

**“Stakeholder Perspectives on Priorities for the
Quadrennial Homeland Security Review (QHSR)”**

**U.S. House of Representatives, Committee on Homeland Security
Subcommittee on Oversight and Management Efficiency**

June 20, 2014


**Frank J. Cilluffo
Director
Homeland Security Policy Institute
and Cybersecurity Initiative
The George Washington University**

Introduction

Chairman Duncan, Ranking Member Barber, and distinguished Members of the Subcommittee, thank you for the opportunity to testify before you today.

The Department of Homeland Security has now completed its second Quadrennial Homeland Security Review (QHSR), and is expected to issue its report to Congress on the results of this review shortly. My testimony today will comment on key issues addressed in a draft version of the report, beginning with general remarks and then focusing on what I believe are the two most critical threats facing the homeland today: terrorism threats and cyber-related threats.

This QHSR comes at a time of significant international instability. Although our homeland security posture has improved substantially in the last decade-plus, the



terrorist threat climate in which the United States finds itself today is in many ways reminiscent of that prior to 9/11, sharing a number of similar attributes and characteristics. The current climate is also one marked by budget cuts as well as the rollback of hard-earned gains that had been achieved through the investment of billions of dollars and, most importantly, the lives of thousands of our men and women in uniform.

Against this background, it is all the more disconcerting to see that in Iraq and Syria, terrorist groups have found space and time in which to maneuver, plot and execute attacks; all while US forces prepare to draw down in Afghanistan. In Africa, we see a constellation of active and skilled terrorist groups in the Maghreb and Sahel, from Boko Haram in Nigeria, to Al Qaeda in the Arabian Peninsula (AQAP) in Yemen, to Ansar al-Sharia in Libya, to Ansar al-Dine in Mali, to Al-Shabaab in Somalia. At the same time, advances in technology have increased the lethality of weapons, targeting systems and means of communications used by terrorists. New and powerful avenues of recruitment and radicalization have opened up, notably through social media. These tools have in effect shrunk the globe as young, tech-savvy and likeminded extremists are connecting in the dark corners of the Web – as evidenced by the swell of foreign fighters flocking to Syria. As a result, what happens overseas has significant domestic implications, including with respect to homegrown violent Islamist extremism.

In addition to the Islamist threat posed by terrorism, the cyber domain is a permissive environment, which is made for plausible deniability, for a wide range of U.S. adversaries who need never set foot in this country in order to do us harm. Our political, military and economic secrets including our intellectual property are being siphoned out covertly by cyber means, specifically computer network exploitation (CNE). From CNE – to include mapping of our critical infrastructure systems, to computer network attack, to cyber-crime perpetrated by forces whose capabilities have grown to such an extent that some of these criminal groups are now even on par with some nation-states' abilities and capacities, the range of activities and actors with hostile intent is both wide and deep. Nation-states are investing in and building up

their cyber war capabilities, as well as integrating these capacities into their broader warfighting doctrine and operations. Moreover, nation-states are making use of proxies for both physical and cyber-attacks. In these regards, China, Iran, North Korea and Russia are of abiding concern.

The ecosystem of threats facing DHS and the homeland is thus varied and seriously challenging. From physical threats to cyber threats, and the nexus between the two, DHS and the nation must stand ready and prepared for the full gamut of these scenarios. We must position ourselves to be as nimble in prevention and response as is required to meet whatever variant or form in which the threat of today and tomorrow manifests.

Overview of the QHSR

Congress established the Quadrennial Homeland Security Review in law in 2007 as a mechanism to focus senior leadership attention at DHS on long-term strategic issues, enhance the strategic planning processes within the Department, and then ultimately to “strengthen the linkages between strategy and execution”¹, particularly with respect to the Department’s operational requirements and budget decisions.

The first QHSR report, released at the end of 2009, played a valuable role with respect to defining the strategic priorities of the Department, but did not have a significant impact in terms of implementation. Very few of the initiatives outlined in the follow-on “Bottom Up Review” were ultimately implemented, and the QHSR did not appear to have a major impact on successive budget requests within DHS.

This second QHSR has built on the positive and negative lessons of the first review, and the activities that informed the review have matured in the past four years. Overall, the strategic framework defined within the report is robust, and reflects hard choices about which issues are of greatest priority to the Department. Notably, it calls out biological threats as a significant homeland security priority – an area that I

¹ Quoted from page 403 of H.R. 110-259, House-Senate Conference Report for the Implementing Recommendations of the 9/11 Commission Act of 2007, July 25, 2007.

believe has received insufficient attention by policy makers in the last few years, but which is likely to represent the greatest long-run catastrophic terrorist threat that we face.²

But the real verdict on this QHSR will come in the months and years ahead. It is imperative that this QHSR is used to inform key strategic decisions in the next four years, starting with the fiscal year 2016 budget request to Congress that will be released next February. As the primary House authorizing committee for DHS, this Committee has the opportunity in the next four years to hold the Department accountable for implementing the strategic priorities outlined in this review.

I should note here that it is refreshing that Secretary Johnson and his leadership team are taking these strategic issues seriously, particularly with respect to the “Unity of Effort” initiative that is underway within the Department, as outlined in a memorandum by Secretary Johnson sent to his senior leadership team in April of this year.³ The issues raised by the Secretary in this memorandum are critical, particularly with respect to the integration and effectiveness of policy, management and operational activities within the Department. I would urge the Committee to consider legislation that strengthens key offices – such as the Office of Policy, which has never been authorized in statute – and holds DHS accountable for making progress on these “unity of effort” objectives, along the lines of what you have already done with the recently-passed legislation on DHS acquisition. I should also note that the Homeland Security Policy Institute is forming a task force that will take an independent look at these “unity of effort” issues, and we look forward to engaging further with the Committee on this in the months ahead.

For the remainder of my testimony, I will focus on two of the five top-level homeland security missions defined within the QHSR framework: preventing terrorism and addressing cyber threats. While my remarks center on these two areas, I would

² See for example Nathan Myhrvold, *Strategic Terrorism: A Call to Action*, The Lawfare Research Paper Series, Research Paper No. 2 - 2013 (July 2013 Working Draft). <http://fortunedotcom.files.wordpress.com/2013/10/strategic-terrorism-myhrvold-7-3-2013.pdf>

³ Memo available at: <http://www.hlswatch.com/wp-content/uploads/2014/04/DHSUnityOfEffort.pdf>

emphasize that we must also remain focused on other important DHS missions, to include emergency preparedness and disaster response, and the task of securing the nation's borders.

Preventing Terrorism

The terrorist attacks and atrocities within the past week in Iraq by ISIS (the Islamic State in Iraq and Syria), in Kenya by Al-Shabaab, and in Nigeria by Boko Haram are stark reminders of the persistent Islamist terrorist threat, not only in the region, but also with respect to the threat of attacks against the homeland. They are also an example of the increasing fragmentation and diversification of terrorist threats; as the introduction to the draft QHSR report notes, “the terrorist threat is increasingly decentralized and may be harder to detect.”

Of particular concern is the foreign fighter threat in Syria, which is now also spilling over into Iraq; indeed, I would argue that the two conflicts are merging into a single regional insurgency. In Syria, we have seen the ongoing civil war become a magnet for foreign fighters from no less than 74 countries around the world.⁴ Up to 3000 westerners have traveled to fight in Syria since the conflict began, including more than 70 Americans.⁵ Disturbingly, the Syrian conflict has given rise to new networks and new connections. For example, bomb makers are meeting up with individuals who are well versed in media, especially social media. Armed with Kalashnikovs, laptops and cellphones, foreign fighters are thus amassing and emerging with new and blended skill-sets and expertise, including potentially expertise with chemical weapons.

Within the past month, we have begun to see examples of the global implications of this foreign fighter threat. In late May, a French national and former Syrian foreign fighter committed a terrorist attack at a Jewish museum in Brussels, Belgium, killing four people. The United Kingdom and Spain both made high-profile arrests of

⁴ Aaron Y. Zelin, “Up to 11,000 foreign fighters in Syria; steep rise among Western Europeans,” The International Centre for the Study of Radicalisation (ICSR) – Insight (Dec. 17, 2013), <http://icsr.info/2013/12/icsr-insight-11000-foreign-fighters-syria-steep-rise-among-western-europeans/>

⁵ Kimiko De Freytas-Tamura, “Foreign Jihadis Fighting in Syria Pose Risk in West,” *New York Times* (May 29, 2014), <http://www.nytimes.com/2014/05/30/world/middleeast/foreign-jihadis-fighting-in-syria-pose-risk-in-west.html>

individuals recently who had traveled to Syria to fight or who were involved in facilitating such travel. And an American citizen from Florida who was fighting in Syria carried out a suicide truck bombing attack in late May. ISIS is now issuing English-language propaganda, similar in nature to Al Qaeda in the Arabian Peninsula's Inspire magazine.⁶ These examples are likely to be leading indicators of a direct terrorist threat that the United States and other western nations will face in the months and years ahead.

Countering the challenge posed by foreign fighters must therefore be a priority mission for DHS, and not just conceptually. The Department of Homeland Security already plays an important role in one way in mitigating potential threats to the homeland from Syrian foreign fighters: its activities to detect and prevent terrorist travel and entry into the United States. It is critical that key activities related to terrorist travel – at CBP, TSA, ICE, US-VISIT, and the Office of Intelligence and Analysis – are maintained and strengthened even in this difficult budget environment for the Department.

Another key responsibility for DHS (along with the FBI, National Counterterrorism Center, the State Department and other agencies) has been less well developed: countering the ideologies of violent Islamist extremism (“CVIE”) that radicalize individuals and replenish the ranks of our terrorist adversaries. This is the biggest missing dimension of US counterterrorism statecraft to date. The State Department's Center for Strategic Counterterrorism Communications is doing some good work overseas in this area in foreign languages, but very little is being done domestically. A systematic strategic communications effort is needed, aimed at exposing the hypocrisy of our adversaries' words versus their deeds. The goal is to knock terrorist groups off balance; embarrass their leadership by bringing to light their seamy connections to criminal enterprises and drug trafficking organizations; and broker infighting among al Qaeda, its affiliates, and the broader jihadi orbit in which they reside – which will damage violent extremists' capability to propagate their message and organize

⁶ Rosen, Armin, “ISIS is Bragging about its ‘Brazen’ Attack on Mosul in its English Language Magazine.” *Business Insider* (June 10, 2014). <http://www.businessinsider.com/isis-is-bragging-in-its-english-language-magazine-2014-6>

operations.⁷ Again, it is crucial to link priorities with budgets. A former senior White House official, Quintan Wiktorowicz, recognizes as much in recent commentary that emphasizes the need for a dedicated CVIE budget: “It is Time to Fund Domestic Counter-Radicalization.”⁸ The piece makes several solid points, including the need to invoke community engagement in this effort. While that is part of the equation, however, CVIE also needs to support the pointier end of operational counterterrorism efforts, federally and at the state and local level.

The current conflict in Syria and Iraq is symptomatic of a broader concern: the circumstance of ungoverned or under-governed spaces that provide our adversaries with the time and space needed to recruit, train and plot. Instead of being back on their heels, looking over their shoulders, our adversaries are benefiting from conditions that provide them with a level of freedom of action that they have not experienced in recent history. Note that ungoverned and under-governed spaces do not need be geographically vast in order to facilitate terrorist activity; under-governed neighborhoods in large cities in countries such as Pakistan, Kenya and Nigeria can also provide a form of safe haven to terrorist groups. Urban environments also serve to limit US military options. To further cement the dilemma, these developments are taking place when our intelligence collection platforms are becoming fewer and perhaps less effective than in the past, due to the drawdown of American forces in Afghanistan and Iraq and due to the damaging revelations of critical US intelligence collection activities in the past year.

For all of these reasons, the terrorist threat to the homeland is becoming increasingly grave, and it is critical that DHS and its federal, state and local partners remain focused on detecting and countering these threats in the months and years ahead. As threats evolve, DHS also needs to be agile and continuously evaluate the effectiveness of its various activities in countering such threats, and invest in new tools and capabilities to address emerging threats. This Committee can play a significant role in

⁷ Frank J. Cilluffo and Sharon L. Cardash, “It’s the Ideology, Stupid,” *The National Interest* (June 3, 2013), <http://nationalinterest.org/commentary/it%E2%80%99s-the-ideology-stupid-8537>

⁸ <http://www.lawfareblog.com/2014/06/the-foreign-policy-essay-it-is-time-to-fund-domestic-counter-radicalization>

ensuring that the Department does not succumb to inertia and is focused on anticipating and addressing such emerging threats.

Cybersecurity

The rapid growth in cyber-related threats in the last few years has led some senior government officials to assert that cyber threats have now surpassed terrorism as the most significant national security threat to the United States. I am not yet prepared to agree with such an assessment, for all of the reasons discussed in the previous section; and would argue instead that it is not an either/or proposition – that we must be prepared to defend against both types of threats. But it is undoubtedly true that the cyber threats to US national security and economic interests have significantly advanced in recent years, and taken on new dimensions, particularly in the area of cyber threats to critical infrastructure.

The cyber and physical threats to critical infrastructure have been a key focus of executive branch policy making in the past two years, through activities mandated by Executive Order 13636 and Presidential Policy Directive 21. These threats are also highlighted in the draft QHSR report, which discusses how cyber-physical convergence and interdependence has “changed the risks to critical infrastructure in sectors ranging from energy and transportation to agriculture and health care.” Vulnerabilities in these sectors could give rise to catastrophic outcomes, especially if cascading effects ensue as a result of interdependencies between and among critical sectors. The physical attack last year on the PG&E Metcalf substation is an example of this convergence and interdependence of threats; if that attack had been slightly more damaging, it could have had a severe impact on the power grid in Silicon Valley.

DHS plays a critical role in addressing and mitigating these cyber threats, working with other federal, state and local government partners on threats to government networks, and of equal importance, forming strong partnerships with the private sector. These public-private partnerships are critical given that the predominant share of the relevant cyber infrastructure and expertise is located within the private sector – in Silicon Valley, and in our key economic sectors, including defense, energy, finance

and telecommunications. DHS has made significant progress in building its relationships with the private sector on cybersecurity in recent years, particularly with respect to its incident response activities at the National Cybersecurity & Communications Integration Center (NCCIC) and Industrial Control Systems Cyber Emergency Response Team (ICS-CERT). But it still needs to improve, particularly with respect to its analytic activities on cyber threats and risks. Currently responsibility for cyber analysis is split between the DHS Office of Intelligence and Analysis (I&A), and the National Protection and Programs Directorate. These two parts of DHS need to become better synchronized in their analytic efforts and work together to best support critical infrastructure stakeholders in the private sector.

Final Thoughts and Recommendations

The QHSR is an important deliberative process for the Department of Homeland Security. Unless we define our priorities clearly and fund them accordingly, we will not be optimizing our efforts to address these critical threats to the homeland.

But such a review cannot simply be an exercise that takes place every four years; the threats that we face are evolving too rapidly for such widely spaced reviews. Instead, this process of review and assessment needs to be fully embedded into the day-to-day decision-making processes of the Department. One proposal that would promote this is the establishment of an Office of Net Assessment (ONA) within DHS, similar to the office of the same name at the Department of Defense. The ONA would produce comprehensive long-term analysis of future homeland threats and the capabilities needed to meet those threats. I would urge this Committee to consider establishing the ONA in law, building on the existing capabilities of the Office of Strategy, Planning, Analysis and Risk within the DHS Office of Policy. This is not a new idea, but rather one that Congressman Lee Hamilton and I first put forward back in January 2007, in the Homeland Security Advisory Council (HSAC) Report of The Future of Terrorism Task Force.⁹

⁹ Report available at: <http://www.dhs.gov/xlibrary/assets/hsac-future-terrorism-010107.pdf>

In closing and as detailed above, I would recommend the following actions for your consideration:

- The ultimate value of the QHSR will be determined by the influence that it has on budgets, plans, and operational requirements. This Committee can use its oversight function to determine whether this is being done. Otherwise, policies such as the QHSR are merely empty rhetoric.
- Introduce and work to pass a set of DHS authorization bills. This is a challenge given the fragmented structure of Congressional oversight of DHS, but is worth pursuing, and can be done in piecemeal manner to reduce the complications caused by this jurisdictional situation. In particular, the Committee can authorize the headquarters elements of the Department and update core DHS authorities in the Homeland Security Act. Legislation can also be moved to authorize other components of DHS, such as Customs and Border Protection, as Chairman McCaul has recently proposed.
- To support DHS authorization, the Committee should work with the Department to strengthen the annual Future Years Homeland Security Program (FYHSP) reports required currently in the Homeland Security Act, so that they can be used as a critical source of information for authorization legislation, along the lines of the role played by the Future Years Defense Program (FYDP) reports for annual defense authorization legislation.
- As part of authorization legislation, establish the DHS Office of Policy in law, to be led by an Under Secretary for Policy. This idea was originally proposed by Secretary Chertoff nearly nine years ago, but has stalled because of resistance by Congressional committees that have secondary jurisdiction over parts of DHS. It is time to elevate and strengthen the Office of Policy by the finally establishing it in law, a step that will also give Congress greater influence over its priorities and functions.
- Establish an Office of Net Assessment (ONA) within DHS to provide the Secretary with comprehensive analysis of future threats and U.S. capabilities to meet those threats.

- Prioritize the challenge posed by foreign fighters, particularly those fighting in Syria and Iraq. In part this means maintaining and strengthening key DHS activities related to terrorist travel, even in this difficult budget environment. It also means placing greater priority and increasing funding for programs and activities intended to counter violent Islamist extremism.
- Better synchronize I&A and NPPD in terms of their cyber analytic activities and private sector stakeholder outreach.

Thank you again for the opportunity to testify before you today. I look forward to trying to answer any questions that you may have.

##