

**“The Department of Homeland Security:
An Assessment of the Department and a Roadmap for its
Future”**

**The U.S. House of Representatives
Committee on Homeland Security**

September 20, 2012

Statement of Frank J. Cilluffo

**Director, Homeland Security Policy Institute,
Co-Director, Cyber Center for National and Economic Security
The George Washington University**

Chairman King, Ranking Member Thompson, and distinguished Members of the Committee, thank you for the opportunity to testify before you today. Throughout your tenure as Chairman of this Committee, Congressman King, you have consistently taken on the hard issues facing our country, and have committed to addressing them. Thank you for your leadership. Turning to the timing and subject of today's hearing both are well-selected. As recent events from the Middle East and North Africa through to Southeast Asia regrettably illustrate, violent extremism continues to thrive. With the United States and its interests still in the cross-hairs of jihadi and Islamist militants across the globe, the present moment is sadly opportune to assess the activities of the Department of Homeland Security (DHS) and give careful consideration to a roadmap for its future. Despite significant progress, especially on the counterterrorism front, the existing and projected threat climate is such that continued vigilance and a robust as well as proactive posture is needed—not only at DHS but throughout government, at all levels, and supported by approaches that effectively integrate the private sector and the efforts of individual citizens too.

THE THREAT ECOSYSTEM OF TODAY AND TOMORROW: CHALLENGES FOR DHS AND BEYOND

Al Qaeda (AQ) has been a shrewd practitioner of the art of stoking, piggybacking upon, and exploiting local grievances in order to further AQ's own goals and objectives and the broader global jihad. In a military context, this is referred to as tactical, operational and strategic "swarming"; and it has clearly been adopted by others as well, as recent incidents around the globe have unfortunately demonstrated. Usama bin Laden may be dead, but the toxic ideology that he left behind lives on, and the narrative that it informs continues to resonate powerfully in certain quarters. Today perhaps the most significant locus of his legacy and methods is in Africa; though Pakistan's Federally Administered Tribal Areas, better known as FATA, remain a combustible region, one where it would be imprudent to ease up on U.S. pressure against militants.¹

In Africa, al Qaeda in the Arabian Peninsula (AQAP), al Qaeda in the Islamic Maghreb (AQIM), Al Shabab (Somalia), Ansar al-Din (Mali), Boko Haram (Nigeria), and their ilk persist in sowing discord and violence in a cross-continental swath ranging from east to west, leaving not even Timbuktu untouched. Indeed, even Yemen, the subject of significant counterterror efforts on the part of the United States (and others), remains home to AQAP and to one of the world's most dangerous bomb-makers, Ibrahim al-Asiri. Notwithstanding U.S. and allied counterterrorism efforts that have yielded a good measure of success, these terror affiliates remain committed to carrying forward the mantle of bin Laden, and to exploiting both ungoverned and under-governed spaces. The latter tactic pre-dated the Arab Spring, but evidenced reinforcement and magnification thereafter. The tragic violence of recent days, beginning in Benghazi and directed against U.S. personnel and interests (and those of allies), may come to further prove this point, though key facts remain under investigation.

¹ U.S. military actions, including the use of drones, have had significant operational effects on al Qaeda (and associated entities) by disrupting foreign fighter pipelines to the region, activities of key facilitators, and training camps. Think of it as suppressive fire. The more time al Qaeda and associated entities spend looking over their shoulders, the less time they have to train, plot and execute terrorist attacks. And with al Qaeda senior leaders on their back heels, now is the time to exploit this unique window of counterterrorism opportunity by maintaining the operational tempo to consolidate these gains.

As observed in a report on Mauritania published earlier this year by the Carnegie Endowment for International Peace, Africa is a hot spot because of the confluence of multiple factors, including poverty, corruption and weak governance. The ensuing void left in countries like Mauritania, where state infrastructure like the education system is weak, offers an opening to “mahadras” (religious schools) propagating violent ideologies, which in turn spur the growth of militancy. The outlook for the Continent is not entirely bleak however; as the study points out, “there is a high level of distrust between black Africans and AQIM, a movement led and dominated by Arabs”—which portends a recruitment challenge for al Qaeda forces in the area, at least in the longer term.² The outcome is not predetermined, though, as AQ was able to surmount and ingrain itself into the tribal populations indigenous to the FATA by pursuing a concerted strategy of marrying into these clans. Whether a similar or other course might further pave the way for inroads into African countries remains to be seen and merits continued U.S. vigilance, as well as that of our allies.

The various terrorist organizations cited above are exhibiting, moreover, an increasing willingness to reach out and partner with one another, as well as with others, who may be able to help build their indigenous capacities and further their particular goals. The twin phenomena of violent extremism and cross-group cooperation of such forces is assuredly not limited to Africa, and extends to the veritable witch’s brew of forces that ranges from Iraq, Pakistan, and the Caucasus, to Mali, Nigeria, and Somalia—where militants linked to al Qaeda tried to kill the country’s new President just last week in a double suicide/homicide blast. Pakistan is especially complex, and dangerous. Groups that were once regionally focused now subscribe ever-more to al Qaeda’s goals and the broader global jihad. This toxic blend includes the Haqqani network³, Laskhar-e-Taiba (LeT), Tehrik-i-Taliban Pakistan, Harkat-ul-Jihad al-Islami (HuJI), Jaish-e-Mohammed, and the Islamic Movement of Uzbekistan; all of which cooperate with al Qaeda on a tactical and sometimes strategic basis, linked by an affinity for militant Islamist ideology—with U.S., Indian, Israeli and Western targets increasingly in their cross-hairs. Historically, collaborative efforts among such groups were primarily linked to covert logistical support, including the provision of money, safe havens, and arms, as well as the movement back and forth of key personnel from one entity to another.

Not so today, where the relationships between terrorist groups are becoming more overt and strategic in nature. As events on the ground in Syria demonstrate, there will be no shortage of opportunities for foreign fighters who wish to travel to jihadi conflict zones. Consider also Africa, where the head of U.S. Africa Command General Carter Ham has stated that “` the linkages between AQIM and Boko Haram are probably the most worrisome in terms of the indications we have that they are likely sharing funds, training and explosive materials that can be quite dangerous’.”⁴ So too closer to home, where the Commander of U.S. Southern

² Anouar Boukhars, *The Drivers of Insecurity in Mauritania* *Carnegie Paper* (April 2012) <http://carnegieendowment.org/2012/04/30/drivers-of-insecurity-in-mauritania#>

³ Recently designated a Foreign Terrorist Organization by the Department of State (a too-long delayed move, though one rightly supported by the Chairman of this Committee). <http://translations.state.gov/st/english/article/2012/09/20120907135632.html#axzz26kbUie00>; see also Frank J. Cilluffo, “U.S.-India Counterterrorism Cooperation: Deepening the Partnership” *Hearing before the House of Representatives Committee on Foreign Affairs, Subcommittee on Terrorism, Non-proliferation and Trade* (September 14, 2011) http://www.gwumc.edu/hspi/policy/testimony9.13.11_cilluffo.pdf.

⁴ Tristan McConnell, “Triple threat: Coordination suspected between African terrorist organizations” *Global Post* (June 26, 2012) <http://www.globalpost.com/dispatches/globalpost-blogs/africa/triple-threat-coordination-suspected-between-african-terrorist-or>

Command General Douglas M. Fraser has observed a similar type of convergence (based on convenience) between terrorist and criminal organizations in the Tri-Border area of Argentina, Brazil, and Paraguay.⁵ Within the Continental United States, furthermore, the New York City Police Department has expanded its decade-plus focus on core al Qaeda, affiliates, and the homegrown threat (inspired by AQ), to include Iran and Hezbollah—as part of NYPD’s continuing efforts to build a robust and independent counterterror posture for the City of New York.⁶ In turn, the Los Angeles Police Department recently elevated the government of Iran and its proxies (notably Hezbollah) to a Tier One threat.⁷ This last development is particularly concerning given Iran’s ongoing drive to achieve nuclear weapons capability, and the statement this month of Lebanese Hezbollah leader Sayyed Hassan Nasrallah to the effect that there will be no distinction drawn between Israel and the United States in terms of retaliation, should Israel attack Iran to halt its progress toward the nuclear goal: “If Israel targets Iran, America bears responsibility.”⁸ Both the Director of the (U.S.) National Counterterrorism Center and the Director of National Intelligence have underscored concern about Iran and their proxies, suggesting respectively in recent testimony (the former before this Committee) that “Iran remains the foremost state sponsor of terrorism”⁹; and that Iran is “now more willing to conduct an attack in the United States.”¹⁰

All this to say there is little ground for complacency, as toxic forces converge and cooperate in multiple spots across the globe, more than ever before; as ideology and narrative continue to inspire, including those here in the United States—recall that 58-plus homegrown jihadi terrorism plots have been discovered in this country since 9/11; and as foreign fighters return to their homelands battle-hardened and armed with Western passports—ten feet tall in the eyes of those who admire their exploits, and more importantly, a direct threat to Western security given their familiarity with potential targets they may select to attack.¹¹ Where foreign fighters are concerned, so-called “bridge figures” are of special importance, as they ensure that particular fighter pool is replenished, by helping to inspire, radicalize, and motivate. These figures exude charisma, and exhibit cultural and linguistic fluency as well as other skills that propel them to positions of leadership, guidance, and prominence. Abdullah

⁵ Statement before the Senate Armed Services Committee (March 6, 2012) <http://www.armed-services.senate.gov/statemnt/2012/03%20March/Fraser%2003-13-12.pdf>

⁶ 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) <http://homeland.house.gov/sites/homeland.house.gov/files/Testimony-Silber.pdf>

⁷ Frank J. Cilluffo, Sharon L. 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/>

⁸ Reuters, “Nasrallah: Iran could strike US bases if attacked” *The Jerusalem Post* (September 3, 2012) <http://www.jpost.com/IranianThreat/News/Article.aspx?id=283706>

⁹ Matthew G. Olsen, “Understanding the Homeland Threat Landscape” *Hearing before the House Committee on Homeland Security* (July 25, 2012) <http://homeland.house.gov/sites/homeland.house.gov/files/Testimony-Olsen.pdf>

¹⁰ James R. Clapper, “Unclassified Statement for the Record on the Worldwide Threat Assessment of the US Intelligence Community for the Senate Select Committee on Intelligence” (January 31, 2012) <http://intelligence.senate.gov/120131/clapper.pdf>

¹¹ Frank J. Cilluffo, “Open Relationship” *ForeignPolicy.com* (February 15, 2012) http://www.foreignpolicy.com/articles/2012/02/15/open_relationship?page=0.0; and 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).

al-Faisal, a Jamaican with ties to shoe bomber Richard Reid and to (attempted) Times Square bomber Faisal Shahzad, is but one example.¹²

Just as the threat has gravitated and metastasized to areas in the physical world that will best support the ideology and activities at issue, so too has the threat taken hold in (and of) the cyber domain—where terrorists are still afforded too much freedom of maneuver. Being squeezed in Pakistan's FATA, the Sahel, Yemen, or elsewhere, does not mean "game over" when the Internet offers a transnational base and springboard for a variety of operations, including fundraising, recruitment, planning, training, and even implementation and execution of plots and plans.¹³ As I outlined in testimony before the Senate five years ago: "Extremists value the Internet so highly that some have adopted the slogan 'keyboard equals Kalashnikov'. Terrorist groups now have their own media production arms (al Qaeda relies on As-Sahab and the Global Islamic Media Front, for example). Terrorists produce their own television programs and stations, websites, chat rooms, online forums, video games, videos, songs, and radio broadcasts."¹⁴ Having said that, and as I have indicated in further Senate testimony, this one more than a decade ago: "Bits, bytes, bugs, and gas will never replace bullets and bombs as the terrorist weapon of choice."¹⁵

However, as kinetic measures (U.S. and allied) generate gains in the real-world, this may lead al Qaeda and its sympathizers to enter even more deeply into the cyber domain. Indeed, al Qaeda and their jihadi ilk may be surfing in the wake of "Anonymous" and other such groups, to learn from and perhaps also exploit their actions. The cyber threat writ large is much broader and more multifaceted, though. It may emanate from individual hackers, "hacktivists," criminal or terrorist groups, nation-states or those that they sponsor. Moreover, the threat spectrum affects the public and private sectors, the interface and intersections between them, as well as individual citizens. From a homeland security perspective, foreign states are (by and large) our principal concerns in the cyber domain, at least in terms of sophistication; specifically those countries that pose an advanced and persistent threat, namely Russia and China. Their tactics may also be exploited by others.¹⁶ Furthermore, as laid out in my testimony to a joint hearing of two Subcommittees of this body in April 2012, the government of Iran and its terrorist proxies are serious concerns in the cyber context. What Iran may lack in capability, it makes up for in intent; and our adversaries do not need

¹² Frank J. Cilluffo, Jeffrey B. Cozzens, and Magnus Ranstorp, *Foreign Fighters: Trends, Trajectories & Conflict Zones* (October 1, 2010)

http://www.gwumc.edu/hspi/policy/report_foreignfighters501.pdf

¹³ The George Washington University Homeland Security Policy Institute (HSPI) and the University of Virginia Critical Incident Analysis Group (CIAG), *NETworked Radicalization* (Special Report: May 2007) <http://www.gwumc.edu/hspi/policy/NETworkedRadicalization.pdf>

¹⁴ "The Internet: A Portal to Violent Islamist Extremism" (May 3, 2007)

http://www.gwumc.edu/hspi/policy/testimony5.3.07_cilluffo.pdf

¹⁵ "Critical Infrastructure Protection: Who's In Charge" (October 4, 2001)

http://www.gwumc.edu/hspi/policy/testimony10.4.01_cilluffo.pdf

¹⁶ Frank J. Cilluffo, "The U.S. Response to Cybersecurity Threats" *American Foreign Policy Council (AFPC) Defense Dossier* (August 2012) <http://www.afpc.org/files/august2012.pdf>; see also Office of the National Counterintelligence Executive (NCIX), *Foreign Spies Stealing US Economic Secrets in Cyber Space: Report to Congress on Foreign Economic Collection and Industrial Espionage 2009-2011* (October 2011)

http://www.ncix.gov/publications/reports/fecie_all/Foreign_Economic_Collection_2011.pdf

highly sophisticated capabilities—just intent and cash—as there exists an arms bazaar of cyber weapons, allowing our adversaries to buy or rent the tools they need or seek.¹⁷

The cyber threat (and supporting technology) has markedly outpaced our prevention and response efforts. Use of cyber means as a force multiplier for kinetic activities, which would represent the convergence of the physical and cyber worlds, constitutes probably the area of greatest concern over the next 5 to 10 years. Foreign militaries are increasingly integrating computer network attack (CNA) and computer network exploitation (CNE) capabilities into their warfighting, and military planning and doctrine.¹⁸ Such activity may involve “intelligence preparation of the battlefield,” to include the mapping of perceived adversaries’ critical infrastructures. 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. Foreign intelligence services, too, are engaging in cyber espionage against us, often combining technical and human intelligence in their exploits. Here, 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 significantly degrade our national defense and national security, and thereby undermine the trust and confidence of the American people in their government.

New opportunities for resilience, generated by forces including changing technologies, will assuredly present themselves. Indeed it is this ability to reconstitute, recover, and get back on our feet is in fact perhaps the best deterrent. The storms that battered the National Capital Region this summer 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 U.S. critical infrastructure from 2009 to 2011.¹⁹ The good news, on the other hand, is that the most serious of these incidents could have been avoided 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.

¹⁷ “The Iranian Cyber Threat to the United States” *Statement before the House of Representatives Committee on Homeland Security, Subcommittees on Counterterrorism and Intelligence, and on Cybersecurity, Infrastructure Protection, and Security Technologies* (April 26, 2012) <http://www.gwumc.edu/hspi/policy/Iran%20Cyber%20Testimony%204.26.12%20Frank%20Cilluff%20.pdf>

¹⁸ Bryan Krekel, Patton Adams and George Bakos, *Occupying the Information High Ground: Chinese Capabilities for Computer Network Operations and Cyber Espionage*, Prepared for the U.S.-China Economic and Security Review Commission by Northrop Grumman Corporation (March 7, 2012) p. 54 [http://www.uscc.gov/RFP/2012/USCC%20Report Chinese CapabilitiesforComputer Network OperationsandCyberEspionage.pdf](http://www.uscc.gov/RFP/2012/USCC%20Report%20Chinese%20CapabilitiesforComputer%20NetworkOperationsandCyberEspionage.pdf)

¹⁹ 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/>

DHS: A LOOK BACK AND AHEAD

Looking ahead, U.S. and allied counterterrorism efforts that achieved localized successes must be woven into a larger, sustained and strategic effort; one that continues to apply targeted pressure to deny adversaries the time and space to maneuver, including in cyberspace. Since the threat now comes in various shapes, sizes, and forms—ranging from al Qaeda's Senior Leadership (Ayman al-Zawahiri and his top deputies), to its principal franchises and affiliates, to individuals inspired by (if not directly connected to) al Qaeda's ideology, which includes the "homegrown" threat—the U.S. response, and that of DHS in turn, must be at once both sufficiently comprehensive in scope and sufficiently nimble in approach to address effectively the multidimensional threat landscape of today as well as tomorrow.

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. A sustained, comprehensive, integrated, and effective effort to combat violent Islamist extremism is, in my view, the biggest element missing from U.S. statecraft on counterterrorism. Although the Department of State's Center for Strategic Counterterrorism Communications (CSCC) is doing some good work and represents a positive development in this space, now is the time to double down, do more, and hit back harder. 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 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. The increasingly hybrid nature of the threat presents additional opportunities in this last regard, as drugs and arms trafficking are used to finance terrorism, and so too kidnapping for ransom (think Abu Sayyaf and AQIM). Brokering infighting between and among 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. In short, we could and should do more to drive wedges and foment distrust (including by exploiting points of conflict between local interests and the larger global aims of AQ); encourage defectors; delegitimize and disaggregate our adversaries' narrative; and above all, remember the victims.²⁰

As the distinction between home and abroad increasingly blurs, due in part to technologies and tools such as social media, it is important to study and ultimately institutionalize counterterrorism lessons learned elsewhere, including about tactics, techniques, and procedures. In the aftermath of the "26-11" Mumbai attacks, for instance, the Los Angeles, Las Vegas, and New York City Police Departments each sent a team of experts to Mumbai. The objective was to meet with Indian counterparts to learn about Mumbai's response model and then-existing loopholes, which knowledge LAPD, LVPD, and NYPD could then apply to their home cities, with an eye to closing gaps in their own counterterrorism strategies and operations. More initiatives of this kind are needed, as is the continuation of those that

²⁰ Frank J. Cilluffo, "The Future of Homeland Security: Evolving and Emerging Threats" *Hearing Before the Senate Committee on Homeland Security & Governmental Affairs* (July 11, 2012) <http://www.gwumc.edu/hspi/policy/Testimony%20-%20SHSGAC%20Hearing%20-%2011%20July%202012.pdf>

already exist (such as police exchanges). Endeavors of this type are particularly important in a resource-scarce environment, as they can help avoid the need to reinvent the wheel.²¹

To obtain a truly “rich picture” of the threat in this country, we must focus on the field—not the Beltway. As recent history shows, the military and intelligence communities have 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. 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) in terms of intelligence; 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, which 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 “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. Moreover, opportunities still exist to tap and apply intelligence and information from the field of organized crime to the field of counterterrorism, and vice versa. Hybrid thinking that marries up the two fields in this way, in order to further build our reservoir of knowledge on the counterterrorism side could prove valuable.

Straightforward yet powerful steps remain to be taken. This was revealed starkly in multiple rounds of survey work—first with the major metropolitan intelligence chiefs and later with the fusion centers—that the Homeland Security Policy Institute (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 in June of this year, 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. Furthermore, 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.²² In tandem, and without taking anything away from the Fusion

²¹ Cilluffo, “U.S.-India Counterterrorism Cooperation.”

²² 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”

Centers, Joint Regional Intelligence Groups (JRIGs) also have a role to play, including by helping to place national threat information into State and local context.

DHS continues to mature over time. However its capacities generally still remain reactive in nature. As a result, the Department's internal capabilities to assess future threats and then take actions are not yet evolved to the level that the security ecosystem demands. This is a significant shortfall, especially relative to the cyber domain where threats may morph and metastasize in milliseconds. Volume and pace in the cyber arena alone make for a serious challenge, including the potential for damage to critical U.S. infrastructure such as water and power systems, and telecommunications and finance. Since (as mentioned above) cyber tools/attacks may also be leveraged, acting as a force multiplier in connection with kinetic actions undertaken by our adversaries, the ability to look over the horizon and think creatively, including through the eyes of those of those who may bear hostile intent towards this country, is to be prized. Yet DHS does not currently have the built-in structural capacity to do so. Precisely because the Department must be able to respond to a wide range of threats that may materialize quickly, an Office of Net Assessment (ONA) could and should be created.

The ONA would fill the much-needed role of brain trust, 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 United States requires the constant questioning of assumptions, the asking of what-ifs, and the thinking of the unthinkable, all 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. The duties of ONA should 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. Admittedly, this is a tall order. The alternative, however, is to walk into the future partly blind and thus remain more vulnerable than we need to or should be.

This proposal is not new, I should add. To the contrary, it appeared in the January 2007 Homeland Security Advisory Council Report of the Future of Terrorism Task Force, for which I served as Vice Chairman together with Chairman Lee Hamilton.²³ 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, we must not lose sight of the long game either. Indeed, the general qualities needed from an organizational standpoint (U.S./DHS) mirror many of the traits that our adversaries have exhibited over time. They are proactive, innovative, well-networked, flexible, patient, young and enthusiastic, technologically savvy, and learn and adapt continuously based upon both successful and failed operations around the globe. We and our government must be and do likewise. Our institutions, both their

CTISR (September 2011). <http://www.gwumc.edu/hspi/policy/HSPI%20Research%20Brief%20-%20Counterterrorism%20Intelligence.pdf>

²³ <http://www.dhs.gov/xlibrary/assets/hsac-future-terrorism-010107.pdf>

structure and culture, must be responsive to the ever-changing threat environment. This entails much more than rearranging boxes on an organization chart. Together with policy and technology, people are a crucial component of the equation. Organizational change will not take root unless supported by cultural change, which in turn takes time, leadership, and both individual and community commitment. Many at DHS have worked long and hard to bring about a cohesive and collaborative culture that drives mission success; but we would do well to keep striving on that front, if only because sustaining an end-state can be as difficult as arriving at it in the first place.

The type of forward-leaning assessment and evaluation described above could have a range of salutary knock-on effects, including the possibility of better-calibrated budgeting, operational planning, and acquisitions, through the provision of a foundation from which forward-estimates may be derived. As things now stand, the Department still has a ways to go in terms of aligning actions with future threats—although the Quadrennial Homeland Security Review (QHSR), while less than perfect, has served as a useful starting point. Still, as a mechanism and process for helping to bring DHS resources and plans into sync with the threat environment, the QHSR is not as forward-leaning as it could or should be. The country would be better served by a more robust posture and process, one that anticipates threats before they manifest, and that allows the Secretary to determine what tools are needed for meeting them, what force structure is needed (at the federal, state and local levels), and what resources are needed from Congress to make that plan a reality. Importantly, we do not yet have a true “rich picture” of the domestic threat landscape because the National Intelligence Estimate (NIE) does not fully elaborate upon that dimension. This gap must be remedied, with State and local officials at the heart of that exercise, because they are best-positioned to undertake the task.

Cyber threats in particular manifest in nanoseconds, and we need to be able to enact cyber response measures that are almost as quick. This means developing and implementing an “active defense” capability to immediately attribute and counter attacks and future threats in real-time. Although much work remains to be done on the counterterrorism side, the country has achieved significant progress in this area. In contrast, the U.S. cybersecurity community's state of development is akin to that of the counterterrorism community as it stood shortly after 9/11. Despite multiple incidents that could 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. Officials in the homeland security community should 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. Working together with DHS Intelligence and Analysis colleagues, the Department's National Protection and Programs Directorate (NPPD) could and should do more in terms of threat and intelligence reporting, especially in relation to critical infrastructure, where DHS is well positioned to add real and unique value given the Department's relationship with and responsibilities towards the private sector. Consider the cyber-attacks on Saudi Aramco and Qatari RasGas this past summer, which hit thousands of computers at these critical oil and gas producers with a virus. As events unfolded, one would expect that counterpart industries here in the United States would have welcomed DHS products that directly assessed these events and kept U.S. owners and operators abreast of latest developments, their broader significance and potential follow-on implications.

The United States should also develop and clearly articulate a cyber-deterrence strategy. Such a deterrence policy should apply generally, and also 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, in turn, would free up resources (human, capital, technological, etc.) to focus our limited resources and bandwidth on the high-end of the threat spectrum and on those which are most sophisticated and persistent. To operationalize these recommendations, we must draw lines in the sand. 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. More investment needs to be made in our offensive capability as well, in order to support the foregoing proposals in terms of practice and at the level of principle (to signal a credible commitment). Cybersecurity by definition is transnational in nature and will require some level of transnational solutions, yet it must not be approached like an arms control treaty (i.e., attribution and verification are still a ways away). Notably NPPD, which manages the cyber-portfolio for DHS, has done some good work in the international arena, including cyber-specific capacity-building efforts and exercises, in multilateral settings and with bilateral partners. However, as the Department's Inspector General noted in a report issued just this month²⁴, DHS must continue to build on its *Cybersecurity Strategy* of November 2011²⁵, such as by clearly delineating "roles and responsibilities" for NPPD.²⁶

Plainly we have not yet made the requisite business case for the private sector to undertake and implement needed cybersecurity measures. This represents a fundamental problem, given that the majority of critical infrastructure in this country is owned and operated by the private sector. The urgency for making this case needs no further explanation, but we must take care to strike just the right balance of carrots—such as tax breaks, priority in government contracting opportunities, and indemnification of liability, allowing those who have done what has been asked of them to avoid costly litigation—and sticks; and of measures that ensure both privacy and security. To help ensure compliance with standards and best practices, a "Good Housekeeping" seal of approval could be granted to those who meet the bar. To the extent that this encourages industry-wide adoption and robust outcomes, such measure could spur the insurance and reinsurance sectors to step into the fray. In addition, the federal government has a responsibility to share threat information (i.e., signatures, hostile plans and techniques to degrade, disrupt or destroy systems) that places our critical infrastructures at risk. The pilot program introduced within the confines of the defense industrial base offers a solid starting point, and an example of a promising information-sharing environment.²⁷ It probably should go without saying, but part of leading by example also entails the U.S. government striving to place its own house in order, as a crucial corollary to meeting the threat.

²⁴ DHS Office of Inspector General, *DHS Can Strengthen Its International Cybersecurity Programs (Redacted)* (August 2012) http://www.oig.dhs.gov/assets/Mgmt/2012/OIGr_12-112_Aug12.pdf

²⁵ *Blueprint for a Secure Cyber Future: The Cybersecurity Strategy for the Homeland Security Enterprise* <http://www.dhs.gov/xlibrary/assets/nppd/blueprint-for-a-secure-cyber-future.pdf>

²⁶ Mickey McCarter, "NPPD Lacks Strategy To Guide International Cybersecurity Efforts" *Homeland Security Today* (September 4, 2012) http://www.hstoday.us/index.php?id=3392&no_cache=1&tx_ttnews%5Btt_news%5D=25801

²⁷ Frank J. Cilluffo and Andrew Robinson, "While Congress Dithers, Cyber Threats Grow Greater" *Nextgov.com* (July 24, 2012) <http://www.nextgov.com/cybersecurity/2012/07/while-congress-dithers-cyber-threats-grow-greater/56968/>

In conclusion, the challenges that lie on the horizon remain substantial, but with the requisite will and leadership—to lean forward and exhibit a field bias towards military, intelligence community, and law enforcement experts on the front lines—the country can and will continue to make progress towards meeting those imperatives. Again, I wish to thank 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.

##