THE GEORGE WASHINGTON UNIVERSITY
HOMELAND SECURITY POLICY INSTITUTE

"The Future of Homeland Security: Evolving and Emerging Threats"

U.S. Senate Committee on Homeland Security & Governmental Affairs

July 11, 2012

Statement of Frank J. Cilluffo

Director, Homeland Security Policy Institute

The George Washington University

Chairman Lieberman, Ranking Member Collins, and distinguished Members of the Committee, thank you for the opportunity to testify before you today. This first in a series of hearings looking both back at what has been accomplished and ahead to what remains to be done in the area of homeland security is a prudent and thoughtful approach. While a host of constructive and valuable changes to policy and practice have been formulated and implemented in the decade plus since 9/11, there remain important gaps and shortfalls in our homeland and national security posture and readiness. Though we do not often laud those individuals, such as yourselves, who have remained steadfast and dedicated to the cause of improving the safety and security of Americans day in, day out, for years—even when the public mind and public opinion may have made the task more challenging than it already was—it bears remembering that we have made significant strides and in a relatively short period of time. Having said that, some significant shortcomings still exist, and some of these are more urgent than others to remedy or at least redress in part.

My remarks today will focus on two major areas: counterterrorism and cybersecurity. My approach, which I hope will be helpful, is to identify weaknesses and vulnerabilities in U.S. strategy and operations on both counts—with an eye to offering recommendations on how best to move forward, particularly in an economic climate in which resources are limited. Indeed, to the extent that we can derive greater bang for our buck, it is our shared responsibility to do so. What I would urge against however, is a more broadbrush approach (from a financial perspective) which runs the risk of privileging convenience over thoughtful strategic action, and may thereby do damage to our national/homeland security posture, even if inadvertently. Blunt cuts are simply not the answer. Instead we should prune and trim carefully, by prioritizing according to risk, by allowing good programs to live, and by taking off life support those programs that should rightfully expire.

Counterterrorism

As many counterterrorism officials have observed recently, al Qaeda's Senior Leadership is back on their heels. Key leaders have met their demise including, of course, Usama Bin Laden and Anwar al-Awlaki. Nevertheless, the ideology that Bin Laden and others such as the culturally fluent American-born extremist and self-styled cleric al-Awlaki have propounded lives on. This ideology is the lifeblood that continues to sustain the vitality and growth of the global jihadist movement. Make no mistake: while the core of al Qaeda may be seriously and significantly diminished, thanks largely to targeted U.S. military action overseas, the threat now comes in various sizes, shapes and forms. There are still many and varied al Qaeda affiliates that continue to thrive, most notably in Yemen and the Sahel, and in Somalia. Indeed, there is an arc of Islamist extremism that stretches across Africa from east to west, through the Sahel and the Maghreb, incorporating Boko Haram in Nigeria and Ansar Dine in Mali. At the same time, a veritable witch's brew of jihadists exists in Pakistan, including for example, the Haqqani network, Lashkar-e-Taiba (LeT), Tehrik-i-Taliban Pakistan (often dubbed the "Pakistani Taliban"), Harkat-ul-Jihad al-Islami (HuJI), Jaish-e-Mohammed, and the Islamic Movement of Uzbekistan. We have seen in the past and continue to see substantial evidence of cooperation and collaboration between these latter groups and al Qaeda. Though some of these groups may be more regionally or locally focused, they increasingly ascribee and subscribe to al Qaeda's goals and the broader global jihad, with U.S. and western targets increasingly in their crosshairs..[1] Nor can we take our eye off the ball of state-sponsored terrorism, such as that perpetrated by the Government of Iran and proxies such as Hezbollah.

[1] Frank Cilluffo "Open Relationship: The United States is doing something right in the war on terror" *Foreign Policy* (February 15, 2012). http://www.foreignpolicy.com/articles/2012/02/15/open_relationship. See also Sudarsan Raghavan "In Niger refugee camp, anger deepens against Mali's al-Qaeda-linked Islamists" *Washington Post* (July 7, 2012). http://www.washingtonpost.com/world/africa/in-niger-refugee-camp-anger-deepens-against-malis-al-qaeda-linked-islamists/2012/07/07/gJQAS25SUW_story.html

Unfortunately, our efforts to counter and defeat the jihadist ideology have been lacking, with the result that the terrorist narrative lives on and continues to attract and inspire those who wish us harm—despite and in some cases even empowered by—--the so-called Arab Spring. This is the biggest element missing from our statecraft on counterterrorism. This sustaining pool of recruits is, as Defense Secretary Panetta recently observed, the fundamental challenge: "the real issue that will determine the end of al-Qaida is when they find it difficult to recruit any new people...".[2] Arguably the most difficult challenge is the so-called "lone wolf" who self-radicalizes and prepares to commit violence without directly reaching out to al Qaeda or others for support and guidance. The term lone wolf is a bit of a misnomer, however, since individuals in this category have at least been inspired, goaded and in some cases facilitated by external forces—which in turn blurs the line between the foreign and domestic. In such cases, the mission of prevention is all the harder because there may be little for law enforcement or counterterrorism professionals to pick up on ahead of time, when we are still left of boom. The mission remains critical, though, as evidenced by the discovery of 58 "homegrown" jihadi terrorism plots since September 11, 2001. [3] Keeping eyes and ears open, at home and abroad and in partnership with our allies, is perhaps the best safeguard (and I will offer key recommendations on the intelligence front, below).

Notwithstanding the importance that non-state and individual actors have taken on, in an era when their actions can have profound impact and consequences, it bears reinforcing that traditional State and State-sponsored threats have not gone away. To the contrary, the latter are in some instances resurgent and reinvigorated. Consider for example Iran. The Director of National Intelligence recently stated that Iran is "now more willing to conduct an attack in the United States"[4] — a concern that has also been voiced by LAPD's Deputy Chief, Michael Downing, and by NYPD's former Director of Intelligence Analysis, Mitchell Silber.[5] To wit: the recently thwarted Iranian plot to assassinate Saudi Arabia's ambassador to the United States. Note also that up until 9/11, it was in fact Iran's chief proxy, Hezbollah, which 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.

In addition, law enforcement officials have observed a striking convergence of crime and terror.[6] Hezbollah's nexus with criminal activity is greater than that of any other terrorist group. 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. 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] "Al Qaeda Senior Leadership Nearly Eradicated: Panetta" *Global Security Newswire* (June 22, 2012). http://www.nti.org/gsn/article/al-qaida-senior-leadership-nearly-eradicated-panetta-says/?utm_source=BNT+June+25%2C+2012--AoH&utm_campaign=BNT+06252012&utm_medium=email

[3] Jerome P. Bjelopera "American Jihadist Terrorism: Combating a Complex Threat" *CRS Report for Congress* (November 15, 2011). http://www.fas.org/sgp/crs/terror/R41416.pdf (but note that numbers have increased since the Report was published)

[4] Testimony of James R. Clapper before the Senate Select Committee on Intelligence, "Worldwide Threat Assessment of the U.S. Intelligence Community" (January 31, 2012). http://www.dni.gov/testimonies/20120131_testimony_ata.pdf

[5] "Tensions with Iran raise US safety concerns, but intelligence official says attack unlikely" *Associated Press* (February 17, 2012). http://www.foxnews.com/politics/2012/02/17/tensions-with-iran-raise-us-concern-possible-terror-attack/

[6] See for example "The Hybrid Threat: Crime, Terrorism and Insurgency in Mexico" *Joint Study of HSPI and the U.S. Army War College Center for Strategic Leadership* (December 2011). http://www.gwumc.edu/hspi/events/resources/Hybrid%20Threat%20Monograph%20(Internet%20version).pdf

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. It is also important to note that Iran itself is not a monolith when it comes to its terrorist (or cyber) activities. Indeed, Iran's Islamic Revolutionary Guard Corps (IRGC) operates as a semi-independent entity—and it is unclear just how much they coordinate with Iranian intelligence (the Ministry of Intelligence and Security, or MOIS). Notably, the IRGC has a substantial economic enterprise internal and external to Iran, including telecommunications. Given its close connections with Hezbollah and active training of terrorists, that makes Iran a key threat—and despite the imposition of sanctions on Iran, it is quite clear that the IRGC is not running out of money.[7] Taken as a whole, the various developments above suggest that our longstanding frames of reference and the "redlines" they incorporated have shifted. Correspondingly, we must re-examine our long-held assumptions, challenging them in light of current evidence, and recalibrate our stance and response mechanisms as needed.[8]

These developments draw warranted attention to the risk posed by hybrid threats—threats in which an adversary acquires from a third-party the necessary access, resources, or know-how, needed to attack or threaten a target—and how such might be employed strategically against the United States.

As is the case with the Federally Administered Tribal Areas (FATA) in Pakistan and Afghanistan, ungoverned and under-governed spaces, such as Yemen and the Sahel as well as Somalia, pose a different but still potent challenge. There, failed, failing or weak states, offer a propitious climate for jihadists to recruit, regroup, train, plan, plot, and execute attacks. In recent weeks, General Carter Ham, head of U.S. Africa Command (AFRICOM), warned that al Qaeda in the Islamic Maghreb (AQIM—operating in southern Algeria, northern Mali, and eastern Mauritania, and spreading elsewhere in the Sahel), al-Shabaab in Somalia, and Boko Haram in Nigeria "are seeking to coordinate and synchronize their efforts." He characterized each of these groups as "by itself, a dangerous and worrisome threat," but was particularly concerned by the emerging trend of them sharing "funds, training and explosive material."[9] Granted, some of these groups' top goals may be inward-focused, targeting the specific states in which these groups are primarily rooted. Their activities, however, breathe life into the larger jihadist movement and give it continued currency at a time when the Senior Leadership core has been seriously weakened.

So what can and should we do about all of these concerning realities? For starters, at the level of principle, we need to be as flexible and adaptive as our adversaries, who are nothing if not creative and ever-thinking. A static posture is an ineffective one. After all, each time we raise the security bar (often at great cost to the U.S. Treasury) our adversaries devote themselves determinedly to crafting a reasonably inexpensive and clever way around the latest security measure(s). Their ingenuity and inventions are often vivid, and include body and "booty" bombs. Now is not the time to ease off the gas pedal. Rather we should and must keep up the pressure and exploit this unique window of counterterrorism opportunity by maintaining, if not accelerating, the operational tempo. The threat would look and be markedly different otherwise.

---

[7] Julian Borger and Robert Tait "The financial power of the Revolutionary Guards" *The Guardian* (February 15, 2010). http://www.guardian.co.uk/world/2010/feb/15/financial-power-revolutionary-guard

[8] Testimony of Frank J. Cilluffo before the U.S. House of Representatives Committee on Homeland Security, Subcommittee on Counterterrorism and Intelligence; and Subcommittee on Cybersecurity, Infrastructure Protection and Security Technologies, "The Iranian Cyber Threat to the United States" (April 26, 2012). http://www.gwumc.edu/hspi/policy/testimony4.26.12_cilluffo.pdf

[9] David Lerman "African Terrorist Groups Starting to Cooperate, U.S. Says" *Bloomberg* (June 25, 2012). http://www.bloomberg.com/news/2012-06-25/african-terrorist-groups-starting-to-cooperate-u-s-says.html

Overall, Yemen-based al Qaeda in the Arabian Peninsula (AQAP) remains the most adaptive and lethal terrorist threat to the United States. Despite the past year's drone and Special Operations Forces' (SOF) achievements, al-Asiri, AQAP's innovative bomb-maker remains alive and continues to craft increasingly sophisticated attacks against Western airliners. Yet drones and SOF remain critical counterterrorism tools for denying AQAP safe haven in Yemen. Although an imperfect tool, drone strikes suppress terrorists, deny them safe havens, and limit jihadists' ability to organize, plan, and carry out attacks. These strikes help shield us from harm and serve our national interests. Along with SOF, the targeted use of drones should constitute key components of U.S. counterterrorism efforts for many years to come.

Having said that (and as former CIA officer and former State Department Coordinator for Counterterrorism, Ambassador Hank Crumpton, pointed out when featured in a recent HSPI roundtable), drones are important but cannot be a substitute for human intelligence (HUMINT). Indeed, intelligence remains our greatest need in Yemen. Improved intelligence will have an added benefit, too, by helping continue to improve the accuracy of drone strikes while minimizing collateral damage to civilians.[10]

From a counterterrorism standpoint, it is crucial to focus on and seek to enhance all-source intelligence efforts. This 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."[11] 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, especially law enforcement.

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 (or is simply not best suited to do), 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.

To obtain a truly "rich picture" of the threat in this country, we must focus on the field—not the Beltway. As history shows, the intelligence community has come to just such a field bias. For the counterterrorism community to do otherwise is to risk stifling and stymieing the good work being done where the rubber meets the road. Fusion Centers, for instance, should be given ample opportunity to flourish. The equivalent of Commanders' Intent, which gives those in the field the leeway to do what they need to do and which incorporates an honest to goodness "hotwash" after the fact to determine what went wrong and how to fix that, is needed in present civilian context for counterterrorism and intelligence purposes. Simple yet powerful steps remain to be taken. This was revealed starkly in multiple rounds of survey work (first with the major metropolitan intelligence

[10] Clinton Watts and Frank J. Cilluffo "Drones in Yemen: Is the U.S. on Target?" *HSPI Issue Brief* (June 21, 2012). http://www.gwumc.edu/hspi/policy/drones.pdf

[11] 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). http://www.foxnews.com/opinion/2012/03/20/is-americas-view-iran-and-hezbollah-dangerously-out-date/

chiefs and later with the fusion centers) that HSPI recently completed in an attempt to bring a little science to the art of intelligence. For example, too few Fusion Centers currently do threat assessments. This is unacceptable, especially in a climate of limited resources in which allocation decisions (regarding human, capital, and financial resources) should be priority-ordered, meaning that scarce resources should be directed to those counter-threat measures, gaps and shortfalls that constitute areas of greatest need. And Fusion Center-specific threat assessments are just a start. Regional threat assessments are also needed. Our adversaries do not respect local, State, or even national boundaries hence our response posture must be similarly nimble and cohesive. Yet, according to HSPI survey research published last month, only 29% of Fusion Center respondents reported that their Center conducted a regional threat assessment on at least a yearly basis. Almost half reported that their Centers simply did not conduct regional threat assessments.

Those working in the Fusion Centers have yet to be invested with the analytical skill-craft and training necessary for them to accomplish their mission. Current incentive structures place too much emphasis on information processing and not enough on analytical outcome. Greater resources should be allocated to the professional development of those working in the Centers. Within them lies untapped collection and analysis potential. Realizing and unleashing that potential will further bolster State and local law enforcement efforts, and help develop anticipatory intelligence to prevent terrorist attacks and the proliferation of criminal enterprise operations.[12]

Intelligence to support operations is certainly crucial but we must not lose sight of the long game either. To that end and from a strategic perspective, it would most helpful for the Secretary of Homeland Security to establish an Office of Net Assessment (ONA) within the Department of Homeland Security (DHS) to provide the Secretary with comprehensive analysis of future threats and U.S. capabilities to meet those threats. The ONA would fill the much-needed role of producing long-term assessments and strategy, acting as a brain trust of creativity and imagination, while remaining unfettered by the "crisis du jour" or the day-to-day demands flowing from intelligence needs and operations. The ever-shifting and unpredictable security environment facing the U.S. requires the constant questioning of assumptions, the asking of what-ifs, and the thinking of the unthinkable—in order to identify game changers. The ONA should take a comprehensive, multi-disciplinary approach to its analysis, looking at the full range of factors which will alter and shape the security environment of the future, including social, political, technological, economic, demographic, and other trends.

In order to accomplish this tall order, the duties of ONA would include studying existing threats in order to project their evolution into the future; studying trends in the weapons, technologies, modalities, and targets utilized by our adversaries (i.e., the events that can transform the security landscape); reviewing existing U.S. capabilities in order to identify gaps between current capabilities and the requirements of tomorrow's threats; conducting war games and red team scenarios to introduce innovative thinking on possible future threats; assessing how terrorist groups/cells could operate around, and/or marginalize the effectiveness of, policies and protective measures.

Notably, this proposal is not new. To the contrary, it was in fact contained in the January 2007 Homeland Security Advisory Council Report of the Future of Terrorism Task Force, for which I served

[12] Frank J. Cilluffo, Joseph R. Clark, Michael P. Downing, and Keith D. Squires "Counterterrorism Intelligence: Fusion Center Perspectives" *HSPI Counterterrorism Intelligence Survey Research (CTISR)* (June 2012). http://www.gwumc.edu/hspi/policy/HSPI%20Counterterrorism%20Intelligence%20-%20Fusion%20Center%20Perspectives%206-26-12.pdf. See also Frank J. Cilluffo, Joseph R. Clark, and Michael P. Downing "Counterterrorism Intelligence: Law Enforcement Perspectives" *CTISR* (September 2011). http://www.gwumc.edu/hspi/policy/HSPI%20Research%20Brief%20-%20Counterterrorism%20Intelligence.pdf

as Vice Chairman together with Chairman Lee Hamilton.[13] Now is the time—indeed it is well past time—to take this recommendation off the page and enact it. Our adversaries are patient and they are long-term thinkers whose horizons extend well beyond weeks and months. To help counter them effectively, the ONA should be an independent office that reports directly to the Secretary of Homeland Security.[14]

Before turning from counterterrorism to cybersecurity, I would add some closing thoughts on combating violent Islamist extremism (CVIE). The fact is that addressing specific outbreaks of violent Islamist extremism will not prevent its virulent spread unless the underlying extremist ideology is exposed, unpacked, dissected, and combated. Government agencies currently involved in various aspects of the CVIE mission do not note systemic failures so much as the complete lack of a system at all. Absent clear interagency directives instructing how to distribute resources and coordinate aspects of the mission, individual and broader agency efforts are improvised. As a result, an inconsistent and haphazard approach to dealing with the force underlying today's terrorist threat is all but guaranteed.[15]

Counter-radicalization is an essential complement to counterterrorism. Elements of a cohesive national strategy could incorporate a range of approaches that have proven effective in other contexts. The power of negative imagery, as in a political campaign, could be harnessed to hurt our adversaries and further chip away at their appeal and credibility in the eyes of their peers, followers, and sympathizers. A sustained and systemic strategic communications effort aimed at exposing the hypocrisy of Islamists' words versus their deeds could knock them off balance, as could embarrassing their leadership by bringing to light their seamy connections to criminal enterprises and drug trafficking organizations. Brokering infighting within and between al Qaeda, its affiliates, and the broader jihadi orbit in which they reside, will damage violent Islamists' capability to propagate their message and organize operations both at home and abroad. Locally administered programs are especially significant, as many of the solutions reside outside the U.S. government and will require communities policing themselves.[16] In the last year or two, the United States has made some headway on these fronts, including through the efforts of the Department of State's Office of Strategic Communications—but we could do more and we could (and should) hit harder, especially when our adversaries are back on their heels. Indeed, now is the time to double down rather than ease up on the pressure. In short, we must encourage defectors, delegitimize and disaggregate our adversaries' narrative, and above all, remember the victims.

Cybersecurity

To my mind, the cybersecurity community's state of development is akin to that of the counterterrorism community as it stood shortly after 9/11. Although much work remains to be done on the counterterrorism side, as I emphasized above the country has also achieved significant progress in this area. On the cybersecurity side however, the threat (and supporting technology) have markedly outpaced our prevention and response efforts. Despite multiple incidents that could

[13] http://www.dhs.gov/xlibrary/assets/hsac-future-terrorism-010107.pdf
[14] James Carafano, Frank Cilluffo, Richard Weitz et al. "Stopping Surprise Attacks: Thinking Smarter About Homeland Security" *Backgrounder* (April 23, 2007). http://www.heritage.org/research/reports/2007/04/stopping-surprise-attacks-thinking-smarter-about-homeland-security
[15] Frank J. Cilluffo, J. Scott Carpenter, and Matthew Levitt "What's the Big Idea? Confronting the Ideology of Islamist Extremism" *Joint Report of HSPI and the Washington Institute for Near East Policy* (February 4, 2011). http://www.gwumc.edu/hspi/policy/issuebrief_confrontingideology.pdf. See also: Letter from Senators Lieberman and Collins to the Honorable John Brennan, Assistant to the President for Homeland Security and Counterterrorism and Deputy National Security Advisor (April 2, 2011).
[16] Cilluffo, Carpenter, and Levitt "What's the Big Idea? Confronting the Ideology of Islamist Extremism."

have served as galvanizing events to shore up U.S. resolve to formulate and implement the changes that are needed, and not just within Government, we have yet to take those necessary steps.

The cyber threat is multifaceted and may emanate from individual hackers, hacktivists, criminal or terrorist groups, nation-states or those that they sponsor. The threat spectrum is multifaceted, and affects the public and private sectors, the interface and intersections between them, as well as individual citizens. National security, economic security, and intellectual property are just some of the major interests at stake. Prevention and response requires cooperation and collaboration, in real-time, against sophisticated adversaries. By and large, from a homeland security perspective, at least in terms of sophistication, foreign states are our principal concerns—specifically those that pose an advanced and persistent threat, namely Russia and China. Their tactics may also be exploited by others. Beyond the cited states, other countries such as Iran and North Korea, are not yet on a par with Russia and China insofar as capabilities are concerned—but what Iran and North Korea lack in indigenous capability they make up for in terms of intent.[17] Where there is motivation, persistence tends to follow. The challenge is not only asymmetric in character, but complicated by the nuclear backdrop, as Iran drives towards acquiring nuclear weapons. It would not be wise to ignore these potential threat vectors. Iran is increasingly investing in bolstering its own cyberwar capabilities. Bear in mind also that many of the capabilities that do not exist indigenously may be purchased—making it possible to craft a hybrid threat. There is a veritable arms bazaar of cyber weapons. Our adversaries just need the cash.

Making a complex situation even more complicated, evolution in the cyber domain has taken place so rapidly that the concepts and categories that would ordinarily underlie policy have yet to be fully debated and defined. There is a void in terms of doctrine because fundamental operating principles have yet to be elaborated and developed. Some discussions are underway, such as within the Department of Defense (DoD), where the rules of engagement to apply in this newest domain are currently top of mind. The nature of the challenge, however, requires a national conversation and we as a country have yet to have that talk. Only recently, in the wake of "Stuxnet" and "Flame" and other operations targeting our adversaries and networks of interest, have we begun to see editorial boards as well as current and former senior military and civilian leaders place the issues squarely on the table with an eye to airing them openly and encouraging a whole-of-society consideration of both problem and solution. For instance, 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.[18] Developing doctrine, especially in terms of cyber offense, requires this type of engagement so as to ensure that policy is carefully crafted and widely supported.

As we carve out the contours of what is an act of war in cyberspace and formulate answers and options to other crucial questions, foreign intelligence services are engaging in cyber espionage against us, often combining technical and human intelligence in their exploits.[19] Everything from critical infrastructure to intellectual property is potentially at risk. These exploits permit others to leapfrog many bounds beyond their rightful place in the innovation cycle, by profiting from (theft of) the research and development in which private and public U.S. entities invested heavily. At worst, these exploits hold the potential to bring this country and its means of national defense and national

[17] Cilluffo Testimony, "The Iranian Cyber Threat to the United States" (April 26, 2012). http://www.gwumc.edu/hspi/policy/testimony4.26.12_cilluffo.pdf

[18] CBS News, "Fmr. CIA head calls Stuxnet virus `good idea'" *60 Minutes* (March 1, 2012). http://www.cbsnews.com/8301-18560_162-57388982/fmr-cia-head-calls-stuxnet-virus-good-idea/

[19] Frank J. Cilluffo and Sharon L. Cardash "Commentary: Defense Strategy Avoids Tackling the Most Critical Issues" *Nextgov* (July 28, 2011). http://www.nextgov.com/cybersecurity/2011/07/commentary-defense-cyber-strategy-avoids-tackling-the-most-critical-issues/49494/

security to a halt, and thereby undermine the trust and confidence of the American people in their Government. Indeed, one wonders what purpose the mapping of critical U.S. infrastructure by our adversaries might serve other than what is known in military terms as intelligence preparation of the battlefield. To my mind, the line between this type of reconnaissance and an act of aggression is very thin, turning only on the matter of intent.

Unfortunately, there is no lack of evidence of intent. By way of example, U.S. 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."[20]

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.

Officials in the homeland security community must therefore 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 and potential consequences. The United States should also develop and clearly articulate a cyber-deterrence strategy. 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.[21] 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 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.

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

[21] See Bryan Krekel et al. "Occupying the Information High Ground: Chinese Capabilities for Computer Network Operations and Cyber Espionage," *Report of the 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* (2011) for the espionage activities of China and Russia in particular.

An "active defense" capability—meaning the ability to immediately attribute and counter attacks—is needed to address future threats in real-time. Active defense is a complex undertaking however, as it requires meeting the adversary closer to their territory, which in turn demands the merger of our foreign intelligence capabilities with U.S. defensive and offensive cyber capabilities (and potentially may require updating relevant authorities). Sometimes, however, the best defense is a good offense. Having a full complement of instruments in our toolkit and publicizing that fact, minus the details (which is not to confused with harmful leaks regarding specific operations), 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. 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 that prevail support the need for standards. Ideally these should be 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 (not to mention the inventors of the Internet) 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 along these lines 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. The call has come from a range of powerful, thoughtful and well informed voices including former Secretary of Homeland Security Michael Chertoff in a joint letter with former Director of National Intelligence, Admiral Mike McConnell, and others[22]; and even from industry such as Northrop Grumman Corporation's Chairman, CEO and President, Wes Bush.[23] At the same time though, 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 Admiral McConnell has suggested: the information exchanged must be "extensive,...sensitive and meaningful," and the sharing must take place in "real-time" so as to

[22] Chris Strohm, "Chertoff Urges Swift Action by Senate on Cybersecurity Measures" *Bloomberg Businessweek* (January 25, 2012). http://www.businessweek.com/news/2012-01-25/chertoff-urges-swift-action-by-senate-on-cybersecurity-measures.html
[23] "Effective Cybersecurity: Perspectives on a National Solution" *The 13th Annual Robert P. Maxon Lecture* (April 9, 2012). http://www.gwumc.edu/hspi/events/gwsbBush.cfm

match the pace of the cyber threat. There must be "tangible benefits" for those yielding up the information.[24]

Now is the time to act. For too long, we have been far too long on nouns, and far too short on verbs. The imperative is further underscored if we are to have, as I have recommended, a robust offensive capability. In short, if we are going to do unto others, then we should first be fully inoculated and prepared to defend against others doing the same unto us. This principle is all the more applicable in the cyber context, where blowback against the party initiating first-use of a cyber-weapon is more likely than not, once that weapon is released into the wild and the so-called law of unintended consequences kicks into effect. But readiness is no simple matter in this context, certainly not across the board. Put another way, one of the cyber-related challenges facing this country is that the departments with the greatest capabilities (such as NSA) do not have all the authorities, whereas the departments whose capacities are more nascent (such as DHS) are endowed with relatively greater authority. This misalignment of authorities and capabilities presents and poses challenges in a range of contexts including computer network exploit and attack (CNE and CNA) as well as computer network defense (CND) and cybersecurity more generally. Figuring out how best to bridge the gap between authorities and capabilities is a vexing challenge, but one that would serve us well to think through carefully and in clear-eyed fashion in order to achieve the best possible outcome for the Nation.

Before closing, I would stress that as much as technology matters in this area, HUMINT remains crucial as well. As a general matter, there is simply no substitute for a human source, whether a recruit in place inside a foreign intelligence service, a criminal enterprise, or a terrorist organization. The "rich picture" of the threat, mentioned above in the counterterrorism context, cannot and will not be generated without input and insights from the private sector including the owners and operators of critical infrastructure. To help keep blind spots at a minimum, these owners and operators should be part of our Fusion Centers—yet for more than half of the nation's Centers this is not the case. This notwithstanding the fact that a sizeable majority of the country's Centers are believed by their membership to have "relatively weak capabilities in regard to the gathering, receiving, and analyzing of cyber threats."[25]

Clearly we are just beginning work on the long list of to-do's that pertains to the cyber domain. Having said that, it is important to remember that even in this area, we have already learned much and that knowledge will help us chart a constructive path forward. By way of illustration, 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.[26] Yet there is still a long way to go. At the end of the day, the ability to reconstitute, recover, and get back on our feet is perhaps the best deterrent. The storms that recently battered the National Capitol Region, leaving close to a million people without power during a week-long heat wave, are instructive in terms of our shortcomings on resilience. Mother Nature may be a formidable adversary, but just imagine the level of damage and destruction that a determined and creative enemy could have wrought. There is no lack of trying, as a recently published DHS report makes clear, noting the spike in attacks (from 9 incidents to 198) against US critical infrastructure from 2009 to 2011.[27] The good news, on the other hand, is that the most serious of these incidents could have been avoided

[24] Remarks delivered at HSPI roundtable (February 22, 2012). http://www.c-spanvideo.org/program/CyberSecurityL
[25] CTISR June 2012. http://www.gwumc.edu/hspi/policy/HSPI%20Counterterrorism%20Intelligence%20-%20Fusion%20Center%20Perspectives%206-26-12.pdf
[26] "Conficker Working Group: Lessons Learned" June 2010 (Published January 2011). http://www.confickerworkinggroup.org/wiki/uploads/Conficker_Working_Group_Lessons_Learned_17_June_2010_final.pdf
[27] Suzanne Kelly "Homeland security cites sharp rise in cyber attacks" *CNN.com* (July 4, 2012). http://security.blogs.cnn.com/2012/07/04/homeland-security-cites-sharp-rise-in-cyber-attacks/

through the adoption of basic security steps and best practices. The bad news, of course, is that these fundamental measures were not yet put into place. Plainly we have not yet made the requisite business case for doing so. The urgency for doing so needs no further explanation, but we must take care to strike just the right balance of carrots and sticks and of course measures that ensure both privacy and security.

* * *

More than a decade after 9/11, and in an environment in which resource scarcity prevails, there is opportunity as well challenge—namely an opportunity to reflect and recalibrate, and move forward smartly. While there are many subjects that I have not touched on (such as chemical, biological, radiological, and nuclear weapons, from both a proliferation and terrorism perspective) my aim was to confine comment to two broad subject areas at a strategic level, thereby leaving detailed analysis and option-framing on certain important and complex areas, such as those referenced parenthetically, to other experts. Again, I wish to thank both the Committee and its staff for the opportunity to testify today, and I would be pleased to try to answer any questions that you may have.