorism, John O. Brennan, has stated that U.S. water and power systems are under cyber attack almost daily.[11] Press reports also suggest that the U.S. nuclear industry has experienced up to ten million cyber attacks.[12] Even if only one attempt were to succeed, the magnitude of the impact could significantly undermine, if not shatter, trust and confidence in the system. In addition, cyber capabilities may be used as a force multiplier in a conventional attack.

The good news is that Iran is not as sophisticated as China or Russia insofar as computer network exploitation (CNE), cyber attack and warfare capabilities are concerned (to be

---

[7] Andrew R.C. Marshall and Peter Apps, "Iran 'shadow war' intensifies, crosses borders," *Reuters*, February 16, 2012. Accessed 4/17/12 <http://www.reuters.com/article/2012/02/16/us-iran-israel-security-idUSTRE81F1E720120216>

[8] Corey Flintoff, "New Sanctions Severely Limit Iran's Global Commerce," *NPR,* March 19, 2012. Accessed 4/18/12. <http://www.npr.org/2012/03/19/148917208/without-swift-iran-adrift-in-global-banking-world>

[9] Yaakov Katz, "Iran Embarks on $1b. cyber-warfare program," *The Jerusalem Post*, December 18, 2011. Accessed 4/16/12. <http://www.jpost.com/Defense/Article.aspx?id=249864>

[10] "Fmr. CIA head calls Stuxnet virus 'good idea,'" *60 Minutes,* March 1, 2012. Accessed 4/20/12. <http://www.cbsnews.com/8301-18560_162-57388982/fmr-cia-head-calls-stuxnet-virus-good-idea/>

[11] John O. Brennan, "Time to protect against dangers of cyberattack," *The Washington Post*, April 15, 2012. Accessed 4/23/12. <http://www.washingtonpost.com/opinions/time-to-protect-against-dangers-of-cyberattack/2012/04/15/gIQAdJP8JT_story.html>

[12] Jason Koebler, "U.S. Nukes face up to 10 miilion cyber attacks daily," US News & World Report, March 20, 2012. Accessed 4/24/12. <http://www.usnews.com/news/articles/2012/03/20/us-nukes-face-up-to-10-million-cyber-attacks-daily>

distinguished from intent). As yet, Iran has not shown itself to be a similarly advanced or persistent threat.[13] This is not to give Iran a pass. To the contrary, US officials are investigating "reports that Iranian and Venezuelan diplomats in Mexico were involved in planned cyberattacks against U.S. targets, including nuclear power plants. Press reports based on a Univision (Spanish TV) documentary that contained "secretly recorded footage of Iranian and Venezuelan diplomats being briefed on the planned attacks and promising to pass information to their governments," allege that "the hackers discussed possible targets, including the FBI, the CIA and the Pentagon, and nuclear facilities, both military and civilian. The hackers said they were seeking passwords to protected systems and sought support and funding from the diplomats."[14]

Cyberspace largely levels the playing field, allowing individuals and small groups to have disproportionate impact. This asymmetry can be leveraged by nation-states that seek to do us harm, by co-opting or simply buying/renting the services and skills of criminals/hackers to help design and execute cyber attacks against the United States. For example, do-it-yourself code kits for exploiting known vulnerabilities are easy to find and even the Conficker worm (variants of which still lurk, forming a botnet of approximately 1.7 million computers) was rented out for use.[15] In short, no comfort can be taken from the fact that Iran lacks the sophistication of nations such as China, Russia, or the United States. Proxies for cyber capabilities are available. There exists an arms bazaar of cyber weapons. Adversaries do not need capabilities, just intent and cash.

Iran has a long history of demonstrated readiness to employ proxies for terrorist purposes, drawing on kinetic means. There is little, if any, reason to think that Iran would hesitate to engage proxies to conduct cyber strikes against perceived adversaries. To paraphrase Mark Twain, history may not repeat itself, but it does tend to rhyme. Elements of the IRGC have openly sought to pull hackers into the fold[16]; 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.[17] As in the physical world however, we must keep in mind when crafting security solutions and response mechanisms that Iran is not monolithic: command and control there is murky, even within the IRGC, let alone what is outsourced. The attribution challenge associated with cyberspace is therefore all the more complicated where Iran is concerned. Smoking keyboards are hard to find. Cyberspace is a domain made for plausible deniability.

---

[13] But note Google executive Eric Schmidt's statement: "Iranians are unusually talented [at cyber warfare] for some reason we don't fully understand." "Google admits Iranian superiority in cyber warfare," *Payvand*, December 18, 2011. Accessed 4/17/12. <http://www.payvand.com/news/11/dec/1189.html>

[14] Shaun Waterman, "U.S. authorities probing alleged cyberattack plot by Venezuela, Iran," *The Washington Times*, December 13, 2011. Accessed 4/18/12 <http://www.washingtontimes.com/news/2011/dec/13/us-probing-alleged-cyberattack-plot-iran-venezuela/?page=all>

[15] Conficker Working Group, "Conficker Working Group: Lessons Learned," accessed 4/18/12 <http://www.confickerworkinggroup.org/wiki/uploads/Conficker_Working_Group_Lessons_Learned_17_June_2010_final.pdf>

[16] Golnaz Esfandiari, "Iran Says it Welcomes Hackers Who Work for Islamic Republic," *Radio Free Europe*, March 07, 2011. Accessed 4/18/12. <http://www.rferl.org/content/iran_says_it_welcomes_hackers_who_work_for_islamic_republic/2330495.html>

[17] "The Role of the Basij in Iranian Cyber Operations," *Internet Haganah*, March 24, 2011. Accessed 4/17/12. <http://internet-haganah.com/harchives/007223.html>

In addition to hired or acquired cyber capabilities, the Government of Iran is, according to press reports, investing heavily ($1 billion) to develop and build out its own cyberwar capabilities, both offense and defensive.[18] There is evidence that at the heart of IRGC cyber efforts one will find the Iranian political/criminal hacker group "Ashiyane."[19] In late 2009 and early 2010, hackers calling themselves the Iranian Cyber Army struck Twitter and the Chinese search engine Baidu. [20] The group also appears to have struck Iranian websites managed by the opposition Green Movement, with deleterious results for the opposition's ability to coordinate its activities.[21] The high visibility of these attacks suggests that the Iranian Cyber Army and similar groups might be utilized as proxies by Iran's Islamic Revolutionary Guard Corps. In the event of a conflict in the Persian Gulf, similar attacks on public-facing websites could provide Iran an avenue for psychological operations directed against the U.S. public. Though fluid, hacker groups could be cultivated and guided—if not directly managed—by the IRGC. Iran's ability to conduct Electronic Warfare, including the jamming and spoofing of radar and communications systems, has been enhanced through its acquisition of advanced jamming equipment. In the event of a conflict in the Persian Gulf, Iran might hope to combine electronic and computer network attack methods to degrade U.S. and allied radar systems, complicating both offensive and defensive operations. [22]

There is also an Iranian "cyber police force"[23] that blocks "foreign websites and social networks deemed a threat to national security," with overall policy guidance provided by "The Supreme Council of Virtual Space."[24] Interestingly, a distributed denial of service (DDoS) attack against the BBC this year happened to "coincide with efforts to jam two of the service's satellite feeds in Iran."[25] There has also been considerable speculation about Government of Iran involvement in a number of hacking incidents including against Voice of America, and a Dutch firm in the business of issuing security certificates. Fallout from the latter was significant and affected a range of entities including western intelligence and security services, Yahoo, Facebook, Twitter, and Microsoft.[26]

---

[18] Yaakov Katz, "Iran embarks on $1b. cyber-warfare program," *The Jerusalem Post*, December 18, 2011. Accessed 4/18/12 <http://www.jpost.com/Defense/Article.aspx?id=249864>

[19] Iftach Ian Amit, "Cyber[Crime|War]," paper presented at DEFCON 18 conference , July 31, 2010.

[20] Robert Mackey, "'Iranian Cyber Army' Strikes Chinese Sites," *The Lede* (NYT Blog), January 12, 2010; Scott Peterson, "Twitter hacked: 'Iranian Cyber Army' signs off with poem to Khamenei," *Christian Science Monitor*, December 18, 2009.

[21] Robert F. Worth, "Iran: Opposition Web Site Disrupted," *The New York Times*, December 18, 2009.

[22] Michael Puttre, "Iran bolsters naval, EW power," *Journal of Electronic Defense* vol. 25 no. 4 (April 2002): 24; Robert Karniol, "Ukraine sells Kolchuga to Iran," *Jane's Defense Weekly*, vol. 43 no. 39 (September 27, 2006): 6; Stephen Trimble, "Avtobaza: Iran's weapon in alleged RQ-170 affair?" *The DEW Line*, December 5, 2011. Accessed 4/23/12 <http://www.flightglobal.com/blogs/the-dewline/2011/12/avtobaza-irans-weapon-in-rq-17.html>

[23] Thomas Erdbrink, "Iran cyber police cite U.S. threat," *The Washington Post*, October 29, 2011. Accessed 4/18/12 <http://www.washingtonpost.com/world/middle_east/iran-cyber-police-cite-us-threat/2011/10/27/gIQA1yruSM_story.html>

[24] "Cyber-attack on BBC leads to suspicion of Iran's involvement," *BBC News,* March 14, 2012. Accessed 4/17/12. <http://www.bbc.co.uk/news/technology-17365416>

[25] "Cyber-attack on BBC leads to suspicion of Iran's involvement," *BBC News,* March 14, 2012.

[26] Kevin Kwang, "Spy agencies hit by CA hack; Iran suspected," ZDNet Asia, September 5, 2011. Accessed 4/18/12. <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*,

Not surprisingly, Iran is trying to make its cyber capabilities appear truly muscular. When a U.S. drone fell into Iranian hands in December 2011, Iranian officials were quick to claim that it was brought down by "electronic ambush of the armed forces."[27] The facts surrounding this incident are not all known, but from what U.S. authorities suggest, it seems that the drone likely malfunctioned, and perhaps was also affected by jamming efforts. Regardless, the fact that Iranian officials went public about their supposed capabilities suggests that they plan to do something significant by cyber means, or else they risk losing credibility.

In June 2011, Hezbollah too entered the fray, establishing the Cyber Hezbollah organization. Law enforcement officials note that the organization's goals and objectives include training and mobilizing pro-regime (that is, Government of Iran) activists in cyberspace. In turn and in part, this involves raising awareness of, and schooling others in, the tactics of cyberwarfare. Hezbollah is deftly exploiting social media tools such as Facebook to gain intelligence and information. Even worse, each such exploit generates additional opportunities to gather yet more data, as new potential targets are identified, and tailored methods and means of approaching them are discovered and developed.

Given all the above evidence of (both conventional and cyber) capability and intent on the part of Iran and its proxies, the United States requires a robust posture. There are steps we can take to shore up our stance and create a more solid platform for proactive and, if necessary, reactive purposes. From a counterterrorism and intelligence standpoint, it is crucial to focus on and seek to enhance all-source intelligence efforts. Such is the key to refining our understanding of the threat in its various incarnations, and to facilitating the development and implementation of domestic tripwires designed to thwart our adversaries and keep us "left of boom."[28] Disruption should be our goal. Planning and preparation to achieve this end includes information gathering and sharing — keeping eyes and ears open at home and abroad to pick up indications and warnings (I&W) of attack, and reaching out to and partnering with State and local authorities as well as technical and academic communities. Outreach to respected leaders in the community is essential to keep channels open, build trust, and foster mutual assistance. These dialogues should take place across the board, and not just in major metropolitan centers. The history of the Conficker Working Group, captured in a DHS-sponsored lessons learned document, provides examples of the types of relationships that need to be established and maintained.[29]

February 21, 2011. Accessed 4/19/12. <http://www.washingtontimes.com/news/2011/feb/21/iranian-hackers-break-voa-deface-web-sites/>

[27] Thomas Erdbrink, "Iran shows alleged downed US drone," The Washington Post, December 8, 2011. Accessed 4/18/12. <http://www.washingtonpost.com/blogs/blogpost/post/iran-shows-alleged-downed-us-drone/2011/12/08/gIQAKciXfO_blog.html>

[28] Frank J. Cilluffo, Sharon Cardash, and Michael Downing, "Is America's View of Iran and Hezbollah Dangerously Out of Date?" *FoxNews.com*, March 20, 2012. Accessed 4/18/12 <http://www.foxnews.com/opinion/2012/03/20/is-americas-view-iran-and-hezbollah-dangerously-out-date/>

[29] Conficker Working Group, "Conficker Working Group: Lessons Learned," accessed 4/18/12 <http://www.confickerworkinggroup.org/wiki/uploads/Conficker_Working_Group_Lessons_Learned_17_June_2010_final.pdf>

Searching for I&W will require fresh thinking that identifies and pursues links and patterns not previously established. The above-described nexus between terrorist and criminal networks offers new possibilities to exploit for collection and analysis. To take full advantage, we will have to hit the beat hard, with local police tapping informants and known criminals for leads. State and local authorities can and should complement what the federal government does not have the capacity or resources to collect, and thereby help determine the scope and contours of threat domains in the United States. Further leveraging our decentralized law enforcement infrastructure could also serve to better power our Fusion Centers. The post-9/11 shift of U.S. law enforcement resources away from "drugs and thugs" toward counterterrorism is, ironically, in need of some recalibration in order to serve counterterrorism aims. For the last decade, furthermore, U.S. Government analysts have (understandably) focused on al Qaeda, resulting in a shallower pool of U.S. intelligence on Hezbollah. Recent incidents cited above may provide insight into current tactics, techniques, and procedures, and we should comb through further to mine for and learn possible lessons.

Officials in the homeland security community must undertake contingency planning that incorporates attacks on U.S. infrastructure. At minimum, "red-teaming" and additional threat assessments are needed. The latter should include modalities of attack (such as cyber, and attacks on our critical infrastructures) and potential consequences.

From the perspective of cybersecurity and infrastructure protection, the United States should develop and clearly articulate a cyber-deterrence strategy. Computer network exploitation directed against us is presently a major issue — we are losing billions of dollars in intellectual property as a result. Even more ominous are adversary efforts underway to engage in the cyber equivalent of intelligence preparation of the battlefield, again to be used against us.[30] There is simply no other explanation for the nature and extent of the activity that we have seen so far. Yet, in so far as our response posture is concerned, the current situation is arguably the worst of all worlds: certain adversaries have been singled out in Government documents released in the public domain, yet it is not altogether clear what we are doing about these activities directed against us.[31] The better course would be to undertake and implement a cyber-deterrence policy that seeks to dissuade, deter, and compel both as a general matter, and in a tailored manner that is actor/adversary-specific. A solid general posture could serve as an 80 percent solution, neutralizing the majority of threats before they manifest fully. This would free up resources (human, capital, technological, etc.) to focus in context-specific fashion on the remainder, which constitute the toughest threats and problems, in terms of their level of sophistication and determination. To operationalize these recommendations, we must draw lines in the sand or, in this case, the silicon. Preserving flexibility of U.S. response by maintaining some measure of ambiguity is useful, so long as we make parameters clear by laying down certain markers or selected redlines whose breach

---

[30] Nick Hopkins, "Militarisation of Cyberspace: how the global power struggle moved online," *The Guardian,* April 16, 2012. Accessed 4/17/12. <http://m.guardian.co.uk/technology/2012/apr/16/militarisation-of-cyberspace-power-struggle?cat=technology&type=article>; and <http://m.guardian.co.uk/technology/2012/apr/16/us-china-cyber-war-games?cat=technology&type=article>

[31] See Bryan Krekel et al., *Occupying the Information High Ground: Chinese Capabilities for Computer Network Operations and Cyber Espionage* (Report, U.S.-China Security and Review Commission, 2011); Office of the National Counterintelligence Executive, *Foreign Spies Stealing U.S. Secrets in Cyberspace: Report to Congress on Foreign Economic Collection, 2009-2011* (Washington, D.C.: NCIX, 2011) for the espionage activities of China and Russia in particular.

will not be tolerated. The entire exercise must, of course, be underpinned by all-source intelligence. Lest the task at hand seem overly daunting, remember that we have in past successfully forged strategy and policy in another new domain devoid of borders, namely outer space.

Sometimes, however, the best defense is a good offense. Yet the U.S. cyber offense to defense ratio, at least as represented in the public domain, has skewed overwhelmingly to defense.[32] There are some signs of late that this may be changing, including newspaper reports suggesting that rules of engagement regarding cyber attacks are being developed, and that the Department of Defense is seeking to bolster its arsenal of cyber weapons. [33] These are encouraging developments, if true, because having a full complement of instruments in our toolkit, and publicizing that fact (minus the details), will help deter potential adversaries — provided that we also signal a credible commitment to enforcing compliance with U.S. redlines. Again history provides guidance, suggesting two focal points upon which we should build our efforts. One is leadership — we must find the cyber equivalents of Billy Mitchell or George Patton, leaders who understand the tactical and strategic uses of new technologies and weapons. The other is force protection — not only must we develop offensive capabilities, but we ought to make sure we develop second-strike capabilities. We cannot simply firewall our way out of the problem. U.S. Cyber Command must both lend and receive support, if our cyber doctrine is to evolve smartly and if our cyber power is to be exercised effectively.

While it is up to the Government to lead by example by getting its own house in order, cybersecurity and infrastructure protection do not constitute areas where Government can go it alone. With the majority of U.S. critical infrastructure owned and operated privately, robust public-private partnerships are essential, as is a companion commitment by the private sector to take the steps necessary to reinforce national and homeland security. Government and industry must demonstrate the will and leadership to take the tough decisions and actions necessary in this sphere.

Lest the incentives to do so not be clear to all by now, consider the words of the FBI's then-executive assistant director responsible for cybersecurity, Shawn Henry, who said: "We're not winning." He illustrated his conclusion by citing a company that, due to hackers, lost 10

---

[32] For comments by GEN James Cartwright, USMC, to this effect, see Julian E. Barnes and Siobhan Gorman, "Cyberwar Plan Has New Focus on Deterrence," *The Wall Street Journal*, July 15, 2011. Accessed 4/23/12 <http://online.wsj.com/article/SB10001424052702304521304576446191468181966.html>

[33] Cheryl Pellerin, "DOD Develops Cyberspace Rules of Engagement," American Forces Press Service, March 20, 2012. Accessed 4/23/12 <http://www.defense.gov/news/newsarticle.aspx?id=67625>; Zachary Fryer-Briggs, "U.S. Military Goes on Cyber Offensive," *Defense News*, March 24, 2012. Accessed 4/23/12 <http://www.defensenews.com/article/20120324/DEFREG02/303240001/U-S-Military-Goes-Cyber-Offensive>. See also Testimony of GEN Keith Alexander, USA, before the U.S. House of Representatives Committee on Armed Services, *Fiscal Year 2013 Budget Request for Information Technology and Cyber Operations Programs*, March 20, 2012. Accessed 4/23/12 <http://armedservices.house.gov/index.cfm/hearings-display?ContentRecord_id=92823c77-38f0-4c20-a3ee-36729e8e19a3>

years of effort (R&D) and the equivalent of $1 billion.[34] While we cannot expect the private sector to defend itself alone from attacks by foreign intelligence services, we need to do a better job (as a country) of making the business case for cybersecurity. Failure to shore up our vulnerabilities has national security implications. Yet crucial questions remain open, such as how much cybersecurity is enough, and who is responsible for providing it?

The facts in this case support the need for standards, as identified and self-initiated (along with best practices) by the private sector, across critical industries and infrastructures, together with an enforcement role for Government, to raise the bar higher — in order to protect and promote, not stifle, innovation. The economic and intellectual engines that made this country what it is today are, arguably, our greatest resource. They will power us into the future too, so long as we act wisely and carefully to foster an environment in which they can continue to thrive and grow. To be blunt, legislation of the type described is needed, and it is needed now, in order to remedy crucial gaps and shortfalls, and hold critical infrastructure owners and operators accountable, by focusing on behavior rather than regulating technology.

At the same time, a mix of incentives is needed, to include tax breaks, liability protections, and insurance premium discounts, for private owners and operators of critical infrastructure to take the steps needed to help improve our overall level of security. These measures must also be accompanied by a mechanism to enable and encourage information sharing between the public and private sectors. In addition, as former Director of National Intelligence, Admiral Mike McConnell, has suggested, the information exchanged must be "extensive, ... sensitive and meaningful," and the sharing must take place in "real-time" so as to match the pace of the cyber threat. There must be "tangible benefits" for those yielding up the information.[35]

In conclusion, now is the time to act. For too long, we have been far too long on nouns, and far too short on verbs. Again, I wish to thank both Subcommittees and their staff for the opportunity to testify today, and I would be pleased to try to answer any questions that you may have.

---

[34] Devlin Barrett, "U.S. Outgunned in Hacker War," *The Wall Street Journal*, March 28, 2012. Accessed 4/18/12 <http://online.wsj.com/article/SB10001424052702304177104577307773326180032.html>

[35] VADM J. Michael McConnell, USN (Ret.), remarks given February 22, 2012 at Homeland Security Policy Institute, The George Washington University, Washington, D.C. Transcript and video accessed 4/23/12 <http://www.c-spanvideo.org/program/CyberSecurityL>.