“A Call for a Homeland Security Net Assessment”

Erik J. Dahl
Naval Postgraduate School
Monterey, California¹
ejdahl@nps.edu

Prepared for delivery at the ISAC-ISSS annual conference
Austin, Texas, November 2014

Draft as of November 12: please do not cite without permission
Comments very welcome

Abstract

The concept of net assessment has long been considered an important tool for American national security strategists, and the Pentagon’s Office of Net Assessment is widely regarded as a key influence in security planning. But despite calls by experts for the development of a similar net assessment office in the Department of Homeland Security (DHS), only a few tentative efforts have been made to use the concepts and methodologies of net assessment for the problem of ensuring American homeland security. This paper argues that the tool of homeland security net assessment is even more needed today, when debates over the state of the nation’s security involve discussions not only about the seriousness of the threat, but about the legitimacy of the intelligence and other efforts being employed to combat that threat. It proposes a new model for a homeland security net assessment process that should be undertaken by DHS, and suggests that such an assessment would expand the discussion of homeland security threats beyond terrorism and would encourage greater focus on civil liberties and disaster preparedness.

¹ The views presented in this paper are those of the author, and they do not represent the official position of the Naval Postgraduate School, Department of the Navy, or U.S. government.
Introduction

The concept of net assessment has long been considered an important tool for American national security strategists, and the Pentagon’s Office of Net Assessment is widely regarded as an important influence in security planning. But despite calls by experts for the development of a similar net assessment office in the Department of Homeland Security (DHS), only a few tentative efforts have been made to use the concepts and methodologies of net assessment for the problem of ensuring American homeland security. This paper attempts to sketch out the factors that might be involved in conducting a homeland security net assessment. It argues that the tool of homeland security net assessment is even more needed today, when debates over the state of the nation’s security involve discussions not only about the seriousness of the threat from terrorism and other sources, but about the legitimacy of the intelligence and other counter-terrorism efforts being employed to combat those threats.

Other studies have examined the potential structure of a DHS Office of Net Assessment, and this paper will not focus on organizational issues. Instead, this paper proposes a framework for thinking about the task of homeland security net assessment, and suggests a new model for a homeland security net assessment process that should be undertaken by DHS. A net assessment of homeland security today must involve more than just the two principal factors involved in a traditional net assessment, which are the enemy and one’s own forces. Because homeland security efforts are so directly focused within America’s borders—the homeland—we need in addition to consider the effect of these efforts on the American people and society. For this reason, this paper argues that the three factors of importance in conducting a homeland security net assessment are the threat, our own capabilities to counter that threat, and the legitimacy of those capabilities, such as concerning the challenges presented by domestic intelligence programs to civil liberties and domestic society.

The paper begins by reviewing the concept of net assessment and how it has been used in the U.S. Department of Defense (DoD). The subsequent section examines proposals that have been made for the Department of Homeland Security to establish an Office of Net Assessment following the DoD model. Following that is an argument for how the process of net assessment should be modified for the problem of homeland security, and then a proposed model that could

---

be adopted by DHS. The final section of the paper offers some very preliminary suggestions for what the results might be from such a homeland security net assessment process.

What is net assessment?

The concept of net assessment arose during the Cold War, when it was realized that the traditional tools and systems for analyzing national security challenges did not include any place or procedure for carefully integrating assessments of the enemy threat with an understanding of one’s own capabilities. Intelligence agencies and officials typically refrained from analyzing “blue force” capabilities, while operational planners, who did understand U.S. capabilities, could not be sure that they were privy to the best (and often most highly classified) intelligence information on the enemy they were planning against. In addition, there was no institutional advocate for taking a long-term, strategic level approach to national security problems; within the intelligence community and the policy establishment, current problems and issues invariably prevented senior analysts and decision makers from being able to think about long term goals and threats.

Net assessment is closely identified with Andrew Marshall, the founder and still today—although he has recently announced he plans to retire—Director of the Office of Net Assessment in the Department of Defense. Although Marshall and his office have become famous among strategic thinkers, the concept of net assessment remains relatively little known outside defense circles. Several think tanks and analysts have adopted the idea, and a few scholars have suggested that net assessments should become more widely used today.


It is often said that the Pentagon’s Office of Net Assessment has encouraged pessimistic thinking and worst-case scenarios. During the late years of the Cold War, for example, Eliot Cohen argued that a net assessment approach helped to demonstrate the weakness in the analysis of some authors and scholars whom he called Optimists, who believed that the conventional military balance in Europe at the time favored NATO rather than the Warsaw Pact. More recently, one critic has called the ONA “a full-time office of threat inflation,” and some have charged that Marshall and ONA tend to exaggerate threats, in particular concerning China, which has been the subject of a great deal of ONA-sponsored work in recent years. Marshall acknowledged in an interview that “We tend to look at not very happy futures.”

Early in his tenure, Marshall wrote that national assessments “are intended to provide insight for policymakers at the highest levels by discovering and illuminating the nature of major national security problems.” The key element of a net assessment is a comparison of two sides in interaction with one another. In the words of Eliot Cohen, “Net assessment is the appraisal of military balances.” It might strike an observer as self-evident that strategists and military planners should be taking into account assessments of both sides of a situation. After all, Sun Tzu famously advised that a general must “know the enemy and know yourself; in a hundred battles you will never be in peril.” But in fact, this is only rarely done. As the authors of a Carnegie Endowment net assessment put it, “only a net assessment requires the analyst to have an understanding of the capabilities of friendly forces. Although obtaining an understanding of friendly forces sounds easy—especially for government analysts—is can be anything but.”

Although the net assessment approach has been used most notably by the Pentagon, it does not focus only on purely military factors. The Department of Defense defines net assessment as “the comparative analysis of military, technological, political, economic, and other

6 Lewis, “Yoda Has Left the Building.”
8 Jaffe, “Real Tensions Over a Theoretical War.”
factors governing the relative military capability of nations. Its purpose is to identify problems and opportunities that deserve the attention of senior defense officials.”

Most advocates of net assessment see it as a broad-based, interdisciplinary approach, taking into account economic, political, technological, and social factors in addition to military.

Its focus is on the long term, looking out past the typical American government perspective that is often shaped by the length of a presidential administration. Paul Bracken writes, “One of the greatest contributions of net assessment is that it calls for consciously thinking about the time span of the competition you are in.” This long-term view may in fact be one reason why the Pentagon’s Office of Net Assessment has been seen as successful: it can be hard to criticize assessments about a future that is decades away.

Advocates of the net assessment approach believe in the importance of identifying long-term trends. As Aaron Friedberg has noted, “Trends are important because the past will always shape, even if it does not completely determine, the future.”

Another key aspect of the net assessment approach, as it has been practiced in the Pentagon, is that it does not produce specific policy recommendations. Marshall writes that net assessment should “Aim at providing diagnosis of problems and opportunities, rather than recommended actions. The focus on diagnosis rather than solutions is especially significant.”

He explained in an interview that the need to provide policy prescriptions can “corrupt the analysis,” because it will tend to blur objectivity. He said, “People psychologically favor certain policies and then distort the analysis. In order to get [an] even handed, objective approach you [need] to . . . constrain it to the diagnosis problem.”

Net assessments involve both quantitative and qualitative analysis. Even in assessments of the military balance between two countries, which might lend themselves to a largely quantitative analysis, advocates prefer to avoid a strictly numbers-based approach. Eliot Cohen,
for example, argued during the Cold War that it was important “to get beyond mere ‘bean counting’” and understand how each side operated its forces.20

**DHS and net assessment**

There is no central office or organization in the U.S. government responsible for producing net assessments focusing on homeland security issues. The National Counterterrorism Center (NCTC) is chartered with having the primary responsibility within the U.S. government for conducting net assessments of terrorist threats.21 But its work appears to be mostly classified, and it is not known whether it conducts regular net assessments, or whether they are useful to policy makers. Some elements of DHS do appear to conduct net assessments, such as the Domestic Nuclear Detection Office (DNDO), which has as one of its functions the mission of performing red team and net assessments.22 But many observers have argued that DHS should make greater use of net assessments, and should establish a net assessment office similar to the Pentagon’s.

In 2007 the Homeland Security Advisory Council issued a report calling on DHS to “establish an Office of Net Assessment (ONA) within the Department to provide the Secretary with comprehensive analysis of future threats and U.S. capabilities to meet those threats.”23 A report by the Heritage Foundation argued that DHS should form a small, nonpartisan Office of Net Assessment that would be able to focus on long-term challenges and help address the complaint by the 9/11 Commission and others that the nation suffered from a “lack of imagination.”24 A strong advocate of establishing a net assessment capability within DHS has been Frank J. Cilluffo, the Director of the Homeland Security Policy Institute at the George Washington University. Cilluffo argues that DHS responds to most threats reactively, and has only a limited capability for assessing future threats:

> 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.25

One particular area in which a net assessment has been called for is bioterrorism. In 2004 the Bush administration published Homeland Security Presidential Directive 10, *Biodefense for the 21st Century*, which called for “a periodic senior-level policy net assessment that evaluates progress in implementing this policy, identifies continuing gaps or vulnerabilities in our biodefense posture, and makes recommendations for re-balancing and refining investments among the pillars of overall defense policy.”26 Such a net assessment was reportedly conducted, but has not been publicly released.27

Patrick Forrest and Alex Hilliker argue that an Office of Net Assessment is needed within DHS in order to provide long-term strategic assessments of future security threats, without being subject to the many reporting requirements that are placed on existing DHS offices such as the Office of Strategic Plans (OSP).28 They write that DHS leadership has suffered from a lack of data-driven, long-term threat assessments, and as a result billions of dollars have been spent on ineffective programs such as the Secure Border Initiative Network.29 They suggest that a relatively small, independent office reporting directly to the Secretary of Homeland Security be established whose focus “would be solely on producing assessments intended to increase the leadership’s situational awareness regarding future challenges to the homeland security enterprise.”30

**A new model for homeland security net assessment**

In recent years national security leaders have frequently argued that the threats facing America’s security today are more challenging than those seen in the past. Director of National

---

Intelligence James Clapper testified before the Senate that “Looking back over my now more than half a century in intelligence, I’ve not experienced a time when we’ve been beset by more crises and threats around the globe.” General Martin Dempsey, the Chairman of the Joint Chiefs of Staff, testified that “I will personally attest to the fact that it [the world] is more dangerous than it has ever been.” Some critics have charged that such dire warnings are exaggerations, and DHS Secretary Jeh Johnson has not taken quite such a pessimistic view. But Johnson has also made it clear that the threat is serious: “the United States faces a constantly evolving threat environment. Thirteen years after the 9/11 attacks, threats to our nation have not subsided.”

What threats should be part of a homeland security net assessment? Clearly, one focus would be on the terrorist threat to the United States. DHS Secretary Johnson has said that “The cornerstone of our mission at the Department of Homeland Security has been, and should continue to be, counterterrorism—that is, protecting the nation against terrorist attacks.” A focus on terrorism might suggest that a homeland security net assessment should compare the threat from specific groups or actors (such as al Qaeda or ISIS) with the counter-terrorism capabilities available to the combat them. Although estimates of the terrorist threat are available in abundance, there appear to be few, if any, net assessments available that would compare the terrorist threat with U.S. counterterrorist capabilities.

But even though terrorism might be considered “job one” for homeland security, it is not the only threat and not the only mission for the homeland security enterprise. The recently concluded Quadrennial Homeland Security Review found that terrorism is only one of several primary homeland security concerns:

- The terrorist threat is increasingly decentralized and may be harder to detect.
- Cyber threats are growing and pose ever-greater concern to our critical infrastructure systems as they become increasingly interdependent. Natural

---

36 At least one analyst has called for such work to be done: Adam Elkus, “Towards a Counterterrorism Net Assessment,” Small Wars Journal, December 21, 2011.
hazards are becoming more costly to address, with increasingly variable consequences due in part to drivers such as climate change and interdependent and aging infrastructure.37

These three categories of challenges—terrorism, cyber, and natural hazards—may provide a useful and more complete framework for understanding the threats that would be examined by a homeland security net assessment.

There is more to a net assessment, though, than an examination of the threat. A net assessment must also provide decision makers with an understanding of our own capabilities, and this aspect is even more important in the area of homeland security than national security. Rose McDermott has noted that the second part of Sun Tzu’s advice—the need to know oneself—is especially important in the field of homeland security: “Certainly for purposes of homeland security, recognizing our own gaps and failings is an important part of triumphing over our limitations.”38 The adversary may not be far away in a distant land, but is instead here in the middle of the American homeland. The capabilities developed to counter homeland security threats will tend to involve and affect a broader range of American citizens than will the military, foreign policy, and intelligence capabilities that are used to counter foreign threats.

A homeland security net assessment, then, might examine the threats from terrorism, cyber, and natural hazards, and the capabilities that have been developed to address each of these threats. But that, too, would not be enough. Because homeland security efforts are directly focused within America’s borders, we need in addition to consider the effect of those efforts on the American people and society. If a national security net assessment is the appraisal of military balances, as Eliot Cohen described it above, then a homeland security net assessment should be the appraisal of other, equally important balances, such as the balance between security and liberty that is at the forefront of many discussions of homeland security. The requirement to understand the effect of our policies on the American people might be captured in the concept of legitimacy: are the capabilities that our government has developed to keep us safe seen as legitimate in the eyes of the people they are designed to serve?

There is nothing new in arguing that domestic and public concerns are critical for understanding threats and strategies. Advocates of net assessment often cite Carl von Clausewitz

approvingly, noting his argument that war is an extension of politics by other means—implying that both political and military issues must be involved in conducting a true net assessment.\(^{39}\)

Even more appropriate for our purposes may be what Clausewitz referred to as the “remarkable trinity.” This trinity has often been translated as the people, the army, and the government; Clausewitz argued that war is the product of the interaction of these three forces, and a strategist can only understand war by understanding all three.\(^{40}\)

A similar trinity—a homeland security trinity—may be helpful in understanding the forces that must be understood in order to conduct a homeland security net assessment. This trinity involves the threats, capabilities, and legitimacy involved in homeland security.\(^{41}\) When these three factors are arrayed against the three types of threats identified above, we develop a matrix that may be used in conducting a homeland security net assessment:

<table>
<thead>
<tr>
<th></th>
<th>Terrorism</th>
<th>Cyber</th>
<th>Natural hazards</th>
</tr>
</thead>
<tbody>
<tr>
<td>Threat</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Capability</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Legitimacy</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Our proposed homeland security net assessment process, then, would examine the threat to America’s security in three broad categories: terrorism, cyber, and natural hazards. And for each threat, the assessment would examine the nature of that threat; the capabilities that have been developed to counter the threat; and whether those capabilities are seen by the American

\(^{39}\) For example, Skypek, “Evaluating Military Balances Through the Lens of Net Assessment,” 6.

\(^{40}\) It is important to note that Clausewitz’s discussion of the trinity is considerably more complex than simply the interaction of the people, the army, and the state. He described the components of the trinity as 1) primordial violence, hatred, and enmity; 2) the play of chance and probability; and 3) the subordination of war to rational policy. He went on to state that the first of these mainly concerns the people, the second the army, and the third the government, but scholars have argued that this shorter definition of the trinity is too simplistic or even wrong. For a discussion of this debate, see Edward J. Villacres and Christopher Bassford, “Reclaiming the Clausewitzian Trinity,” Parameters, Autumn 1995, 9-19.

\(^{41}\) I am grateful to Captain Todd Veazie, U.S. Navy, for suggesting that Clausewitz’s concept of the trinity can be helpful in understanding homeland security.
people as legitimate or are seen as risking civil liberties or other democratic values. The next section will undertake to sketch out what such a homeland security net assessment might reveal.

**A very preliminary homeland security net assessment**

Although the Pentagon’s Office of Net Assessment has often been seen as a source of pessimistic, worst-case thinking, a homeland security net assessment would be most useful for policy makers if it were seen as producing objective, fact-based reports on long-range trends and issues concerning the most important threats facing the nation. These assessments could fill a niche between, on the one hand, the pessimistic studies often produced by outside critics of whichever administration is in power, and on the other hand the considerably more optimistic reports that are typically issued from government agencies when they attempt to assess their own accomplishments.

This section attempts to suggest some of the issues and problems that a homeland security net assessment might help to illuminate.

**Terrorism**

In its analysis of the terrorist threat facing the United States, a homeland security net assessment would need to take a broad, long-range view. An example of such a perspective can be found in the work of Brian Jenkins, who has noted that the level of terrorist violence in the U.S. during the past decade has been considerably less than that experienced during the 1970s, “when there were 50 to 60 terrorist bombings a year in the United States.”

That statistic is likely to come as a surprise to most Americans, and a task for a net assessment would be to determine how significant such historical comparisons are for today.

A net assessment would also need to consider the impact of more recent events such as the death of Osama bin Laden, the upheaval of the Arab Spring, and the rise of ISIS. The last National Intelligence Estimate to be written (or at least made public) on the terrorist threat to the United States was in 2007, suggesting that a new assessment is overdue. Such an assessment

---


43 Recent studies that take such a broad approach, and might serve as models for a homeland security net assessment, include Bruce Hoffman, “A First Draft of the History of America’s Ongoing Wars on Terrorism,” _Studies in Conflict and Terrorism_, accepted author version posted online October 14, 2014; and Bipartisan Policy Center, 2014: Jihadist Terrorism and Other Unconventional Threats, September 2014.
might reflect the conventional view among terrorism experts that al Qaeda has been weakened in recent years, largely as a result of the counterterrorism efforts that have been undertaken by the United States and its allies since 2001. A recent report by the Bipartisan Policy Center describes some of these improved capabilities:

For example, on 9/11, there were 16 people on the U.S. “no fly” list. Today, there are more than 40,000. In 2001, there were 32 Joint Terrorism Task Force “fusion centers,” where multiple law enforcement agencies work together to chase down leads and build terrorism cases. Now there are 103. A decade ago, the U.S. Department of Homeland Security, National Counterterrorism Center, Transportation Security Administration, Northern Command, and Cyber Command didn’t exist. In 2014, all of these new post-9/11 institutions make it much harder for terrorists to operate in the United States.44

But despite the decline in the threat from al Qaeda, the threat from a broader range of groups and individuals is widely considered to be greater today than it was in the immediate post-9/11 period. An assessment will need to consider the rising threat from lone wolf terrorists and other homegrown extremists. As DHS Secretary Johnson has said, “This is the type of threat that may be hardest to detect. It involves independent actors potentially living in the United States, which easy access to items that, in the wrong hands, can become tools for mass violence.”45 A net assessment would need to examine the quantitative data that is available on such threats. The New America Foundation, for example, has found that homegrown jihadist extremists have killed 26 people since 9/11, while non-jihadist extremists have killed 38.46 But the assessment would also have to wrestle with more difficult questions about how to measure and compare different kinds of threats facing the nation. For example, during the same week in which the Boston Marathon bombings killed three people, a fertilizer plant in West, Texas, exploded, killing 14. The Boston bombings received much more media attention, but a net assessment might consider whether the risk from industrial accidents or other kinds of disasters represent a greater homeland security threat than terrorism.

A net assessment would closely examine the legitimacy of American counter-terrorism capabilities. One of the most important—and most controversial—of these capabilities is the use of unmanned drone strikes. These strikes, which often result in civilian casualties, are seen by

44 Bipartisan Policy Center, 2014: Jihadist Terrorism and Other Unconventional Threats, 9.
many critics of American policy as illegitimate. The rules governing drone use are only now being developed, and the Bipartisan Policy Center writes that “The choices the United States makes regarding its use of drones for targeting killing operations and the rules that regulate such operations will shape the global environment in the coming decades.”

Some of the most important changes in counter-terrorism capabilities have been improvements in domestic intelligence, at the federal as well as the state and local level. As Brian Jenkins notes, homeland security intelligence is likely to become even more important in the coming years: “Domestic intelligence collection is essential, especially as al Qaeda places more emphasis on inspiring local volunteers to take action.” And the intelligence gathered to detect such threats will almost inevitably need to sweep up information on American citizens who are not themselves threats. Gregory Treverton writes that “Today, it’s not enough to know about them; intelligence can’t understand them without knowing a lot about ‘us.’”

America’s current domestic intelligence structure encompasses a complex system that includes counterterrorism organizations led by the NCTC; other federal-level organizations and efforts, including those within the FBI, DHS, and Department of Defense; and state, local, and private sector activities. One of the most important developments as been the establishment of a network of 78 state and local intelligence fusion centers, which typically receive DHS funding and support but are under local control. These fusion centers are not widely known, but they have had some notable successes in helping to prevent terrorist attacks and assisting law enforcement agencies in capturing criminals. They have also generated controversy. A Senate committee report found that fusion centers “often produced irrelevant, useless or inappropriate intelligence reporting to DHS, and many produced no intelligence reporting whatsoever.” A RAND study examined fusion centers and the FBI-led Joint Terrorism Task Forces, and reported that “What we found was organized chaos: a federally subsidized, loosely coordinated system for

---

47 Bipartisan Policy Center, 2014: Jihadist Terrorism and Other Unconventional Threats, 47.
50 The Colorado Information and Analysis Center (CIAC), for example, was recognized as the Fusion Center of the Year in February 2010 for its support to the Najibullah Zazi terrorism investigation, and more recently it provided information that helped lead to the arrest of a bombing suspect; see “Fusion Centers: Empowering State and Local Partners to Address Homeland Security Issues,” DHS blog July 18, 2011, http://blog.dhs.gov/2011/07/fusion-centers-empowering-state-and.html.
sharing information that is collected according to varying local standards with insufficient quality control, accountability, or oversight.”

A homeland security net assessment might argue that in evaluating domestic intelligence programs, we should follow the same standard that the U.S. Food and Drug Administration does in determining whether drugs can be marketed: they need to be both safe and effective. For counter-terrorism intelligence programs this would mean that a program needs to be both effective in preventing terrorist attacks, and sufficiently safe for civil liberties and personal freedoms to be judged legitimate and worthwhile. Some of the most controversial American counter-terrorism capabilities—such as the National Security Agency’s bulk data collection programs that were revealed by Edward Snowden—may not pass this test. Not only is the legitimacy of these programs in question, but there is considerable debate over whether they are effective in preventing terrorism. Intelligence community leaders have claimed that these programs are necessary for national security, but two official studies, by the President’s Review Group and the Privacy and Civil Liberties Oversight Board, argued that one program, at least—the collection of American phone data—had not been useful. Outside researchers have also found that bulk collection of phone data has not prevented a single terrorist attack.

**Cyber**

Estimates of the threat from cyber terrorism range from the extremely dire to the moderately sanguine. Some scholars and computer security experts argue that the nation faces the threat of a “cyber Pearl Harbor,” while others claim that threats of cyberwar are little more than a myth. Former Secretary of Homeland Security Janet Napolitano warned that a “cyber 9/11” could happen “imminently.” But on the other hand, a classified national intelligence assessment in 2013 was reported to conclude that cyber-espionage, most notably from China, represented a greater threat to the nation’s security than cyber terrorism.

---

A net assessment could be especially useful in helping to advance the debate over the different kinds of cyber threats facing the nation. The Bipartisan Policy Center recently argued that:

Overall, the cybersecurity debate has matured but does not yet sufficiently distinguish among the various threats. The next step must be a more nuanced approach to address this problem and a more careful use of terms—especially ‘cyber attack,’ ‘cyber war,’ and ‘cyberterrorism.’58

A net assessment, taking a long-term view and making use of available data on specific cyber threats, would likely note that as Colin Gray has written, “despite the acute shortage of careful strategic thought on the subject, and notwithstanding the ‘Cybergeddon’ catastrophe scenarios that sell media products, it is clear enough today that the sky is not falling because of cyber peril.”59 It seems likely that a net assessment would adopt the relatively cautious approach taken by terrorism expert Martha Crenshaw, who notes that the most disruptive cyber attacks, such as the Stuxnet virus used against Iranian centrifuges, have been the work of sophisticated state actors, and not terrorist groups or individuals.60

Just as the debate over the cyber threat is relatively new and under-developed, the discussion of cyber capabilities is also at a fairly undeveloped stage. The U.S. military has established a Cyber Command, which is under the command of the NSA director. Some critics worry that the U.S. may be combining too much military and civilian authority into one organization; Peter Singer of the Brookings Institution said that “the mashing together of the NSA and Cyber Command has blurred the lines between a military command and a national spy agency.”61 But other critics argue that more needs to be done, such as the creation of a U.S. Cyber Force that would operate alongside the existing military services.62 Richard Clarke, who has been an outspoken advocate for concern about cyber threats, argues that the United States needs urgently to develop greater cyber defense capabilities: “If anything is clear, it is that we have a remarkably well-developed offensive capability, but no commensurately serious

58 Bipartisan Policy center, 2014: Jihadist Terrorism and Other Unconventional Threats, 43.
59 Colin S. Gray, Making Strategic Sense of Cyber Power: Why the Sky is Not Falling (U.S. Army War College Strategic Studies Institute, 2013), xi.
commitment to defense. There is neither a plan nor any capability to defend America’s civilian infrastructure, from banking to telecoms to aviation.”

A net assessment of America’s cyber security would likely conclude that more work needs to be done on gauging the effect of increased cyber capabilities on civil liberties. As a National Research Council report noted, effective programs to deter viruses and other malware from Internet traffic may require that traffic to be inspected by a third party, which raises important privacy issues. And from a homeland security perspective, one of the weaker areas of public policy may be at the level of state and local authorities. It appears that the most significant cyber capabilities exist either at the level of the federal government, where most policies originate, or in the private sector, where most research and development is conducted. Some significant state and local efforts are underway, but more needs to be done, and a homeland security net assessment could help to suggest areas of focus below the federal level.

Natural hazards

The disasters of Hurricane Katrina and Superstorm Sandy served to ensure that the threats from natural hazards remain near the top of the list of homeland security concerns facing the nation. According to the Quadrennial Homeland Security Review, “Natural disasters, pandemics, and the trends associated with climate change continue to present a major area of homeland security risk.” The greatest natural hazard risk, the review argues, is of a devastating pandemic, and the recent Ebola outbreak certainly supports that view. But the threat remains high from other kinds of natural disasters, including hurricanes, earthquakes, droughts, and floods, with DHS noting that the risk is increasing as the nation’s infrastructure ages, and as climate change may act as a “threat multiplier.”

A homeland security net assessment would weigh such threats against the capabilities that have been developed to prepare for and respond to them. The Department of Homeland

64 David Clark, Thomas Berson, and Herbert S. Lin, eds., At the Nexus of Cybersecurity and Public Policy: Some Basic Concepts and Issues (National Research Council, 2014), 100.
65 For example, a Joint Action Plan for State-Federal Unity of Effort on Cybersecurity was approved by the National Governors Association in July 2014.
Security argues that the nation’s capability to respond to natural hazards and disasters has improved significantly since Katrina:

Acting on the lessons of Hurricane Katrina, we have improved disaster planning with federal, state, local, tribal, and territorial governments, as well as nongovernmental organizations and the private sector; pre-positioned a greater number of resources; and strengthened the Nation’s ability to respond to disasters in a quick and robust fashion. Seven years after Katrina, the return on these investments showed in the strong, coordinated response to Hurricane Sandy.  

The U.S. government has developed a sophisticated national preparedness system, including a National Preparedness Goal that sets out 31 core national capabilities and a National Preparedness Report that summarizes the progress made in achieving those core capabilities. Most experts agree that the nation is better prepared for disasters than it has been in the past. But an area where more work needs to be done, and where a net assessment could be particularly useful, is in determining how effective these preparedness capabilities really are. The Government Accountability Office found that “DHS and FEMA have implemented a number of efforts with the goal of measuring preparedness by assessing capabilities and addressing related challenges, but success has been limited.”

A number of scholars and homeland security practitioners have been warning in recent years about the danger from what Paul Stockton, former Assistant Secretary of Defense for Homeland Defense and Americas’ Security Affairs, calls “catastrophes more severe than Hurricane Katrina.” Such disasters are sometimes called complex catastrophes, “black swans,” or “wicked problems,” and they appear to be increasing in frequency and seriousness. An example that is often cited of such a potential catastrophe is an earthquake along the New Madrid fault, near the town of New Madrid, Missouri. An estimated magnitude 7.7 earthquake struck that region in 1812, killing few people in what was then an under-populated area, but causing tremendous shocks that collapsed the banks of the Mississippi River and liquefied the ground.

---

Experts estimate that 86,000 people could be killed if a similar earthquake hit that area today.74 FEMA conducted a National Level Exercise in 2011 that focused on the New Madrid threat, and a homeland security net assessment would be able to examine this type of high-impact but low-probability event.

Conclusion

This very preliminary review suggests that in the area of terrorism, there is currently a favorable—but tenuous—balance of threat and homeland security capabilities, which has thus far succeeded in keeping America safer than most experts would have predicted after the 9/11 attacks. America’s global counterterrorism efforts and domestic law enforcement and intelligence systems appear to have been successful in increasing security within the United States, as demonstrated by numerous foiled terrorist plots and the lack of another major successful attack on American soil since 9/11.

But these gains have come at the cost of increasing domestic surveillance and at the risk to civil liberties. By its very nature, domestic and homeland security intelligence is intrusive and risks infringing on civil liberties. As then-Secretary of Homeland Security Michael Chertoff put it:

> Intelligence, as you know, is not only about spies and satellites. Intelligence is about the thousands and thousands of routine, everyday observations and activities. Surveillances, interactions – each of which may be taken in isolation as not a particularly meaningful piece of information, but when fused together, gives us a sense of the patterns and the flow that really is at the core of what intelligence analysis is really about.75

These thousands and thousands of observations are largely observations about people and events in America, and in the years since 9/11 the United States has created a domestic intelligence system to collect them. In some cases the people are terrorists or other types of criminals, and the intelligence collected has helped to prevent bad events from happening. But in many cases these observations, this intelligence, is about routine activities undertaken by ordinary Americans and others who do not intend to cause harm. A net assessment would examine whether these...

---

intelligence and counter-terrorism capabilities are both “safe and effective,” and whether they are sufficiently legitimate today, or whether they should be reexamined.

A net assessment would also be valuable in expanding the discussion of homeland security threats beyond terrorism. By looking at the balance between threat, capability, and legitimacy, it would likely suggest that more attention needs to be paid to the impact of increased cyber capabilities on civil liberties, and on the need for greater cyber defense capabilities at the state and local level. It also might highlight the need to develop better tools for measuring the nation’s preparedness efforts to deal with natural disasters, and with the potentially greater threat of complex catastrophes.

A final important step would be to look farther into the future, as net assessment analysts in the Pentagon did during the Cold War. Paul Bracken notes that thinkers using the concept of net assessment were able to identify the importance of Asia as an area of strategic concern and competition as early as the 1980s, despite the fact that the only immediate problem of Asian security at that time was Korea.76 The comparable question for today might be: what are the rising threats and concerns for homeland security, not simply for the next few years, but for the next several decades?

In recent years we have seen a few, mostly tentative calls for the use of the tools of net assessment in determining and weighing the threats to America’s homeland security. But as we continue to face an increasing variety of challenges in an era of decreasing budgets and government retrenchment, these tools may be more useful than ever. As a first step, the Department of Homeland Security should establish an Office of Net Assessment and direct it to conduct a broad-based study of the threats from terrorism, cyber, and natural hazards.