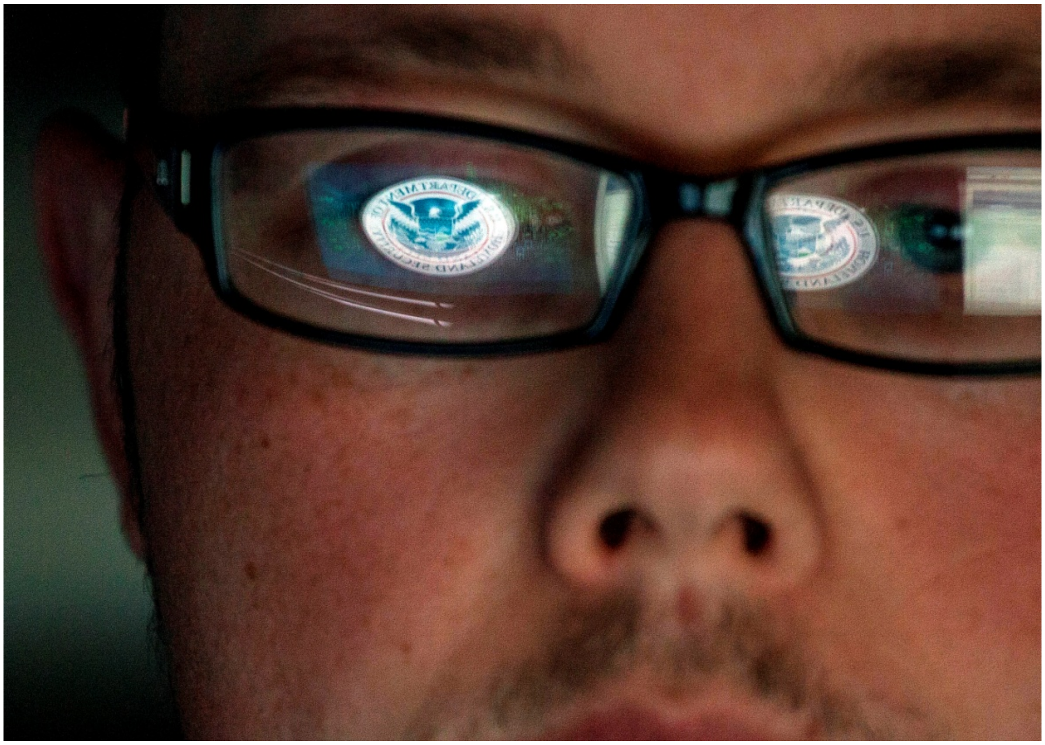
Governance Studies
at BROOKINGS

June 26, 2012



A cyber security analyst works in a watch and warning center at a Department of Homeland Security cyber security defense lab. REUTERS/Jim Urquhart

A Vision for Homeland Security in the Year 2025

Darrell M. West

INTRODUCTION

Imagine a future in which the barriers to catastrophic acts are low, and these capabilities are available to individuals or small groups. Unmanned drones controlled by terrorists, criminals, or drug lords attack critical infrastructure and endanger millions of people; digital intruders disrupt the power grid, financial sector, or Internet service.

Alternatively, these threats could be natural. Changes in weather patterns could result in a rise of water levels that threatens coastal cities or drought elsewhere that ruins crop production. Populations may be forced to move, thereby upsetting commerce, food and medical distribution, and supply chains around the world.

These are just a few of the risks facing the United States. As demonstrated by the devastation of natural events, such Fukishema in 2011, Hurricane Katrina in 2005, and the Indian Ocean earthquake/tsunami in 2004, and the continuing threats of terrorism and cyber intrusions, there are numerous threats with the potential to harm lives and damage our economy, society, and public order.

Darrell M. West is Vice President of Governance Studies and Director of the Center for Technology Innovation at the Brookings Institution.

Together with the MITRE Corporation, we gathered a group of leading experts in November, 2011 to discuss a vision for homeland security in the year 2025.[1] This gathering brought together individuals who were knowledgeable about homeland security from the public, private, and non-profit sectors to think about the country's threats, challenges, and proposed remedies. Guests included leaders from organizations such as federal, state, and local government agencies, Congress, the private sector, non-government organizations, think tanks, and nonprofit organizations for a discussion with an interactive dialogue.

The goals for this event were to help shape strategic thinking for the Department of Homeland Security (DHS), its critical stakeholders, and the nation. A key aim of this effort was to facilitate a forum for national thought leaders and senior government decision-makers to explore the future homeland security environment and consider the implications of evolving hazards, social and economic realignments, and technological advancements on homeland security policy and operations.

This paper summarizes key ideas that emerged from the day's discussion, such as future threats, integration challenges, and the resulting considerations for leaders across the Department of Homeland Security (DHS) as they work to make the United States safer.[2] Key themes that emerged from this dialogue included the following points:

- Understand homeland security as a diverse array of organizations, functions, capabilities, and priorities.
- Raise awareness of a systems approach to homeland security.
- Organize joint action across sectors and leverage private sector resources.

[1] Ken Rapuano and Leslie Anderson made helpful comments on earlier versions of this paper.
[2] Unless otherwise noted, direct and summarized quotations in this paper are from individuals at the November 2011 discussion.

- Develop real-time data analytics and decision-making tools.
- Institutionalize future-thinking across the security agencies.
- Educate senior officials and critical decision-making regarding state and local authority roles, processes, and procedures.

Future Threats

Ten years after the 9/11 terrorist attack and seven years after the stand-up of DHS, the way we think about homeland security in the United States has evolved significantly. Still a fairly young agency, DHS continues to focus on near-term security. Given the multitude of possible threats, it remains challenged by operational issues that hamper the agency’s ability to address its priority missions.

But much progress has been made. For example, the Department has worked to improve inter-agency communications and cooperation. Officials have put together taskforces that represent the agency’s diverse operations and stakeholders. They are integrating data bases, improving the ability to mine incoming information, and becoming more proactive regarding risk assessment.

In order to build on these steps, we need to make serious effort to evaluate future trends and threats to inform the capabilities and structures we’re building today. For the group that assembled, we asked them to think about the threats facing the country. In this section, we review the issues that emerged during that discussion. This included issues related to counter terrorism, geo-political risks, cybersecurity and technology changes, border protection, environmental changes and water shortages, and budgetary pressures resulting from government deficits.

Counter Terrorism: Nuclear, Radiological, Biological, Chemical, Drones, and Improvised Explosive Devices

Counter terrorism refers to activities designed to deter, prevent, or mitigate actions intended to terrorize individuals and/or societies. Threats can come from a range of different sources. At the most sophisticated level, nuclear, radiological, biological and chemical warfare represent major threats in terms of potentially catastrophic impacts on the society and economy.

But other, domestic-based, threats are also particularly worrisome. At our colloquium, federal officials and other participants expressed concern regarding the threats of homegrown radicals. These are individuals, often operating independently or in small groups, who plot attacks of generally low sophistication, such as employing improvised explosive devices (IEDs), drones, or small arms. Homegrown terrorism presents unique challenges in that the individuals of concern are already in the U.S., are frequently American citizens, and their activities are often self-initiated with little to no communications with known terrorist groups. Another threat for which there are concerns is the possibility that violence associated with a Mexican drug cartel will spill over our southwest border.

Ultimately, a major objective of terrorism is to intimidate general populations and influence decisions of governments. Efforts that educate the public, and enlist their participation in preventing, preparing for, and responding to terrorism are central to effective homeland security.

According to David Kaufman, director of the Office of Policy and Program Analysis of the Federal Emergency Management Agency, terrorism is above all "an attack on social trust." Yet increasing social trust and the level of involvement of the public in counterterrorism is a difficult to achieve its low risk and the many other priorities of Americans today.

To raise public awareness and enhance reporting of terrorism threats, DHS has launched a "see something, say something" campaign whereby the public is asked to become more aware and involved in alerting authorities when they observe something that looks suspicious. Through this and other outreach activities, the intent is for the public to adjust to a "new normal" where terrorism risks become part of the national consciousness, and the general population forms a first line of defense against terrorism activities.

...The intent is for the public to adjust to a "new normal" where terrorism risks become part of the national consciousness, and the general population forms a first line of defense against terrorism activities.

Over the past decade since 9/11, the Armed Forces have dramatically improved capabilities to identify and target suspected terrorists overseas. As stated by Vice Admiral Robert Harward, Deputy Commander of the U.S. Central Command, "we've built an amazing counter terrorism machine focused on finding, fixing, and finishing terrorists." He indicated there is a preference is to "get our hands on terrorists, rather than killing them," in order to collect intelligence that can be exploited to identify and target terrorist leadership elements and networks.

Admiral Harward noted that the best systems and processes supporting counter terrorism operations have tended to come from the bottom-up, versus top-down. He suggested the need for a new paradigm that focuses more on pre-attack, or "left of boom," activities representing key enabling functions of terrorist groups, such as recruiting, training, planning, and attack preparations. Enhanced emphasis on these functions includes placing increased importance on rule-of-law, human rights, media, and the establishment of civil and legal norms for better functioning societies.

Another essential element of increased effectiveness against terrorism in the next 10 or 15 years, in the view of many security experts, is continuing to improve how the United States leverages and shares information within government and among the many other stakeholders involved. For this reason, U.S. Central Command (CENTCOM) is focused on intelligence gathering and information sharing in conflict zones that improves prevention, deterrence, and operations down the road.

The experience and knowledge developed by the military in Iraq and Afghanistan have made significant inroads in terms of fighting terrorism. An increasingly experienced and integrated cast of players, enabled by processes and systems that have been tested in a dynamic landscape characterized by complex and evolving threats has been a game changer. However, as we depart Iraq and Afghanistan, there is risk of losing well-honed personnel, expertise, and processes. Leaders will have to make difficult trade-offs regarding how these capabilities can be preserved and improved in a landscape characterized by increasingly scarce resources.

It may be that the threat of Al Qaeda will recede over time as terrorism as a tactic evolves with the needs of those who employ it. According to David Heyman, the Assistant Secretary for Policy at the Department of Homeland Security, “terrorism likely will morph into something tactical adopted by all sorts of actors, and may not be those who we see today.” With the proliferation of technology and know-how, weapons of mass destruction, explosive devices, and drones are examples of tactics and techniques that are likely to become more accessible to a wider range of terrorist groups, “lone wolf” operatives, or criminal organizations in the years ahead.

Geo-Political Risks

Uncertainty in Pakistan, the Middle East, and elsewhere will continue to pose risks for the United States. Some observers fear the prospect of Pakistan imploding the way Iran did in 1979, leading to major instability in the region and significant risks posed by the potential loss of control of elements of Pakistan’s nuclear weapons arsenal. The prospect of wider and increased instability in this particularly problematic region will exacerbate circumstances that could add fuel to radical Islamist or other terrorist organizations. Harward noted, “This may hit us in the face 5, 10, or 15 years out.”

The situation in Egypt, Syria, and the rest of the Middle East as the Arab Spring continues to unfold, has significant implications for key U.S. relationships and stability in the region, and attendant security risks at home. While the military relationship between the United States and Egypt built over the 50 year period since the 1979 Egypt-Israel Peace Treaty remains strong. But conventional military training is not enough. The United States must engage with a wider range of constituencies including the general populations, the media, lawyers, public affairs professionals, and non-government organizations.

Likewise, the possibility of further instability or government collapse in Mexico raises significant implications for homeland security. Secretary of State Hillary Clinton has referred to Mexico’s drug way as a “criminal insurgency,” with the possibility of intra-Mexican violence spilling over the border, and creating northward migration based on internal unrest.

The American government must expand its engagement and development paradigm to extend beyond traditional emphasis on military relationships to address the wider range of stakeholders and conditions that affect our security. An important conclusion looking to the future is that the ability to influence and help governments evolve will require different communications and engagement strategies.

Cybersecurity and Technology Changes

The democratization of science and technology has elevated a number of different risks, especially in areas such as cyber-threats and bio-technology. The fact that individual scientists are able to sequence DNA, device cyber viruses, and produce highly sophisticated explosive devices means that capabilities that heretofore required the financial resources and technical capabilities of a nation-state, are increasingly in the hands of individuals. Bio-threats are quite worrying due to the progressively smaller footprint of resources and activities necessary to create and deliver biological agents with the potential for catastrophic consequences.

It is difficult to overstate the potential impacts of cyber threats to our national security, economic well being, and key societal functions. A senior Obama administration official puts it bluntly: "How we rise to the cybersecurity challenge will determine whether our nation's best days are ahead of us or behind us." According to Rand Beers, the Under Secretary for National Protection and Programs Directorate at the Department of Homeland Security, hackers and persistent security threats can do tremendous harm. Hacking is the most common form of cyber intrusion, and spans the range from annoying to highly disruptive. State-based actions are generally focused on collecting intelligence on state secrets, stealing private sector intellectual property, and identifying points of vulnerability.

Nation-states represent the most sophistical cyber capabilities with the greatest potential to undermine our military and economic advantages, and threaten critical infrastructure and key functions. But "non-state actors" in the form of individuals and groups have a wide range of capabilities and intentions. This includes hackers who more interested in the challenge of circumventing cybersecurity barriers to cyber criminals who want to exploit the Internet for illicit gain or cyber terrorists who seek to harm or intimidate for ideological reasons. Hackers are like pirates in the 16th century- they operate in free spaces that largely are unregulated. According to Heyman, cyber-related risk is a "big unknown with great potential for dramatic, non-linear impacts." He cautions that "preventing these threats will require additional capacity building in the near future."

Hackers are like pirates in the 16th century- they operate in free spaces that largely are unregulated. According to Heyman, cyber-related risk is a "big unknown with great potential for dramatic, non-linear impacts."

Security in this area is weakened by what Beers refers to as "lousy cyber-hygiene." Cyber exploitation and disruption are possible because people have not been properly "locking their doors." The public and businesses need to take cybersecurity more seriously and be more vigilant about passwords and computer safety. A range of tools are being developed and deployed to combat cyber threats into the future, but protecting systems and functions from a dynamic and ever-learning adversary requires constant vigilance and adaptation.

Presently, it is a challenge for NSA and cybersecurity experts to locate the source of attacks. Under current norms and rules, it is difficult to reach-back to individual addresses in order to identify the source of threats, or neutralize threatening Internet Protocol addresses. Some types of cyberspace threats are borderless and transcend political boundaries. They harbor criminal activity and make it difficult to govern the cyber ecosystem.

The other technology trend that has relevance for homeland security is the dramatic increase in use of information technology. According to David Kaufman, "The average American is exposed to three times as much information every day than in the 1980s." In addition, there has been a fundamental shift in how people utilize social networks and social media. Not only do people use advances in information technology to connect with friends and family, they employ these capabilities to mobilize for collective action. There has been a shift away from large centrally governed organizations, toward authority being increasing vested in trusted networks.

This has significant implications for information acquisition, threat management, and emergency response. It suggests that we need a different mindset for the cyber era. Solutions must be tailored to the amorphous capacity and varying scales of cyber-networks. Threats can come from large or small sources and may not be connected to broader social networks.

Border Protection

The free and efficient flow of commerce and people across national borders is fundamental to the freedoms and economic vitality of our nation. By the same token, preventing terrorists, weapons and other harmful materials from entering the United States, and enforcing our immigration laws, are also essential to national security. People think of border protection primarily in terms of land borders with Mexico, said Alan Bersin, the former commissioner of U.S. Customs and Border Protection (CBP). His organization has approximately 22,000 officers at 250 checkpoints. By 2025, more than 10 percent of CBP agents and officers will be working outside the United States. Some of these will be working with Canadian and Mexican officers to pre-clear individuals before entering the North American continent; others will be overseas locations supporting pre-clearance operations. Through the work of these individuals, millions are screened for threats and cleared daily at the borders.

CBP wants to make the haystack smaller and segment traffic to focus on people and packages which have been determined to present higher risk.

CBP is now the largest manager of government information outside of the intelligence community. For many individuals, it is the law enforcement agency that collects data and then acts on it. For example, in the cases of the Detroit bombing attempt and Yemen cargo plot, CBP flagged the perpetrators. The goal is to identify people as far from point of entry into the country as possible. CBP wants to make the haystack smaller and segment traffic to focus on people and packages which have been determined to present higher risk. Improving the capacity to focus on suspicious persons and packages improves the ability to prevent threats, and expedites lawful commerce and travel.

The challenge for the agency is a better understanding of how homeland security relates to national security. By definition, border protection involves connecting international with domestic operations. In this situation, international collaborations improve security through information sharing. For example, sharing information with Canada on our “no fly” list is beneficial to the U.S. That type of collaboration helps each nation to maintain its respective security, and puts the United States on a firmer footing regarding border threats.

Environmental Change and Water Shortages

The United States and other areas around the world face increasing risk of natural catastrophes related to climate change. Leading scientists assess that climate change is occurring more rapidly than most anticipated and will have significant consequences and resulting implications for national security. It is worrisome because a large proportion of the world's population and infrastructure is located in vulnerable geographic areas, and will thereby be exposed to risks of storms, flooding, or rising water levels.

Water shortages and drought conditions furthermore represent a source of risk, according to David Kaufman. Climate changes have made drought an increasing concern in this country. Limited water in certain parts of the country constrains economic development and places restrictions on how individuals and businesses can grow and develop.

But we rarely have declared an official drought in the United States. We need to confront the reality of water shortages and its impact on commerce and economic growth. In some parts of the country, water supplies are quite limited and affect local decision-making. Unless we can address water problems, it will limit future options in those places.

There also is the environmental risk of increases in "normal accidents" involving advanced technology. Recent accidents at Fukashima, Japan and in the Caribbean due to Deep Water Horizons oil drilling suggest that the expanding technological sophistication can increase the risk of natural disasters.

The adoption of technology whose operations and impact are not fully understood challenges our ability to respond when accidents happen. Rather than having a reservoir of experience in terms of how to deal with problems, accidents can turn into crises and have a costly impact on the nation's future. We need better capabilities for risk analysis and threat detection in environmental areas.

Budgetary Risks

As we look to a future characterized by dynamic change and evolving risks, and recognize the need to better integrate within the Department and the broader homeland security enterprise, we must adapt to these dynamics in an austere budget environment. With large government deficits looming, the challenge is how, with fewer resources, we improve integrated functioning of the homeland security enterprise while maintaining necessary investments in maintaining base capabilities.

This is a particular tension in research and development and security infrastructure because of the multiple threats and varying sources of risk faced in the homeland security areas. Problems related to terrorism, geo-politics, cybersecurity, border protection and environmental change are evolving and therefore are not well-integrated into agency operations or budgeting. Limited resources increase the importance of prioritizing homeland security missions and functions to inform our investments towards achieving national goals.

An important consideration is the effect the economic downturn has had on state and local governments, i.e., the 'front lines' of the homeland security enterprise. For example, according to DHS Undersecretary for Science and Technology Tara

O'Toole, the nation has lost 50,000 state and local public health officials to budget cuts since 2007, as well as a number of emergency management personnel. This weakens the capacity of state and local government to respond to environmental change, biohazards, and other national emergencies.

Going forward, our approach must be cognizant of the budget impact on a range of key homeland security stakeholders. We must maintain crucial investments in order to identify threats, manage risks, and safeguard homeland security.

Cross-cutting Missions

Homeland security missions cut across agency boundaries. The Department has large and diverse organizations, many with longstanding histories as independent entities: the Transportation Security Administration, Customs and Border Protection, Citizenship and Immigration Services, Immigration and Customs Enforcement, Secret Service, Federal Emergency Management Agency, and Coast Guard represent the primary operational components. Ever since the Department's stand-up in 2003, the role of headquarters has been to integrate, coordinate, and facilitate communications across these various organizations.

Yet from the very beginning, there have been concerns that DHS is overly siloed and lacks integration, and that these factors made it difficult to identify risks and assess threats. According to David Heyman, when considering the range of different missions within the Department and the dynamic nature of change, "it is difficult to know what the priority mix will be in 15 years." Between organizational shifts, new actors, and evolving threats, it is tough to anticipate what will be the most important problems.

In assessing the current and future homeland security landscape, an important challenge is the cross-cutting nature of homeland security missions. Virtually all the challenges involve different DHS agencies and other federal organizations, state and local government, the private sector, non-profit agencies, and the public at large.

The stove-piped nature of these sectors and organizations means that people, processes, and technologies are inherently difficult to integrate. As noted by David Heyman, homeland security is a "bottom-up and distributed enterprise" with many different levels. Fulfilling each of the DHS missions means getting different people and agencies to share information and work together.

We know that likely drivers of change include rapid technological change, urbanization, geo-political developments, demographic shifts, and environmental factors. These forces affect the roles, responsibilities, and missions of multiple organizations, and demonstrate the increasingly cross-cutting nature of our capabilities to manage these risks.

The intersection of nature, technology, human error, and bad intentions results in events that can range from high-probability/low-consequence to low-probability/high-consequence problems. Just as these factors drive risk levels, they expand the capability requirements of DHS over the next 15 years. Everything from technology and environmental changes to geo-political developments can have broad consequences for FEMA, the Coast Guard, Border Protection, and Immigration Services, among other entities. Changes in various parts of the world can affect the United States by altering agriculture, trade, and migration patterns. Natural disasters no longer are just local events, but can influence people far removed from the actual occurrence due to long supply chains and an interconnected world.

Interdependencies between Federal, State, Local, NGO, and Private Sectors

The most fundamental challenge in homeland security is the need to achieve better coordination among the many different agencies involved in cross-cutting missions. A command and control structure similar to that found in military organization with clearly delineated authorities, responsibilities, and roles doesn't work well when there are differential resources across various levels of government. State and local emergency preparedness officials are responsible for planning and preparedness of incidents ranging from the routine to major disasters, but plans for catastrophic events require financial means far beyond those available at the local level. In addition, local planning authorities are not under the direct control of federal officials or private businesses, so when local efforts fail, the entire response is put at risk.

In the case of Hurricane Katrina, the country experienced a dramatic example of what happens when these interdependencies don't work well.

Disasters such as biothreats or pandemics involve virtually every sector. Responsibilities can cut across federal departments such as Homeland Security, Defense, and Health and Human Services. Businesses are involved because they distribute food, medicine, and water. State and local agencies play a major role because they typically are the first responders who evacuate people, provide medical care, find housing, and deal with transportation.

In the case of Hurricane Katrina, the country experienced a dramatic example of what happens when these interdependencies don't work well. According to Colonel Terry Ebbert, distinguished visiting fellow at the Homeland Security Institute and a former director of Homeland Security for the City of New Orleans, the problem in this and other examples of natural disasters is that local officials "write evacuation plans but don't own busses, planes, or trains." Yet it is local authorities who have the direct responsibility to move threatened populations out of harm's way.

The challenge in these kinds of situations is managing to handle emergencies in a short time frame when officials don't own or control the necessary resources. In cases of actual evacuations, it is complicated to move people without separating families and pets, and making sure people have food and medical supplies. Right now, the country places tremendous responsibility on those who lack the resources to implement their plans. Unless resources match the requirements, it will be impossible to manage system logistics.

The person with the least resources but the greatest responsibility is the local incident commander. He or she must concentrate on planning and training with the available capacity. There *will* be an emergency at some point so it is important to concentrate on planning, training, and spending all the limited money in best means possible. As aptly put by Ebbert, the job of local commanders is similar to that of a NFL coach. "You must learn to play the game with the hand you're dealt, and develop plans around capabilities you are able to control."

The private sector also plays a key role. Michael Jackson, the founder of Firebreak Partners and former Deputy DHS Secretary, noted that businesses and industry are crucial because they provide services for many people. This is especially the case with episodic events. "The private sector can often do it better, faster, and cheaper because they specialize," he said. In the case of food distribution, David Kaufman pointed out that it is important to "connect to a capacity that already exists in an everyday context." There are a small number of companies that transport the majority of foodstuffs to grocery stores, regardless of chain, and most of them are not widely known. Yet in an emergency, they may be the crucial cog in getting people fed.

In a world of digital communications, "the public will not fit into the plan. Instead, the emergency plan needs to fit the public," he said.

The Role of Technology in Emergency Management and Coordination

Information sharing is vital during disasters and emergencies. Getting the word out about threats and emergency response often spells the difference between effective and ineffective responses. If public, private, and non-profit agencies don't cooperate or if people don't know where to go for help, the situation rapidly deteriorates.

David Kaufman explained that social media have changed mass communications. "We have shifted from large organizations as authorities to an authority within a network, whether that person is a legitimate authority or not," he said. Anyone from bloggers to news aggregators to private individuals posting messages on Facebook and Twitter is important. In a world of digital communications, "the public will not fit into the plan. Instead, the emergency plan needs to fit the public," he said.

Technology potentially is an enabler of improved communications, but only if it is coordinated and deployed effectively. Government officials must understand that people receive a lot of information outside of official channels and devise their communications plans to work with existing information providers, both in the old and new media. In too many cases, information is deployed at cross-purposes or in ways that confuses the public. This weakens the ability of service providers to deal with particular crises.

Managing Threats in a Dynamic Environment

Homeland security is a widely distributed and diverse discipline. It is driven by a bottom-up matrix as opposed to the top down, command and control model as is the case in the national security apparatus. The core question is how to bring together the various actors in order to address mission interests in most efficient and effective way – in what is inherently a decentralized and dynamic environment.

To be successful, we must improve the analytic tools of policymakers. This involves risk-assessment for decision making and strategic planning and strategy development. The tools decision makers have in making these decisions right now are *very* weak. One panelist noted that Internet travel engines are better decision-support tools than those that DHS currently has in place. In the future, we must improve the tools so evaluators know which missions on which to focus.

Many of the most important homeland security challenges cross agency lines. For example, this is true with bioterrorism, aviation, or cargo threats. The threat is not neatly reconciled with departmental boundaries. The Department of Homeland Security needs more organizational innovation in order to shift from command and control approaches. In the aviation world, travelers have access to the entire global system, not just one airport and travel route. This means that the international system has to coordinate across national borders.

The same is true with cargo threats. Liquid explosive plots are much more complex because they bring together air, land, and sea organization worldwide. There are increasing interdependencies throughout the world with the need to monitor a wide range of activities. This means that capabilities need to be aggregated to address problems as a whole. That's why the Department is a matrix organization. According to Heyman, "we need to put all capabilities together in the matrix to change the approach problems."

In short, to deal with dynamic threats, we need to bring together people, organizations, technology, and processes. People need to have incentives to coordinate and work together, and solve problems regardless of agency jurisdiction or mission. Only by managing threats in an integrated manner can we have any hope of safeguarding our homeland security.

The Need for Integration

In this paper, we have laid out the most pressing future trends and threats as seen by thought leaders who attended our discussion session. They discussed cross-cutting missions and the resulting complications leaders face at all levels of society and government. Based on this analysis, we have found that our current situation is characterized by several specific characteristics:

- Homeland security faces complex problems in which stakeholders often disagree on the nature of the problems as well as the solutions (i.e., technical and social).
- Their missions are changing rapidly and unpredictably—thus systems must interoperate in ways that their original developers never envisioned.
- People are integral parts of the network, and their behavior will change the nature of the network.
- Homeland security presents complexity that is a consequence of the interdependencies that arise when large numbers of systems are networked together to achieve some collaborative advantage.
- It is further intensified by rapid technology changes. When networked systems are affected by technology and mission changes, the environment

for any given system or individual becomes essentially unpredictable. The combination of large-scale interdependencies and unpredictability creates a dangerous environment for the United States.

In this section, we review the need for integration and ways to build a network that analyzes data in real-time and enables DHS officials to connect the dots in a rapidly changing environment. Based on our analysis, we recommend several steps for improving homeland security:

- Take a systems approach to addressing homeland security missions.
- Organize joint action across sectors and leverage private sector resources.
- Develop real-time data analytics and decision-making tools.
- Institutionalize future-thinking across the security agencies.
- Educate senior elected officials in state and local processes/procedures.

Take a Systems Approach

As federal, state, and local agencies as well as private and non-profit organizations adapt to changing security missions and threats, the operating environment becomes unpredictable. The best way to address the combination of large-scale interdependence and unpredictability is to develop a holistic approach.

There are several examples of how this can work. The DHS Transportation Security Administration must screen and verify individuals arriving or leaving the United States. Currently, there are seven separate information systems to screen air, sea, and land transportation that are not well-integrated. Developing systems that exchange data would improve agency coordination and be more effective at identifying threats and managing risks.

Currently, there are seven separate information systems to screen air, sea, and land transportation that are not well-integrated.

At the state and local level, law enforcement agencies need a means to integrate data bases and operations. Each of the 50 states needs better capacity to exchange homeland security information between federal, state, and local government. This helps front-line responders assess risks and determine who warrants more intensive analysis.

These and other types of systems help to manage uncertainty and interdependence. They build effective and efficient networks that meet the objectives of the whole enterprise. These systems provide operational support to business planning, policy-making, and investment.

Organize Cooperation Across Sectors and Leverage Private Sector Resources

In thinking about system integration, it is important to think about large and small scale models. Sometimes, crises arise from large, whole scale movements, while others are very retail, such as what are the most effective ways to deliver outcomes to people in need during a moment of crisis? In homeland security, we need to think about how we work effectively on both levels.

For example, FEMA must track real life issues such as when stores are open during an ice storm or other weather-related emergency. In general, the quicker you can reconstitute local commerce in the affected area, the faster the area can recover. According to David Kaufman, "one of the key questions is who is feeding people during a disaster?" Working with private sector supply chains and distribution networks is crucial to addressing this issue.

One of the fundamental questions is: what is the relationship between federal and state/local organizations and the private and non-profit sectors. Who is responsible for various activities and how do we coordinate across sectors? These types of relationships are not well-defined in the United States. Limited government resources mean that the public sector must figure out ways to leverage private sector resources.

The question is: what is the best way to incentivize. In the past, this was done largely through monetary incentives, such as subsidies or tax breaks. But in an era of large budget deficits, this is not an ideal way to proceed. We need new ways to incentivize companies and private individuals. For example, in the cyberthreat area, companies should be more forthcoming about reporting threats and unwanted intrusions so that we have better data on cyberattacks. Providing for uniform reporting standards across industries would be a way to protect against market penalties for attacked companies in a way that levels the playing field for all firms.

However, it can be very hard for a private industry to engage DHS. If private sector engagement is key, do we need to change approaches to create that level of trust? There always will be some part of industry that complains about DHS, but the best way to engage would be to set up certain requirements and ask the private industry to find a way to meet those requirements.

In addition, there are dangers of going too far, according to Theodore Chuang, associate general counsel at the Department of Homeland Security. There are conflicts of interest and other issues we run into if the department looks to the private sector for everything. For example, we can increase our resources by having the private sector do things, but the private sector is for-profit and they need to be paid. The Department has to be careful how it manages relationships.

One way to get the public and private sectors to work better together is through joint, online procurement using reverse auctions. The Department can get economies of scale if all acquisitions in common areas are made from one procurement. This is a way to use information technology to save money and improve efficiency of operations.

Develop Real-Time Data Analytics and Decision-Making Tools

We need to get people good information fast. The question is how do we get good information at all times? One way is through real-time data analytics. This approach takes advantage of social media and mobile devices to quickly collect and analyze information.

Yet one of the challenges of crowd-sourcing risk assessment and threat identification to the general public is designing information and management systems that are able to make use of that material in real-time. For many attacks, time is of the essence in prevention or deterrence. Minutes matter in these situations.

For example, a quick-thinking street vendor observed a suspicious car parked in New York's Times Square and called authorities. But with these types of real-time tips, it takes a rapid response capability to act on tips, get law enforcement to the scene, clear the area, and deal with the explosive material. Any time delay along that path would have been too late to prevent a deadly attack.

Institutionalize Future-Oriented Thinking

It is important to institutionalize future-oriented thinking because homeland security officials spend most of their time fighting specific issues in the trenches as opposed to thinking long-term. Building space for this thinking is important, but then you have to align leadership. Some have asked whether DHS should have something like the Department of Defense Office of Net Assessment. According to Heritage Foundation Visting Fellow Paul Rosenzweig, that would be one effective way to institutionalize future-oriented thinking.

Recent reports of bio-surveillance suggest that one of the things we have to deal with is the rapid pace of change. Agency officials need to be more agile in the future.

In addition, the department needs better ways to deal with/respond to rapid pace of change. Recent reports of bio-surveillance suggest that one of the things we have to deal with is the rapid pace of change. Agency officials need to be more agile in the future. Some are concerned that budget pressures and the relative clunkiness of the inter-agency processes will limit the strategic thinking especially about unlikely events.

The department also needs to focus on capacity building, and determining what works and what doesn't. Having a strong program evaluation helps department planning and keeps officials focused on long-term trends.

Train Senior Elected Officials

We need to train senior elected officials at the state and local levels. There are around 1,000 people in the United States making big security decisions so we should be able to educate them. However, one-third of them have held their jobs for two years or less, and often lack information on emergency preparation or response.

Many state and local elected officials do not understand the laws and provisions on the utilization and capability of the government's "Title 10" military forces. "We spend thousands on training emergency forces, yet that is worth nothing if we don't train those who give orders to these forces," said Terry Ebbert. He pointed out that there is a void in understanding who should make what decisions and how to work up the line properly. Often the real decision makers are not involved in training. Education should be done in a peer group, such as getting governors together so they will be more open and receptive. Homeland security will never have the luxury of training military personal for long term, high intensity situations like the Department of Defense does.

The situation is even more complex when entering into issues of cybersecurity, biosecurity, and hospitals. People involved in those issues lack training on emergency response and government decision-makers need much better training exercises than what we have today.

The problem, according to Ebbert, is that:

> *We don't train our local first responders to fight a long war. Firefighters and police officers are 'sprinters' so the local public safety organizations struggled to assist in the response and recovery with Katrina. They had not slept or eaten for 75 hours prior to landfall (and he has learned that you must sleep and eat when fighting a war). You must make sure people take care of themselves while being responders or we will lose people.*

There is a huge psychological impact in taking individuals away from their families for long periods of time while fighting a natural disaster. Tara O'Toole noted that "the sooner you return to some sense of normality, the faster the recovery seems to be. Unless we make progress in those areas, it will be difficult to protect homeland security.

Governance Studies
The Brookings Institution
1775 Massachusetts Ave., NW
Washington, DC 20036
Tel: 202.797.6090
Fax: 202.797.6144
www.brookings.edu/governance.aspx

Editors
Christine Jacobs
Stephanie C. Dahle

Production & Layout
Stefani Jones

Email your comments to gs@brookings.edu

This paper is distributed in the expectation that it may elicit useful comments and is subject to subsequent revision. The views expressed in this piece are those of the author and should not be attributed to the staff, officers or trustees of the Brookings Institution.