STRATEGIC STUDIES QUARTERLY

A Homeland Security Net Assessment Needed Now!

Erik J. Dahl

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. However, 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 article argues that a homeland security net assessment is even more necessary today, since debates over the state of the nation's security involve discussions not only about the seriousness of the threat but also the legitimacy of the intelligence and other efforts 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.

✳ ✳ ✳ ✳ ✳

The concept of net assessment has long been considered an important tool for American national-security strategists, but this tool is largely unavailable in the effort to analyze threats and strategies in the areas of homeland security and homeland defense. The Pentagon's Office of Net Assessment (ONA) is famous within the American national-security

Erik Dahl is an associate professor of national security affairs at the Naval Postgraduate School and serves on the faculty of the Center for Homeland Defense and Security. He is the author of *Intelligence and Surprise Attack: Failure and Success from Pearl Harbor to 9/11 and Beyond* (Georgetown University Press, 2013). A retired Naval intelligence officer, Dahl received his PhD from the Fletcher School of Tufts University and holds master's degrees from the Fletcher School, the Naval War College, and the London School of Economics.

establishment for its influence in security planning, but many critical homeland security threats are outside its scope. Additionally, there is no equivalent net assessment office within the DHS. Despite calls by experts for the development of such a capability within the DHS, only a few tentative efforts have been made to use the concepts and methodologies of net assessment for ensuring US homeland security. A comprehensive homeland security net assessment must involve more than a detailed understanding of external threats. Traditionally, national-security net assessments focus on two key factors: the enemy and one's own forces. To develop a homeland security net assessment, it is more critical to understand our own actions and capabilities, because those actions are focused within America's borders. In the areas of homeland security and defense, more than in traditional national security, governmental actions are likely to have a direct effect on the American people and society. For this reason, a homeland security net assessment must focus not only on the threat but also on our own capabilities to counter that threat.

Debates over the state of the nation's security involve discussions not only about the seriousness of threats from terrorism and other sources but also consideration of the legitimacy of the intelligence and other counterterrorism capabilities being employed to combat those threats. Of particular interest is the effect domestic intelligence programs have on civil liberties and domestic society. Other studies have examined the potential organizational structure of a DHS office of net assessment, so that is not the focus here.[1] Instead, the article proposes a framework for thinking about the task of a homeland security net assessment and suggests a new model for the process that should be undertaken by the DHS in assessing the key threats to the US homeland, which are terrorism, cyber, and natural hazards like disasters and infectious disease. It begins by reviewing the concept of net assessment and how it has been used in the US Department of Defense (DOD). Next it examines proposals for the DHS to establish an office of net assessment following the DOD model and then posits how the process of net assessment should be modified for the problem of homeland security, using a new model that could be adopted by the DHS. The final section offers preliminary suggestions and implications from such a homeland security net assessment process.

What Is Net Assessment?

The concept of net assessment arose during the Cold War, when the United States realized that 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 US capabilities, could not be sure they were privy to the best (and often most-highly classified) intelligence information on the enemy against whom they were planning. Additionally, 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, until recently, director of the DOD's ONA.[2] Marshall and his office became famous among strategic thinkers, and several think tanks and analysts have adopted the net-assessment idea. A few scholars have suggested that net assessments should become more widely used today, but the concept remains relatively little known outside defense circles.[3]

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."[4] 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."[5] 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."[6] 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—it can be anything but."[7]

Although the net-assessment approach has been used most notably by the Pentagon, it does not focus only on military factors. The DOD

defines net assessment as "the comparative analysis of military, technological, political, economic, and other factors governing the relative military capability of nations. Its purpose is to identify problems and opportunities that deserve the attention of senior defense officials."[8] Most advocates of net assessment see it as a broad-based, interdisciplinary approach, taking into account not only military matters but also economic, political, technological, and social factors.

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. 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. The focus is on the long term, identifying long-term trends and looking beyond the typical US government perspective that is often shaped by the length of a presidential administration.[9] As Aaron Friedberg notes, "Trends are important because the past will always shape, even if it does not completely determine, the future."[10] 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."[11] In fact, this long-term view may be one reason why the Pentagon's ONA has been seen as successful. It can be hard to criticize assessments about a future that is decades away.

Another key aspect of the Pentagon's net-assessment approach—and another likely reason why it has been supported through so many administrations—is that it does not produce specific policy recommendations. As one critic has put it, "It could be the case that Marshall's approach has survived precisely because it is so oracular and nebulous."[12] Marshall himself 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."[13] 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."[14]

It is often said that the Pentagon's ONA has encouraged pessimistic thinking and worst-case scenarios. During the late years of the Cold

War, for example, Cohen argued that a net-assessment approach helped to demonstrate the weakness in the analysis of some authors and scholars who he called optimists, who believed that the conventional military balance in Europe at the time favored the North Atlantic Treaty Organization rather than the Warsaw Pact.[15] More recently, one critic has called the ONA "a full-time office of threat inflation,"[16] and some have charged that Marshall and the 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."[17]

Recently the occasion of Marshall's retirement and the publication of a highly favorable book about him by two former colleagues have generated a small flurry of articles assessing his legacy. Supporters, such as Andrew Krepinevich and Barry Watts, laud him as "an intellectual giant comparable to such nuclear strategists as Bernard Brodie, Herman Kahn, Henry Kissinger, James Schlesinger, and Albert Wohlstetter."[18] He has been praised for being one of the first to understand the importance of what became known as the "revolution in military affairs" and for warning about the rise of China long before the current administration's pivot to Asia.[19] Critics, on the other hand, argue he was far from all-knowing—having missed the increasing threat of terrorism prior to the 9/11 attacks. Critics also contend that, because most of the products of the ONA are classified, it is difficult to objectively assess the value of its work.[20]

The debate over Andrew Marshall's legacy will undoubtedly continue.[21] However, the continuing value of the net-assessment approach seems clear, especially in areas of homeland security and defense, where it is especially important to match our understanding of external threats with a clear-eyed assessment of our own internal capabilities.

The DHS and Net Assessment

There is no central office or organization in the US 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 US government for conducting net assessments of terrorist threats.[22] However, its work appears to be mostly classified. Therefore, it is not known whether it con-

ducts regular net assessments, and if it does, whether those assessments are useful to policy makers. Some elements of the DHS, such as the Domestic Nuclear Detection Office (DNDO), do appear to conduct net assessments. That office has as one of its functions the mission of performing red team and net assessments.[23] However, many observers have argued that the DHS should make greater use of net assessments and should establish a net assessment office similar to the Pentagon's ONA.

In 2007, for example, the Homeland Security Advisory Council issued a report calling on the 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."[24] That same year a report by the Heritage Foundation argued that the 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."[25] A strong advocate of establishing a net-assessment capability within the DHS has been Frank J. Cilluffo, the associate vice president and director of the Center for Cyber and Homeland Security at The George Washington University. Cilluffo argues that the 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.[26]

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."[27] Such a net assessment was reportedly conducted, but it has not been publicly released.[28]

Patrick Forrest and Alex Hilliker argue that because homeland threats and challenges such as public safety, emergency management, and law enforcement are largely outside the scope of the DOD, the existing ONA in the Pentagon is insufficient to deal with such important matters. Instead, they argue, a new office of net assessment is needed within the DHS 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. 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. Furthermore, they suggest that a relatively small, independent office reporting directly to the Secretary of Homeland Security be established, the focus of which "would be solely on producing assessments intended to increase the leadership's situational awareness regarding future challenges to the homeland security enterprise."[29]

A New Net-Assessment Model for Homeland Security

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. Testifying before the Senate, Director of National Intelligence James Clapper stated, "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."[30] Gen Martin Dempsey, the chairman of the Joint Chiefs of Staff, testified, "I will personally attest to the fact that it [the world] is more dangerous than it has ever been."[31] Some critics have charged that such dire warnings are exaggerations, and Secretary of Homeland Security Jeh Johnson has not taken quite such a pessimistic view.[32] However, 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."[33]

What threats should be part of a homeland security net assessment? Clearly, one focus would be on the terrorist threat to the United States. Secretary Johnson has said, "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 at-

tacks."[34] A focus on terrorism suggests that a homeland security net assessment should compare the threat from specific groups or actors, such as al-Qaeda or the Islamic State in Iraq and the Levant (ISIL), with the counterterrorism capabilities available to 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 US counterterrorism capabilities.[35]

Even though terrorism might be considered "job one" for homeland security, it is neither the only threat nor the only mission for the homeland security enterprise.[36] *The 2014 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 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.

Few observers would be surprised by the inclusion of terrorism and cyber threats on this list, but some, especially those within the DOD, might wonder why natural hazards should be considered a key homeland security problem. After all, the mission of providing military support to civil authorities following a natural disaster or other emergency is typically considered a secondary one for military planners. However, for homeland security planners and practitioners, disasters and other types of natural hazards are a primary mission—and a mission that has been growing in recent years, following disasters such as Hurricane Katrina, super storm Sandy, and occurrences of other natural threats such as the outbreak of infectious disease. The Obama administration has acknowledged the link between natural hazards and national security. In the 2015 *National Security Strategy* the White House noted that ensuring national security means "reinforcing our homeland security to keep the American people safe from terrorist attacks and natural hazards while strengthening our national resilience."[38]

However, there is more to a net assessment than an examination of the threat. It 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. Political scientist 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."[39] The adversary may not be far away in a distant land but instead can be here in the middle of the 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 US borders, they must also 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 Cohen described it, 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 effects of our policies on the American people might be captured in the concept of *legitimacy*: are the capabilities 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 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.[40] 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.[41]

A similar homeland security trinity may be helpful in understanding the forces that must be understood to conduct a homeland security net assessment. This trinity involves the *threats*, *capabilities*, and *legitimacy* involved in homeland security.[42] Thus, our proposed homeland security net assessment process 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 to counter the threat, and whether those capabilities are seen by the American 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 Preliminary Homeland Security Net Assessment

Although the Pentagon's ONA 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 in between the pessimistic studies often produced by outside critics of whichever administration is in power and the considerably more optimistic reports typically issued from government agencies when they attempt to assess their own accomplishments. The following are some of the issues and problems a homeland security net assessment could help illuminate.

Terrorism

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 Federal Bureau of Investigation (FBI), the DHS, and the DOD; and state, local, and private-sector activities. Despite the development of these counterterrorism organizations and capabilities, many experts argue much more remains to be done, especially in terms of coordinating federal efforts with those of state, local, and private entities. A recent report by a panel of experienced practitioners and scholars argues that, "The United States still lacks a cohesive domestic counterterrorism strategy with the capacity for coordinated execution at all levels of government."[43] Even though

the threat from al-Qaeda has declined, the overall terrorist threat today remains high, with a broad range of groups and individuals continuing to pose significant threats to American lives at home and abroad. Some experts believe the terrorist threat is greater today than it was in the immediate post-9/11 period, but the growing consensus is that while the threat of another catastrophic attack appears reduced, there remains a continuing threat of smaller-scale plots and attacks from al-Qaeda affiliates and homegrown extremists.[44]

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. It must also 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 ISIL.[45] The last *National Intelligence Estimate* 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 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.[46]

An assessment will also need to consider the rising threat from lone-wolf terrorists and other homegrown extremists. It could examine the quantitative data that is available on such threats. As 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, with easy access to items that, in the wrong hands, can become tools for mass violence."[47] 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 39.[48] However, 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 exploded in West, Texas, killing 14. The Boston bombings received much more media attention, but a net assessment might consider whether the risks from industrial accidents or other kinds of disasters represent a greater homeland security threat than terrorism. 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 United States 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."[49] That statistic is likely to come as a surprise to most Americans, and one task for a net assessment would be to determine how significant such historical comparisons are for today.

One of the most important developments has 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.[50] 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."[51] A RAND study examined fusion centers and the FBI-led Joint Terrorism Task Forces and reported, "What we found was organized chaos: a federally subsidized, loosely coordinated system for sharing information that is collected according to varying local standards with insufficient quality control, accountability, or oversight."[52] However, other experts and studies have argued that state and local fusion centers are a vital part of the homeland security enterprise, and a net assessment would be useful in asking questions such as, is 78 the right number of these centers?[53]

Some of the most important changes in counterterrorism capabilities have been improvements in domestic intelligence at the federal, state, and local levels. 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."[54] Additionally, 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, "Today, it's not enough to

know about them; intelligence can't understand them without knowing a lot about 'us.'"[55] A homeland security net assessment might argue that in evaluating domestic intelligence programs, we should follow the same standard as the US Food and Drug Administration in determining whether drugs can be marketed: they need to be both safe and effective. This would mean that for counterterrorism intelligence programs to be judged legitimate and worthwhile, a program needs to be both effective in preventing terrorist attacks and sufficiently safe for civil liberties and personal freedoms.

Some of the most controversial American counterterrorism capabilities—such as the National Security Agency's (NSA) 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 also there is considerable debate over whether they are effective in preventing terrorism. Intelligence community leaders have claimed 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 at least one program—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.[56] The most effective domestic counterterrorism tools have been traditional law enforcement techniques such as the use of undercover officers and informants and close engagement with the local community to encourage tips from the public and from family members of those who might be at risk of radicalization.[57]

Finally, a net assessment would closely examine the legitimacy of American counterterrorism capabilities. One of the most important—and most controversial—of these capabilities is the use of unmanned drone strikes. Many critics of American policy view these strikes—often resulting in civilian casualties, including recently two hostages held by al-Qaeda—as illegitimate.[58] The rules governing drone use are not well understood by the public, and as the Bipartisan Policy Center writes, "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."[59]

Cyber

Estimates of the threat from cyberterrorism 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,"[60] while others claim threats of cyberwar are little more than a myth.[61] Former Secretary of Homeland Security Janet Napolitano warned that a "cyber 9/11" could happen "imminently."[62] On the other hand, a classified national intelligence assessment in 2013 concluded that cyberespionage, most notably from China, represented a greater threat to the nation's security than cyberterrorism.[63] And in his latest testimony to Congress, Director Clapper said the likelihood of a catastrophic "Cyber Armageddon" is remote.[64]

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 a different approach is needed: "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.'"[65]

A net assessment, taking a long-term view and making use of available data on specific cyber threats, would likely conclude, 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."[66] 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—not terrorist groups or individuals.[67]

Just as the debate over the cyber threat is relatively new and underdeveloped, the discussion of cyber capabilities is also at a fairly undeveloped stage. The US military has established a Cyber Command (USCYBERCOM), as a four-star subunified command under the US Strategic Command, with the mission of directing DOD cyber operations and defending military information networks. The commander of USCYBERCOM also serves as director of the NSA, an intelligence organization that provides support to military and national customers, including USCYBERCOM.[68] Some critics worry the United States may

be combining too much military and civilian authority into one organization. Peter Singer of the Brookings Institution said, "The mashing together of the NSA and Cyber Command has blurred the lines between a military command and a national spy agency."[69] Other critics argue more needs to be done, such as creating a US Cyber Force that would operate alongside the existing military services.[70] Richard Clarke, who has been an outspoken advocate for concern about cyber threats, argues the United States needs to urgently develop greater cyber-defense capabilities: "If anything is clear, it is that we have a remarkably well-developed offensive capability, but no commensurately serious commitment to defense. There is neither a plan nor any capability to defend America's civilian infrastructure, from banking to telecoms to aviation."[71]

In recent years it seems as if just about everybody in the national security and intelligence communities has jumped on the cyber bandwagon, with other new cyber organizations including the Cyber Threat Intelligence Integration Center under the director of national intelligence, a new cyber directorate at the Central Intelligence Agency, and the National Cybersecurity and Communications Integration Center under the DHS. However, it is not clear if we have determined the proper "lanes in the road" for these different organizations. The history of the DHS suggests that once major organizational reforms have been made in government, it can be difficult to change course. The DHS often ranks low on surveys of federal government-employee satisfaction and is often criticized for being too big to manage effectively. Although it has undergone several reorganizations since it was first established, it is still largely as it was originally designed. The force of path dependence is strong in government organizations, and a homeland security net assessment would help us realize that the cybersecurity organizations we are establishing today are likely to be around for many years. It is important to think carefully from the beginning about how to deconflict responsibilities and avoid creating stovepipes.

Because cyber issues directly affect virtually all Americans, it is particularly important that a broad net assessment perspective, acknowledging the concerns of stakeholders beyond the traditional national security establishment, inform cyber strategies. The Pentagon understands that the problem of cybersecurity cannot be addressed by military personnel alone and is planning to create a "surge force" of

private-sector and National Guard cyber experts who could be called upon to help protect critical infrastructure sectors in case of a national cyber emergency.[72] Eric Rosenbach, the assistant secretary of defense for homeland defense and global security, has said the DOD is committed to a whole-of-government approach to cybersecurity, including close coordination with other federal agencies, state and local governments, and the private sector.[73] As Adm Michael Rogers, commander of USCYBERCOM and director of NSA, puts it, "Neither the U.S. government, the states, nor the private sector can defend their information systems on their own against the most powerful cyber forces. The public and private sectors need one another's help."[74]

A net assessment of America's cybersecurity would likely conclude that more work needs to be done to gauge 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 the traffic to be inspected by a third party, which raises important privacy issues.[75] Additionally, 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 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 must be done, and a homeland security net assessment could help suggest areas of focus below the federal level.[76]

Natural Hazards

The disasters of Hurricane Katrina and super storm Sandy ensured that 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."[77] The greatest natural-hazard risk, the review argues, is of a devastating pandemic, and the 2014 Ebola outbreak in West Africa provides support for that view.[78] However, the threat remains high from other kinds of natural disasters, including hurricanes, earthquakes, droughts, and floods, with the DHS noting the increasing risk as the nation's infrastructure ages and as climate change may act as a "threat multiplier."[79]

A homeland security net assessment would weigh such threats against the capabilities that have been developed to prepare for and respond to them. The DHS 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."[80]

The US 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.[81] Most experts agree the nation is better prepared for disasters than it has been in the past.[82] However, 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 [Federal Emergency Management Agency] have implemented a number of efforts with the goal of measuring preparedness by assessing capabilities and addressing related challenges, but success has been limited."[83]

A number of scholars and homeland security practitioners have warned in recent years about the danger of what Paul Stockton, former assistant secretary of defense for homeland defense and Americas' security affairs, calls "catastrophes more severe than Hurricane Katrina."[84] Such disasters are sometimes called complex catastrophes, "black swans," or "wicked problems," and they appear to be increasing in frequency and seriousness.[85] 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 underpopulated 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 hits that area today.[86] FEMA conducted a National Level Exercise in 2011 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.

Although it might not seem obvious that legitimacy is an important factor in ensuring homeland security against natural hazards, public acceptance of and support for government efforts may be more important in this area than any other. This is because local, public, and private-sector involvement is critically important in preparing for and responding to natural hazards and disasters. The DHS Strategic Plan argues that a "whole community approach" is necessary "to build the capacity of American society to be resilient in the face of disruptions, disasters, and other crises."[87] A homeland security net assessment would evaluate how successful the DHS has been in engaging the American public and other stakeholders in the effort to prepare for natural hazards and catastrophes.

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 that 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.

However, these gains have come at the cost of increasing domestic surveillance and at the risk of infringing upon civil liberties. By its very nature, domestic and homeland security intelligence is intrusive and risks impinging 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."[88]

These thousands of observations are largely 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. However, in many cases these observations—this domestic intelligence—is about routine activities undertaken by ordinary Americans and others who do not intend to cause harm.[89] A net assessment would examine whether these intelligence and counterterrorism capabilities are "safe and effective" and whether they are sufficiently legitimate or if they should be reexamined.

A net assessment would also be valuable in expanding the discussion of homeland security threats beyond terrorism. Looking at the balance among threat, capability, and legitimacy suggests more attention must be devoted to the impact of increased cyber capabilities on civil liberties and on the need for greater cyber-defense capabilities at the state and local levels. 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. Additionally, whenever possible, the products of such net assessments should be made unclassified and widely available. This is the right thing to do, because Americans deserve to know as much as can reasonably be shared about the actions their government is taking. It is also the strategic thing to do, because homeland security efforts are most effective when they are supported and trusted by the people they serve.

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.[90] The comparable question for today might revolve around what the rising threats and concerns for homeland security are not simply for the next few years but also for the next several decades.

In recent years we have seen a few, mostly tentative calls for the use of net assessment tools in determining and weighing the threats to America's homeland security. However, 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 DHS 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. SSQ

Notes

1. For example, Patrick Forrest and Alex Hilliker, "Why the Department of Homeland Security Needs an Office of Net Assessment," *Risk, Hazards & Crisis in Public Policy* 3, no. 3 (September 2012): 1–18.

2. Mie Augier, "Thinking about War and Peace: Andrew Marshall and the Early Development of the Intellectual Foundations for Net Assessment," *Comparative Strategy* 32, no. 1 (January–March 2013): 1–17. For useful background on the history of the Office of Net Assessment (ONA) see Thomas M. Skypek, "Evaluating Military Balances through the Lens of Net Assessment: History and Application," *Journal of Military and Strategic Studies* 12, no. 2 (Winter 2010): 1–25, and Phillip A. Karber, "Net Assessment and Strategy Development for the Secretary of Defense: Future Implications from Early Formulations" (faculty paper, Georgetown University Institute of International Law and Politics, 15 August 2008), https://georgetown.box.com/s/9s11fgxsokczslxuccq5. Marshall retired in January 2015. Not surprisingly, given his low public profile, the event attracted little fanfare. For a succinct examination of his impact on Washington see "The Quiet American," *Economist*, 10 January 2015, http://www.economist.com/news/united-states/21638157-enigmatic-futurist-last-calls-it-quits-quiet-american.

3. Examples of recently produced net assessments include Peter Chalk, Angel Rabasa, William Rosenau, and Leanne Piggott, *The Evolving Terrorist Threat to Southeast Asia: A Net Assessment* (Santa Monica, CA: RAND, 2009); Mark Fitzpatrick, ed., *North Korean Security Challenges: A Net Assessment* (London: International Institute for Strategic Studies, July 2011); Michael D. Swaine, et al., *China's Military & the U.S.-Japan Alliance in 2030: A Strategic Net Assessment* (Carnegie Endowment for International Peace, 2013); and Michael D. Swaine, Mike M. Mochizuki, Michael L. Brown, Paul S. Giarra, Douglas H. Paal, Rachel Esplin Odell, Raymond Lu, Oliver Palmer, and Xu Ren, *Conflict and Cooperation in the Asia-Pacific Region: A Strategic Net Assessment* (Washington, DC: Carnegie Endowment for International Peace, 2015). For a discussion of a revival in interest in net assessment today, see Yee-Kuang Heng, "The Return of Net Assessment," *Survival* 49 no. 4 (Winter 2007–2008): 135–52.

4. Andrew W. Marshall, "National Net Assessment," memorandum for the record, 10 April 1973, 2. Available from the Digital National Security Archive, file no. 01198.

5. Eliot A. Cohen, *Net Assessment: An American Approach*, Jaffee Center for Strategic Studies Memorandum no. 29 (Tel Aviv: Jaffee Center for Strategic Studies, April 1990), 4.

6. Sun Tzu, "The Art of War," in *Strategic Studies: A Reader,* edited by Thomas G. Mahnken and Joseph A. Maiolo (New York: Routledge, 2008), 64.

7. Swaine, et al., *China's Military & the U.S.-Japan Alliance in 2030*, 8.

8. Department of Defense Directive 5111.11, *Director of Net Assessment*, 23 December 2009, 1.

9. Cohen, *Net Assessment*, 14–15.

10. Aaron L. Friedberg, "The Assessment of Military Power: A Review Essay," *International Security* 12, no. 3 (Winter 1987–1988), 193.

11. Paul Bracken, "Net Assessment: A Practical Guide," *Parameters* 36, no. 1 (Spring 2006), 94.

12. Michael C. Desch, "Don't Worship at the Altar of Andrew Marshall," *National Interest*, January–February 2015, http://nationalinterest.org/feature/the-church-st-andy-11867.

13. Marshall, "National Net Assessment," 1. It is worth noting that while Marshall prefers not to recommend policy options, he does believe it important for the net-assessment process to provide decision makers with *opportunities*. The difference between opportunities and policies may be a fine one, but it appears to have been enough to be useful to Marshall in defusing bureaucratic opposition toward his office.

14. Augier, "Thinking about War and Peace," 12.

15. Eliot A. Cohen, "Toward Better Net Assessment: Rethinking the European Conventional Balance," *International Security* 13, no. 1 (Summer 1988): 50–89. See also the exchange between Cohen and his critics in "Reassessing Net Assessment," *International Security* 13, no. 4 (Spring 1989): 128–79.

16. Jeffrey Lewis, "Yoda Has Left the Building," *Foreignpolicy.com*, 24 October 2014, http://www.foreignpolicy.com/articles/2014/10/24/yoda_has_left_the_building_andrew_marshall_pentagon_futurist.

17. Greg Jaffe, "U.S. Model for a Future War Fans Tensions with China and inside Pentagon," *Washington Post*, 1 August 2012, https://www.washingtonpost.com/world/national-security/us-model-for-a-future-war-fans-tensions-with-china-and-inside-pentagon/.

18. Andrew F. Krepinevich and Barry D. Watts, *The Last Warrior: Andrew Marshall and the Shaping of Modern American Defense Strategy* (New York: Basic Books, 2015), xviii.

19. For example, Douglas J. Feith, "The Hidden Hand behind American Foreign Policy," *Wall Street Journal*, 23 January 2015, http://www.wsj.com/articles/book-review-the-last-warrior-by-andrew-krepinevich-and-barry-watts-1422053324.

20. Desch, "Don't Worship at the Altar;" and Carlos Lozada, "Inside the Mind of the Pentagon's 'Yoda,'" *Washington Post*, 11 January 2015, http://www.washingtonpost.com/news/book-party/wp/2015/01/08/inside-the-mind-of-the-pentagons-yoda-3/.

21. The ONA will also continue: James H. Baker, a retired Air Force colonel who has been a strategist for the chairman of the Joint Chiefs of Staff, has been appointed to succeed Marshall as director of ONA. Thomas Gibbons-Neff, "Pentagon Chief Issues New Marching Orders for 'Yoda' Office," *Washington Post*, 10 June 2015, https://www.washingtonpost.com/news/checkpoint/wp/2015/06/10/pentagon-chief-issues-new-marching-orders-for-yoda-office/.

22. Richard A. Best Jr., *The National Counterterrorism Center* (*NCTC*)*—Responsibilities and Potential Congressional Concerns* (Washington, DCL Congressional Research Service, 19 December 2011), 4, https://www.fas.org/sgp/crs/intel/R41022.pdf.

23. Department of Homeland Security, "About the Domestic Nuclear Detection Office," 21 July 2015, http://www.dhs.gov/about-domestic-nuclear-detection-office.

24. Future of Terrorism Task Force, Homeland Security Advisory Council, Department of Homeland Security, *Report of the Future of Terrorism Task Force* (Washington, DC: DHS, January 2007), 6, http://www.dhs.gov/xlibrary/assets/hsac-future-terrorism-010107.pdf.

25. James Jay Carafano, Frank J. Cilluffo, Richard Weitz, and Jan Lane, "Stopping Surprise Attacks: Thinking Smarter about Homeland Security," *Backgrounder* no. 2016, Heritage Foundation, 23 April 2007, http://www.heritage.org/research/reports/2007/04/stopping-surprise-attacks-thinking-smarter-about-homeland-security.

26. Frank J. Cilluffo, "The Department of Homeland Security: An Assessment of the Department and a Roadmap for Its Future," statement before the US House of Representatives Committee on Homeland Security, 20 September 2012, 8, http://homeland.house.gov/sites/homeland.house.gov/files/Testimony%20-%20Cilluffo_0.pdf. More recently, Cilluffo repeated his call for an ONA within the DHS in commenting on the *Quadrennial Homeland Security Review*. See, Dan Verton, "DHS Releases Quadrennial Homeland Security Review," *FedScoop* (blog), 20 June 2014, http://fedscoop.com/dhs-releases-quadrennial-homeland-security-review/.

27. Office of the Press Secretary, White House, "Biodefense for the 21st Century" (press release, White House, 28 April 2004), http://www.fas.org/irp/offdocs/nspd/hspd-10.html.

28. Judith Miller, "Bioterrorism's Deadly Math," *City Journal* 18, no. 4 (Autumn 2008): http://www.city-journal.org/2008/18_4_bioterrorism.html.

29. Forrest and Hilliker, "Why the Department of Homeland Security," 2–3, 8, and 12.

30. James R. Clapper, director of national intelligence, "Current and Future Worldwide Threats to the National Security of the United States," remarks as delivered to the Senate Armed Services Committee, 11 February 2014, http://www.dni.gov/files/documents/WWTA%20Opening%20Remarks%20as%20Delivered%20to%20SASC_11_Feb_2014.pdf.

31. Gen Martin Dempsey, chairman of the Joint Chiefs of Staff, *Hearing to Receive Testimony on the Impacts of Sequestration and/or a Full–Year Continuing Resolution on the Department of Defense, Hearing before the US Senate Armed Services Committee*, 113th Cong., 1st sess., 12 February 2013, http://www.armed-services.senate.gov/imo/media/doc/13-03%20-%202-12-13.pdf.

32. Christopher A. Preble, *The Most Dangerous World Ever?* (policy report, Cato Institute, Washintgon, DC, September–October 2014), http://www.cato.org/policy-report/septemberoctober-2014/most-dangerous-world-ever.

33. Jeh Johnson, secretary of homeland security, *Written Testimony of DHS Secretary Jeh Johnson for a House Committee on Homeland Security Hearing on "Worldwide Threats to the Homeland,"* 17 September 2014, http://www.dhs.gov/news/2014/09/17/written-testimony-dhs-secretary-jeh-johnson-house-committee-homeland-security.

34. Jeh Johnson, secretary of homeland security, *Statement before the US House Judiciary Committee*, 113th Congress, 2nd sess., 29 May 2014, http://judiciary.house.gov/_cache/files/189c8334-81e9-4d5e-bf46-96e0383e6ee2/dhs-testimony-5.29.14.pdf.

35. At least one analyst has called for such work to be done: Adam Elkus, "Towards a Counterterrorism Net Assessment," *Small Wars Journal*, 21 December 2011, http://smallwarsjournal.com/jrnl/art/towards-a-counterterrorism-net-assessment.

36. The 2015 *National Security Strategy* describes guarding against terrorism as "the core responsibility of homeland security." Barack Obama, *National Security Strategy* (Washington, DC: The White House, February 2015), 8, https://www.whitehouse.gov/sites/default/files/docs/2015_national_security_strategy.pdf.

37. Jeh Johnson, *The 2014 Quadrennial Homeland Security Review* (Washington, DC, DHS, 2014), 5, http://www.dhs.gov/sites/default/files/publications/2014-qhsr-final-508.pdf.

38. Office of the Press Secretary, White House, "Fact Sheet: The *2015 National Security Strategy*" (press release, White House, 6 February 2015), https://www.whitehouse.gov/the-press-office/2015/02/06/fact-sheet-2015-national-security-strategy.

39. Rose McDermott, "Methodology for Homeland Security," *Journal of Homeland Security and Emergency Management* 7, no. 2 (July 2010).

40. For example, Skypek, "Evaluating Military Balances through the Lens of Net Assessment," 6.

41. 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* 25, no. 3 (Autumn 1995): 9–19, http://strategicstudiesinstitute.army.mil/pubs/parameters/Articles/1995/1995%20villacres%20and%20bassford.pdf.

42. I am grateful to Captain Todd Veazie, US Navy, for suggesting that Clausewitz's concept of the trinity can be helpful in understanding homeland security.

43. Business Executives for National Security (firm), *Domestic Security: Confronting a Changing Threat to Ensure Public Safety and Civil Liberties* (Washington, DC: Business Executives for National Security, February 2015), 8, http://www.bens.org/file/CounterterrorismReport.pdf.

44. Brian Michael Jenkins, Andrew Liepman, and Henry H. Willis, *Identifying Enemies among Us: Evolving Terrorist Threats and the Continuing Challenges of Domestic Intelligence Collection and Information Sharing* (Santa Monica, CA: RAND, 2014), http://www.rand.org/content/dam/rand/pubs/conf_proceedings/CF300/CF317/RAND_CF317.pdf.

45. 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* 38, no. 1 (2015): 75–83; and Peter Bergen, Emily Schneider, David Sterman, Bailey Cahall, and Tim Maurer, *2014: Jihadist Terrorism and Other Unconventional Threats* (Washington, DC: Bipartisan Policy Center, 23 September 2014), http://bipartisanpolicy.org/wp-content/uploads/sites/default/files/BPC%20HSP%202014%20Jihadist%20Terrorism%20and%20Other%20Unconventional%20Threats%20September%202014.pdf.

46. Bergen, et al., *2014: Jihadist Terrorism and Other Unconventional Threats*, 9.

47. Johnson, *Statement before the US House Judiciary Committee*.

48. New America Foundation, "Homegrown Extremism 2001–2015," *International Security* (web site), 2015, http://securitydata.newamerica.net/extremists/analysis.html.

49. Brian Michael Jenkins, *Al Qaeda after bin Laden: Implication for American Strategy* (Santa Monica, CA: RAND, 22 June 2011), 5, http://www.rand.org/content/dam/rand/pubs/testimonies/2011/RAND_CT365.pdf.

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 later CIAC provided information that helped lead to the arrest of a bombing suspect. See Homeland Security Blog Team, "Fusion Centers: Empowering State and Local Partners to Address Homeland Security Issues," *DHS* (blog), 18 July 2011, http://web.archive.org/web/20130524232705/http://blog.dhs.gov/2011/07/fusion-centers-empowering-state-and.html.

51. US Senate Committee on Homeland Security and Governmental Affairs, Permanent Subcommittee on Investigations, *Federal Support for and Involvement in State and Local Fusion Centers*, staff report (Washington, DC: Senate, 3 October 2012), 2.

52. Michael Price, *National Security and Local Police* (New York: Brennan Center for Justice, New York University School of Law, 2013), 3, https://www.brennancenter.org/sites/default/files/publications/NationalSecurity_LocalPolice_web.pdf.

53. For a much more positive view on fusion centers than the Senate report noted above, see US House Committee on Homeland Security, *Majority Staff Report on the National Network of Fusion Centers* (Washington, DC: House, July 2013).

54. Jenkins, "Al Qaeda after bin Laden," 7.

55. Gregory Treverton, "Intelligence Test," *Democracy: A Journal of Ideas* 11 (Winter 2009): http://www.democracyjournal.org/11/6667.php?page=all.

56. Bailey Cahall, David Sterman, Emily Schneider, and Peter Bergen, "Do NSA's Bulk Surveillance Programs Stop Terrorists?" (policy paper, New America Foundation, Washington, DC, January 2014), https://www.newamerica.org/international-security/do-nsas-bulk-surveillance-programs-stop-terrorists/.

57. See for example, Christopher Hewitt, "Law Enforcement Tactics and Their Effectiveness in Dealing with American Terrorism: Organizations, Autonomous Cells, and Lone Wolves," *Terrorism and Political Violence* 26, no. 1 (2014): 58–68.

58. Peter Baker, "Obama Apologizes after Drone Kills American and Italian Held by Al Qaeda," *New York Times*, 23 April 2015, http://www.nytimes.com/2015/04/24/world/asia/2-qaeda-hostages-were-accidentally-killed-in-us-raid-white-house-says.html?_r=0.

59. Bergen, et al., *2014: Jihadist Terrorism and Other Unconventional Threats,* 47.

60. James J. Wirtz, "The Cyber Pearl Harbor," in *Cyber Analogies*, edited by Emily O. Goldman and John Arquilla (Monterey, CA: Naval Postgraduate School, 28 February 2014), 7–14.

61. Erik Gartzke, "The Myth of Cyberwar," *International Security* 38, no. 2 (Fall 2013): 41–73; and Thomas Rid, "Cyber War Will Not Take Place," *Journal of Strategic Studies* 35, no. 1 (2011): 5–32.

62. Deborah Charles, "U.S. Homeland Chief: Cyber 9/11 Could Happen 'Imminently,'" *Reuters*, 24 January 2013, http://www.reuters.com/article/2013/01/24/us-usa-cyber-threat-idUSBRE90N1A320130124.

63. Ellen Nakashima, "Cyber-Spying Said to Target U.S. Business," *Washington Post*, 11 February 2013.

64. James R. Clapper, *Worldwide Threat Assessment of the US Intelligence Community*, statement for the record before the Senate Armed Services Committee, 26 February 2015, 1.

65. Bergen, et al., *2014: Jihadist Terrorism and Other Unconventional Threats*, 43.

66. Colin S. Gray, *Making Strategic Sense of Cyber Power: Why the Sky is Not Falling* (Carlisle, PA: US Army War College Strategic Studies Institute, 2013), xi.

67. Clifton B. Parker, "Fight against Terrorism Likely Slow and Incomplete, Stanford Scholar Says," *Stanford News Service*, 3 September 2014, http://news.stanford.edu/news/2014/september/terrorism-strategy-crenshaw-090314.html.

68. Although the commander of USCYBERCOM is also the director of the NSA and the two organizations are both located at Fort Meade, Maryland, the two commands have different missions and operate under different legal authorities. See National Security Agency, "Frequently Asked Questions about NSA," https://www.nsa.gov/about/faqs/about_nsa.shtml#about10.

69. Quoted in Ellen Nakashima, "Dual-leadership Role at NSA and Cyber Command Stirs Debate," *Washington Post*, 6 October 2013, https://www.washingtonpost.com/world/national-security/dual-leadership-role-at-nsa-and-cyber-command-stirs-debate/2013/10/06/ffb2ac40-2c59-11e3-97a3-ff2758228523_story.html. See also Frank J. Cilluffo and Joseph R. Clark, "Repurposing Cyber Command," *Parameters* 43, no. 4 (Winter 2013–14): 111–18.

70. James Stavridis, "Why the Nation Needs a US Cyber Force," *Boston Globe*, 29 September 2013, https://www.bostonglobe.com/opinion/2013/09/29/why-nation-needs-cyber-force/quM4WWdJOh0FoSyE7rmxJI/story.html.

71. Richard Clarke, "Foreword," *Strategic Insights* 10, no. 1 (Spring 2011): 1, http://edocs.nps.edu/npspubs/institutional/newsletters/strategic%20insight/2011/SI_v10_I1_Spring_2011.pdf.

72. Aliya Sternstein, "Pentagon to Recruit Thousands for Cybersecurity Reserve Force," *Defenseone.com*, 16 April 2015, http://www.defenseone.com/technology/2015/04/pentagon-recruit-thousands-cybersecurity-reserve-force/110407/.

73. Eric Rosenbach, *Statement for the Record before the U.S. Senate Committee on Armed Services, Subcommittee on Emerging Threats and Capabilities*, 114th Cong., 1st sess., 14 April 2015. In July 2015, Rosenbach was named chief of staff to Secretary of Defense Ashton Carter. See also the recently released *DOD Cyber Strategy*, April 2015.

74. Michael S. Rogers, *Statement before the House Committee on Armed Services Subcommittee on Emerging Threats and Capabilities*, 114th Cong., 1st sess., 4 March 2015, 12.

75. David Clark, Thomas Berson, and Herbert S. Lin, eds., *At the Nexus of Cybersecurity and Public Policy: Some Basic Concepts and Issues* (Washington, DC: National Research Council, 2014), 100.

76. For example, a *Joint Action Plan for State-Federal Unity of Effort on Cybersecurity* was approved by the National Governors Association in July 2014. For an argument that city governments must take on more responsibilities in cyber security, see Mitchell D. Silber and Daniel Garrie, "Guarding Against a 'Cyber 9/11,'" *Wall Street Journal*, 16 April 2015, http://www.wsj.com/articles/guarding-against-a-cyber-9-11-1429138821.

77. Johnson, *2014 Quadrennial Homeland Security Review*, 21.

78. See for example The Centers for Disease Control and Prevention, "2014 Ebola Outbreak in West Africa," http://www.cdc.gov/vhf/ebola/outbreaks/2014-west-africa/.

79. Johnson, *2014 Quadrennial Homeland Security Review*, 22.

80. Ibid., 8.

81. Department of Homeland Security, *National Preparedness Report* (Washington, DC: DHS, 30 March 2014), http://www.fema.gov/media-library-data/1409688068371-d71247cabc52a55de78305a4462d0e1a/2014%20NPR_FINAL_082914_508v11.pdf.

82. See for example, Brian A. Jackson, *Applying Lessons Learned from Past Response Operations to Strengthening National Preparedness* (Santa Monica, CA: RAND, July 2014), http://www.rand.org/content/dam/rand/pubs/testimonies/CT400/CT411z1/RAND_CT411z1.pdf.

83. William O. Jenkins Jr., "Measuring Disaster Preparedness: FEMA Has Made Limited Progress in Assessing National Capabilities," Testimony before the Senate Committee on Homeland Security and Governmental Affairs, 17 March 2011.

84. Paul Stockton, "Ten Years After 9/11: Challenges for the Decade to Come," *Homeland Security Affairs* 7 (September 2011): https://www.hsaj.org/articles/582.

85. Thad W. Allen, "Confronting Complexity and Creating Unity of Effort: The Leadership Challenge for Public Administrators," *Public Administration Review* 72, no. 3 (May–June 2012): 320–21.

86. Christopher Dickey, "Time to Brace for the Next 9/11," *Newsweek*, 12 September 2011, http://www.newsweek.com/time-brace-next-911-67389.

87. Department of Homeland Security, *Fiscal Years 2014-2018 Strategic Plan* (Washington, DC: DHS, no date), 35, http://www.dhs.gov/sites/default/files/publications/FY14-18%20Strategic%20Plan.PDF.

88. Michael Chertoff "Remarks by the Secretary of Homeland Security Michael Chertoff" (speech, Bureau of Justice Assistance, Washington, DC, 14 March 2006), http://www.dhs.gov/xnews/speeches/speech_0273.shtm.

89. For a discussion of the civil liberties implications of domestic intelligence collection, see Erik J. Dahl, "Domestic Intelligence Today: More Security but Less Liberty?" *Homeland Security Affairs*, September 2011, https://www.hsaj.org/articles/67.

90. Bracken, "Net Assessment: A Practical Guide," 94.