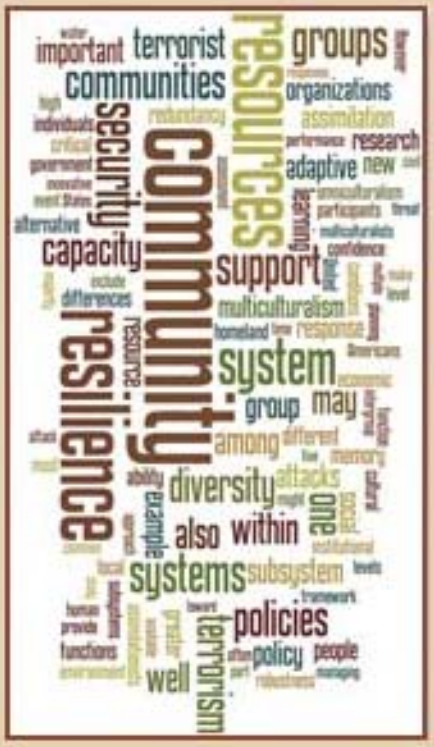
VOLUME VI, ISSUE 3: SEPTEMBER 2010

HOMELAND SECURITY AFFAIRS

THE JOURNAL OF THE
NAVAL POSTGRADUATE SCHOOL CENTER FOR HOMELAND DEFENSE AND SECURITY



ISSN 1558-643X HTTP://WWW.HSAJ.ORG

Report Documentation Page

Form Approved
OMB No. 0704-0188

1. REPORT DATE	2. REPORT TYPE	3. DATES COVERED
SEP 2010		**00-00-2010 to 00-00-2010**

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
The Journal of the Naval Postgraduate School Center for Homeland Defense and Security. Volume 6. Issue 3	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **Naval Postgraduate School,Monterey,CA**	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S)
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release; distribution unlimited

13. SUPPLEMENTARY NOTES

14. ABSTRACT

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT **unclassified**	b. ABSTRACT **unclassified**	c. THIS PAGE **unclassified**	**Same as Report (SAR)**	**124**	

Notes from the Editor

The articles and essays in this issue of *Homeland Security Affairs* all reflect – in some manner – on how we, as a nation, approach the process of homeland security. Ranging from specific suggestions for procedures and systems to more philosophical discourses on guiding principles, each author (or set of authors) offers a unique perspective on the overriding question of "how do we manage the security mission in the face of perceived threats?"

In "Organizational Innovations in Counterterrorism," Daniel R. Langberg argues that today's national security environment demands whole-of-government approaches to meet the security challenges of the twenty-first-century. These challenges include terrorism, trafficking in persons, and cyberspace security. At present, our national security system is organized along functional lines, with weak coordinating mechanisms across functions. Langberg suggests that the counterterrorism community offers a practicable model for national-level interagency coordination.

This need for coordination is emphasized by James Steiner in "More is Better: The Analytic Case for a Robust Suspicious Activity Reports Program." Steiner outlines the suspicious activity report (SAR) process, from collection through analysis, and looks at the validity of concerns that an expanded SAR program represents a threat to civil liberties. He then presents two analytic requirements for the collection of more – rather than less – information through the SAR process to increase the probability of identifying pre-operational terrorist activity and to improve the efficiency and effectiveness of critical infrastructure protection.

Robert T. Mahoney also offers a model – for preparing emergency responders to deal with terrorist attacks as well as routine emergencies. "Threat-based Response Patterns for Emergency Services" proposes a process by which emergency service departments can conduct a comprehensive risk assessment as a basis for developing new response patterns. These new patterns acknowledge that a terrorist crisis condition is different from the daily, routine conditions for which most first-responders are trained.

This process of developing new patterns of response may need to be implemented at the federal level as well. Albert J. Mauroni argues that the Department of Homeland Security (DHS) has erred in applying Department of Defense (DOD) concepts and scenarios, based on responding to weapons of mass destruction, to the threat of chemical, biological, radiological, and nuclear (CBRN) terrorism. The DOD military response to support state and local emergency responders is not appropriate for today's conditions. In "Homeland Insecurity: Thinking About CBRN Terrorism," Mauroni identifies a methodology for reviewing DHS CBRN-response policies and suggests there are more moderate, sustainable strategies for dealing with CBRN terrorism.

Twenty-first-century security threats are also the topic of Raphael Sagarin's "Natural Security for a Variable and Risk-filled World." The key to addressing these threats, according to Sagarin, may lie in a common solution framework based on adaptability,

which applies the basic tenets and specific strategies of natural security systems to the analysis, planning, and practice of security in human society. As he observes, natural security is adaptable; organisms in nature achieve adaptability through a decentralized organization where threats are detected and responded to peripherally, by managing uncertainty and turning it to their advantage. This adaptive capacity is illustrated in how U.S. troops have used organizational structure, uncertainty, and symbiotic relationships to respond to and protect against IED attacks in Iraq and Afghanistan.

Adaptive capacity, along with resource robustness, is cited as the basis of community resilience in "Building Resilient Communities." Drawing on an interdisciplinary body of theoretical and policy-oriented literature, Patricia Longstaff and colleagues provide a definition of resilience and suggest a framework that will serve as a tool for guiding planning and allocating resources. This is accomplished by examining resilience attributes according to five key community subsystems: ecological, economic, physical infrastructure, civil society, and governance.

Another aspect of community – racial and ethnic diversity – and the role this diversity plays in perceptions of threat is the subject of "Homeland Security and Support for Multiculturalism, Assimilation, and Omniculturalism Policies among Americans" by Fathali M. Moghaddam and James N. Breckenridge. Using a representative probability sample of more than 4,000 Americans, the study presented here found a majority preference for omniculturalism that cuts across American sociodemographic differences, yet predicts critical variations in the perceived threat of terrorism, the priority of terrorism, confidence in government, and support for aggressive counter-terrorism measures. These preferences, according to the authors, deserve the attention of homeland security professionals.

As always, we publish these essays and articles with the goal of furthering the homeland security debate. Your comments and contributions are welcome at www.hsaj.org.

The Editors

Organizational Innovations in Counterterrorism: Lessons for Cyber-security, Human Trafficking, and Other Complex National Missions

Daniel R. Langberg

All too often our national security and foreign policy institutions are slow to learn lessons from their own successes and failures. Lessons are identified and applied to an even lesser extent across different institutions and missions. But when problems and solutions are systemic – due to systems designed for a much different era – the experiences of one discrete organization or community can offer valuable insights to an entirely different set of actors.

One issue that demands particular attention in the contemporary security environment is how best to apply whole-of-government approaches to complex national missions, ranging from combating terrorism and trafficking in persons to securing cyberspace. These and many other twenty-first-century security challenges require an agile and integrated response; however, our national security system is organized along functional lines (diplomatic, military, intelligence, law enforcement, etc...) with weak coordinating mechanisms across these functions. Today, there is no definitive model for integrating capabilities and funding for inherently interagency missions.

Recent reforms in the U.S. government counterterrorism community provide a valuable case study on this subject for several reasons. First, the terrorist threat is representative of twenty-first-century national security challenges that are complex, trans-border, and fraught with multiple sets of networked, non-state adversaries. Second, like all multifaceted problems, counterterrorism requires a holistic approach to address; in this case, the law enforcement, financial, diplomatic, military, legal, and other dimensions of the terrorist threat. Third, the tragic events of September 11, 2001 led to the most systemic review and subsequent set of national security reforms thus far in the 21st century.

The creation of the Directorate of Strategic Operational Planning (DSOP) within the National Counterterrorism Center (NCTC) to conduct counterterrorism planning and assessments provides one model for integrating high-priority, high-complexity, multi-agency missions. Interagency teams for other national missions, such as cyber-security, should be seriously considered to support the National Security Staff in strategic management of end-to-end processes (policy, strategy, aligning resources with strategy, planning, execution, and assessment) and to fulfill functions such as:

- Clarifying interagency roles and responsibilities;
- Conducting integrated policy analysis and teeing up policy options;
- Developing national strategies;
- Conducting deliberate, dynamic and/or contingency planning;
- Conducting assessments of the nation's progress in meetings its goals and objectives; and

- Conducting long-term assessments on the changing nature of the threat/opportunity.

Certain key enablers must be in place for any interagency team or organization to be fully effective. These include:

- A reporting chain to the president;
- An institutionalized linkage to the National Security Staff;
- Requisite authorities;[1]
- Congressional support and clear jurisdictional ownership;
- An untangling of overlapping mandates and authorities; and
- Interagency national security professionals with critical experience and skill sets (e.g., planning and assessments, negotiation, appreciation of diverse agency cultures, etc.) and interagency and intergovernmental organizations with planning, execution, and reach-back capabilities.

The 9/11 Commission found that the counterterrorism mission is in need of "joint planning" and "joint action" to ensure that unity of purpose and unity of effort are achieved. The Commission further recognized that the National Security Council staff, consumed with managing day-to-day crises, was unable to fulfill the functions of strategic planning and oversight and was therefore incapable of effectively managing a whole-of-government approach to counterterrorism on its own. Attempting to rectify these deficiencies, the Commission envisioned the National Counterterrorism Center as fulfilling these roles and "breaking the older mold of national government organization."[2]

In 2004, the Intelligence Reform and Terrorist Prevention Act (IRTPA) established NCTC to serve as the U.S. government's locus for counterterrorism intelligence and strategic operational planning. Part of the NCTC mandate was "to conduct strategic operational planning for counterterrorism activities, integrating all instruments of national power, including diplomatic, financial, military, intelligence, homeland security, and law enforcement activities within and among agencies." To accomplish this, the IRTPA established the Directorate of Strategic Operational Planning within NCTC and gave it responsibility for developing interagency strategic operational plans, assigning roles and responsibilities for plans, coordinating interagency operational activities, monitoring implementation of plans, and conducting assessments.[3]

In February 2010, the Project on National Security Reform (PNSR) released a report – *Towards Integrating Complex Missions: Lessons from the National Counterterrorism Center's Directorate of Strategic Operational Planning* – that studied DSOP in depth and found it to be a promising example of a national-level integrating mechanism for a complex mission such as counterterrorism.[4] The Directorate conducts a broad range of integrating functions including interagency planning, assessment, and resource oversight to help ensure a holistic approach to the mission. Although this fledgling institution continues to face the inherent challenges of operating in an outdated system, the concept it embodies – an interagency mechanism

to support the National Security Staff in strategic management of a discrete mission – is worthy of consideration in other contexts.

Imagine, for example, an interagency cyber-security team chartered by the president and reporting to him through the National Security Staff. The team would report to the president, but could be housed in the Department of Homeland Security in the near-term for administrative and other support.[5] It would consist of a permanent cadre of subject matter experts and individuals trained in strategic planning and assessments working alongside detailees from across the government. A cyber-security team could assist senior policy-makers by analyzing policy options, teeing up decisions, and developing planning, resource, and assessment products related to cyber-security. More specifically, an interagency cyber-security team could:

- Develop a comprehensive national cyber-security strategy that identifies goals and objectives and assigns roles and responsibilities;
- Conduct interagency contingency planning to consider how the nation would respond to a variety of cyber attacks;
- Conduct dynamic planning to disrupt or respond to an actual attack;
- Conduct assessments to determine if the nation is making progress in achieving its goals and propose actions to increase effectiveness;
- Conduct long-term assessments to consider what the cyber threat might look like in the future;
- Perform various resource oversight functions in support the Office of Management and Budget (OMB); and
- Integrate perspectives of other mission partners such as intergovernmental, private sector, and non-government stakeholders.

Today, no entity has responsibility for deliberately fulfilling these functions on a whole-of-government basis for the cyber-security mission. Other interagency mission areas have integrating mechanisms in place, but most are not fulfilling these roles. For instance, the National Counter Proliferation Center (NCPC) – also established by the IRTPA – does not have an equivalent to DSOP that looks beyond the intelligence community to conduct planning and assessments with all counter-proliferation stakeholders.

Or consider human trafficking, a twenty-first-century national security concern that has been linked to organized crime, drug trafficking, migrant smuggling, and terrorist financing. Similar to counterterrorism, counter-proliferation, and cyber-security, trafficking is a complex, multifaceted challenge that does not fall under the jurisdiction of any single executive branch organization. The anti-trafficking challenge unites nearly thirty offices in at least seven major U.S. government departments and agencies, as well as numerous intergovernmental and other mission partners. Out of recognition for the need to integrate these diverse capabilities, the President's Interagency Task Force (PITF) and supporting Senior Policy Operating Group (SPOG) were established as

policy-coordinating bodies and a Human Smuggling and Trafficking Center (HSTC) was created to serve as an information clearing house.[6]

Despite these developments, the anti-trafficking mission is still without a national strategy that establishes goals and objectives and delineates roles and responsibilities. There is no national planning and assessments capability that can integrate the perspectives of all mission partners. What would an interagency planning cell within the HSTC look like? Reporting to the president through the SPOG, this interagency team could lead all stakeholders (interagency and intergovernmental)[7] in strategic planning and assessments for the anti-trafficking mission.

The PNSR study identifies several important lessons from the DSOP experience that are applicable to other mission areas. First, this case study demonstrates the importance of a reporting chain to the president. The director of NCTC reports to the Director of National Intelligence (DNI) for the intelligence aspects of the NCTC mission but reports to the president for DSOP work on whole-of-government planning and assessments. This chain of command and proximity to the president convey an informal authority that is beneficial, if not necessary to lead an effective interagency team.

In addition to a direct link to the president, just as critical is a seamless and institutionalized linkage to the team's customers in the interagency space – including relevant National Security Staff Directorates, NSC Committees, and OMB staff. These relationships are necessary to stay relevant and add value as organizational arrangements and policy priorities shift within and across administrations.

Moreover, the linkage to Congress is just as critical. The lack of congressional oversight and funding mechanisms that can look holistically at a complex national mission such as counterterrorism or cyber-security will also inhibit the effectiveness of any interagency team. A congressional champion is critical to resource the team and to provide streamlined oversight of the national mission. Furthermore, Congress must resource the participating departments and agencies that are being asked to contribute to a mission that may not be a core part of their mandate.

The State Department's Office of the Coordinator for Reconstruction and Stabilization (S/CRS)[8] is an example of the "lead agency" approach to integration. S/CRS was established in 2004 to support the secretary of state in leading and coordinating U.S. government reconstruction and stabilization efforts. The office has made progress integrating U.S. government capabilities to prepare, plan for, and conduct stabilization and reconstruction activities, but these efforts have been hindered as a result of S/CRS being buried within the State Department and without strong and consistent congressional support.[9]

In addition to the informal authority brought about by proximity to the president, the relevancy derived from an institutionalized relationship with the National Security Staff, and the formal authority derived from a champion on the Hill, other systemic impediments will plague any future interagency team just as they have plagued DSOP. For any complex, multi-agency mission such as counterterrorism or cyber-security, untangling overlapping mandates and authorities to ensure that all actors understand the need for the existence of, and leadership from, an interagency team is necessary for the team to achieve its full potential.

Any planning cell – including DSOP and S/CRS – will suffer from a lack of civilian planning and assessment capacity resident throughout the U.S. government. Until a government-wide human capital system is established to provide personnel with the necessary experience, expertise, and incentive, an interagency team will struggle to find sufficient numbers of individuals with the right skill sets. Beyond trained individuals, entire departments must be prepared to provide planning and reach-back support to personnel deployed to the field or to an interagency team in Washington.[10]

Complex national missions such as cyber-security, reconstruction and stabilization, and anti-trafficking in persons demand an integrated approach. Formal integrating mechanisms are needed to support an overburdened and understaffed National Security Staff. The experience of the Directorate of Strategic Operational Planning within the National Counterterrorism Center offers many valuable lessons for future interagency teams and provides insights into the challenges associated with operating in an outdated system. Before true integration can be achieved, the overall national security system must be modernized and recalibrated to put national missions ahead of parochial interests. Absent holistic reform, however, much can be done to improve on existing approaches and bolster mechanisms that enable the United States to bring all its capabilities to bear in the twenty-first-century security environment.

Daniel Langberg is a founding member of the Project on National Security Reform (PNSR) – a comprehensive effort to improve the U.S. government's ability to meet the strategic challenges of the twenty-first-century. He currently serves as deputy director for interagency teams and planning and was recently the deputy director of the first-ever comprehensive study of the National Counterterrorism Center's Directorate of Strategic Operational Planning. Mr. Langberg is also an analyst at the Institute for Defense Analyses where he conducts research on a variety of issues related to complex contingencies and interagency affairs. He may be reached at dlangberg@pnsr.org.

---

[1] For a discussion on a range of possible integrating functions and authorities, see: Project on National Security Reform, *Towards Integrating Complex National Missions: Lessons from the National Counterterrorism Center's Directorate of Strategic Operational Planning* (Arlington: Project on National Security Reform, 2010), http://www.pnsr.org/data/files/pnsr_nctc_dsop_report.pdf.

[2] National Commission on Terrorist Attacks Upon the United States, *The 9/11 Commission Report* (New York: W.W. Norton & Company, 2004), 399-403.

[3] Intelligence Reform and Terrorism Prevention Act of 2004, Pub. L. No. 108-458, 119 Stat. 3673 (2004).

[4] Project on National Security Reform, *Towards Integrating Complex National Missions: Lessons from the National Counterterrorism Center's Directorate of Strategic Operational Planning* (Arlington: Project on National Security Reform, 2010), http://www.pnsr.org/data/files/pnsr_nctc_dsop_report.pdf.

[5] The current national security system cannot accommodate an entity like DSOP standing on its own in the "interagency space"—the space below the president and above the departments. Just as DSOP is housed within NCTC inside the Office of the Director of National Intelligence, any new team will require an organizational home for administrative and other support. One option for a long-term solution is to build a capacity in the National Security Council staff to either a) house and manage priority teams or b) manage priority missions along with the overall system from a central hub. For a thoughtful discussion on

the latter approach see: Bob Polk, *The Thinking and Doing of National Security* (Washington, DC: Trafford, 2010).

[6] Daniel R. Langberg, "U.S. Government Response to Human Trafficking in the 21st Century," in *Case Studies Volume I*, ed. Richard Weitz (Arlington, VA: Project on National Security Reform, 2008), 131-171, http://www.pnsr.org/data/files/pnsr%20case%20studies%20vol.%201.pdf.

[7] *Interagency* is defined as United States government federal departments and agencies; *Intergovernmental* refers to federal, state, local, and tribal governments.

[8] State Department, "Office of the Coordinator for Reconstruction and Stabilization," www.crs.state.gov.

[9] For a more detailed discussion on the limitations of the "lead agency" approach and the S/CRS model see: Project on National Security Reform, *Forging a New Shield* (Arlington, VA: Project on National Security Reform, 2008), 138-140; 573, http://pnsr.org/data/files/pnsr%20forging%20a%20new%20shield.pdf.

[10] For more on the need to train entire departments for interagency missions see: Robert Polk and Merriam Mashatt, "From Deploying Individuals to Deploying Departments," *Prism* 1, No. 3 (2010): 13-20, http://www.ndu.edu/press/from-deploying-individuals.html.

Threat-based Response Patterns for Emergency Services: Developing Operational Plans, Policies, Leadership, and Procedures for a Terrorist Environment

Robert T. Mahoney

America is at war. Unlike most of America's past wars, this war is being fought simultaneously in multiple locations overseas and within our borders. Our military continues to function in its traditional role as the front line troops overseas, but the frontline duties at home in this war of terrorism have become the responsibility of those who have not been tasked with that previously: America's emergency services.[1]

Several of our communities have been attacked and/or threatened. Thousands of our citizens and hundreds of our emergency personnel have been injured and murdered in this war at home. Yet, there is little in the experience, organization, structure, training and response patterns of the emergency services that have prepared them for this role as war fighters.

Numerous directives and guidelines have been produced at all levels of government concerning preparation, protection, recovery, etc. from terrorist attack,[2] but how to incorporate that information into the day-to-day operations of the emergency services and their response patterns has been largely left to the discretion of the emergency services themselves. How those operational changes develop and evolve will require an understanding of a series of steps and dynamics that will have to be taken at the individual community and departmental levels in order for those agencies to adopt and adapt to their new war fighting tasks.

In spite of the fact that the terrorist threat to the United States has been realized for many years, and even after the disasters of September 11, 2001, not all emergency service departments have fully absorbed the lessons of that day. Some have not coordinated the work of each of their operational and administrative elements *to create response patterns that specifically address this changed and highly dangerous operational environment.* Unfortunately, at times the work of these different elements can become parochial and self-focused, and they may fail to coordinate their response pattern development efforts to reach a collective, functioning, best outcome that benefits the entire department. This condition may be reflective of, among other possibilities, insufficient organizational structure, ineffective leadership, individual personality differences, or a lack of a common understanding of the purpose and primary objectives of the organization itself. Such parochial difficulties, particularly in the current operational environment created by terrorism, can result in a lack of efficiency, a loss of effectiveness, duplication of effort, unnecessary expenditure of funds and resources, loss of public trust and confidence, increased danger to department personnel, and the loss of life and property.

Correcting this condition can be largely addressed through an awareness and adoption of a professional methodology that conforms a department's organization, planning, leadership, functioning, training, and response pattern into one that has a common understanding of the nature of the threat environment and of the fact that the department is involved with war-fighting.

A Form of War

As previously noted, a department responding to terrorism is involved in a form of warfare. In this current state of conflict, it is referred to as "asymmetrical" warfare, which for the purposes of this article will mean the forces, means, and capabilities of the terrorists are dramatically out of balance with that of their enemies. Given that, the terrorist must try to compensate for this imbalance by selecting targets, using tactics and weapons, etc., that provide them with an impact greatly in excess of their size and resources. Since terrorism is a form of unconventional or "asymmetrical" warfare, it is useful to note certain situations from past wars which can highlight the difference between routine and crisis conditions and thinking as regards to response patterns.

The Civil War battle of Antietam was the bloodiest battle ever fought in America. In one day, 22,719 were killed. At Antietam, there is a small, triple arch, twelve-foot-wide stone bridge over the Antietam creek, now known as Burnside Bridge. Union General Ambrose Burnside, following orders, sent multiple waves of soldiers to attack across the bridge. Although each successive attempt was decimated, he nonetheless kept repeating the tactic he had been trained in, which was the then currently accepted method relied on *routinely* in past battles.[3]

Fifty years later, in World War I, French Field Marshal Joseph Joffre, British General Sir Douglas Haig and other allied commanders, sent attack after attack out of the trenches for months, against the German machine guns, at the Battle of the Somme. A half million soldiers died in that one battle; 60,000 British on the first day alone.[4] Joffre, Haig and the other commanders apparently found it impossible to change methods and tactics, or to realize and adapt to the changed threat (weapon) environment.

Both these warfare examples are indicative of a thought process that displays the difference between routine and crisis preparation, thinking, recognition, and response. Both examples demonstrate the use of the *routine* form of thinking and response.

Conversely, the British admiralty had a number of wooden warships under construction on the day they received word of the battle between the first ironclads – the Monitor and the Merrimac – during the American Civil War. They quickly accelerated plans to have iron plates bolted to the sides of their new ships, recognizing that the operational environment had permanently changed and that wooden hulled ships were no longer sufficient and could not serve as the core of their navy.[5] While some senior naval officers probably failed to accept that their routine methods had to be changed, the organization as a whole grasped and understood the *crisis* condition that existed, and started to develop methods that addressed their new operating environment.

The purpose of this article is to consider how a number of operational and administrative skills and abilities, familiar to emergency services but not necessarily suited to meeting the current terrorist condition, should be re-examined and corrected. This article will demonstrate how those familiar elements are not isolated, independent issues, but are in fact parts of a continuum of the same problem (the threat) that must be addressed comprehensively to meet the requirements of, and to operate in, this new terrorist war-fighting environment.

In order to create appropriate response patterns it is first necessary to completely understand the nature of the terrorist threat and risk that a department can be facing,

both generally and to the responding entities specifically. This is done through a risk assessment process.

This article reviews what an emergency service department should understand about the elements of 1) threat, 2) risk, 3) security, 4) resources, 5) crisis leadership, 6) training, and 7) planning. This article then reveals how gaining an understanding of each of these elements both informs and improves all the other elements. Such knowledge enables these elements to be mutually supportive in the development of counter terrorism response patterns. This process uses a series of understandings, transitioning in sequence from one element to the next, and each builds on the previously gained knowledge. These transitions are:

Transition 1: Understanding Threat Informs Risk Analysis

Transition 2: Risk Analysis Informs Security Mitigations

Transition 3: Security Ensures Resource Allocation for Terrorist Events

Transition 4: Terrorist Events Require Crisis Leadership Skills

Transition 5: These Issues, Addressed Through Training and Plans

THE TERRORIST ENVIRONMENT

Records of the Global Terrorism Database at the University of Maryland show that worldwide there have been over 10,000 terrorist attacks on police facilities and officers since 1970.[6] Hospitals have also been attacked as part of wider terrorist actions. In the Mumbai, India, terrorist attack in November 2008, the terrorists attacked the counter-terrorism forces while they were responding from their headquarters, killing several of them, including the commanding chief of the Anti-Terrorist Squad.[7]

The *9/11 Commission Report* noted that Khalid Sheikh Mohammed who planned the attack on the World Trade Center admitted to having sent Dhiren Barot (aka. Issa al Britani) to New York six months before the 9/11 attack to conduct surveillances of the World Trade Center and other targets.[8] The video tapes he made were found in a computer seized in Pakistan in 2005. Barot was sentenced to 136 years in prison for terrorism in the United Kingdom in 2007 and copies of the tapes he made were released to the public by Scotland Yard. Among the targets he photographed and concentrated on were a Fire Department of the City of New York (FDNY) firehouse and the police presence in the vicinity of the World Trade Center.[9]

In the United States, as in other countries around the world, the use of "secondary devices" or bombs, to kill and injure first responders as they arrive at a scene, has been a tactic used by terrorists and is an attack method that first responders and their departments have become aware of. Under such conditions, responding units know they need to have a heightened sense of security as they approach such a scene, but the above information suggests a further threat.

Barot's video taping of a fire station as part of an array of targets, the bombing of hospitals and police stations as *targets themselves* and/or as part of a wider attack on a primary target, is a clear indication that the terrorists understand the high target value these first responder personnel, units, and locations represent. However, recognizing

the possibility of terrorists targeting and attacking the first responder locations and resources – *as prime objectives themselves* – is generally not part of the operations and response planning of first responder units and departments in this country. Past terrorist actions indicate that such occurrences are foreseeable risks that emergency services should consider including in their planning.[10]

The May 2010 attempted car bombing of New York City's Times Square is an instructive event. The initial call transmitted from the police on scene was for a car fire. The first arriving emergency service was the fire department, which responded according to routine protocol to commence a fire suppression operation based on the information that had been received. Due to their counter terrorism awareness, the FDNY quickly assessed and realized that the situation was potentially a vehicle-borne improvised explosive device (VBIED) and took appropriate action. Had this not been done and had the device exploded, it is probable that the department would have again experienced the highest casualty rate among the emergency services.[11]

It is important to understand that, nationally, most of the response patterns currently in place for routine operations are insufficient to address the types of situations a department will encounter in responding to an ongoing terrorist attack such as the Times Square incident. New plans must be created for these situations. There is a process that can be used to assist department leaders and planners in developing threat-based response patterns, one that uses the transition of knowledge gained in each element to assist in the development of the next one. It starts with a fully inclusive risk assessment.

TRANSITION 1: Understanding Threat Informs Risk Analysis

Determining which threats a department faces does not necessarily mean there is an equal risk associated with each of the threats. To develop appropriate response patterns to terrorist threats, a department must convert knowledge of threats into risk.

A formal process of conducting a risk assessment within a department is the initial step in developing plans, policies, and procedures to address operations within the current terrorist environment. Risk assessments use established protocols and algorithms in their analytical process. These protocols can be complex and/or proprietary in nature, depending on which of several available methodologies is selected. The following is a simplified review of the sequence of steps that a risk assessment may contain. It is not a detailed explanation of each of the elements involved in every step of the process, but rather an overview of the objective of the steps leading to an organized indication of risk. With this knowledge a department or organization can proceed to the development of response operations suitable to address the known and identified threats and risks. Without this knowledge a department will resort to guessing about the actual functional condition of their capabilities and counterterrorism profile.

Risk Assessment

The first step in the elimination of internal parochial planning concerns is conducting a risk assessment, and the first part of that is determining the nature of the threat

scenarios the department is likely to encounter. The process described below focuses on the terrorist environment as the specific threat being addressed, as compared to ordinary or routine response circumstances. While it is recognized that the current interest in an "all hazards" approach to planning has significant utility and appeal, the array of situations an emergency department can find itself involved in may already include many, if not all of the naturally occurring, unintended, and accidental emergencies present in an all hazards approach to planning. Departments whose territory and response activity include blizzards, earthquakes, tornados, or other cyclically occurring emergencies may have become prepared and conditioned to manage such matters through years of response to such emergencies. However, large explosive charges, the use of chemical and radiological weapons, directly attacking department locations and personnel, etc., presents a much different set of circumstances for which departments are not as prepared. Existing natural hazard response plans may or may not need up-dating, but planning for and responding to terrorist activity is different than other emergencies.[12] Addtionally, plans based on terrorist risk assessments can bring benefit to departmental capabilities in responding to an "all hazards" environment.

The Risk Assessment process being discussed in this article consists of seven sequential sub-elements: 1) threat, 2) criticality, 3) vulnerability (likelihood), 4) response and recovery capabilities, 5) impact (consequence), 6) risk, and 7) needs.

1. The *threat* component permits a department to identify the types of terrorist weapons it needs to consider and protect against, as well as the means by which each of those weapons can be used against the department. A specific threat is dependent upon the terrorist's objectives, motivations, and capabilities, as well as the target attractiveness of the department's assets to the terrorists.

2. The *criticality* element permits the department to rate the relative importance of each of its assets in accomplishing the department mandate. Establishing this hierarchy of criticality also suggests which assets require protection from the terrorists' methods of attack.

3. The *vulnerability* component evaluates the amount of security an asset has as compared to the possibility of a successful attack upon it. Noting the specific vulnerabilities per type of attack also suggests potential security enhancements to counter those vulnerabilities.

4. The *response and recovery* element measures the capability of the department to respond to and recover from each of the types of attack upon the department itself. This is not to be confused with response patterns for operations in the terrorist environment generally.

5. The *impact (or consequence)* part of the assessment measures the percentage of loss of the assets' criticality to the department that would occur due to a successful attack. This metric also represents the relationship between the

terrorists' capabilities to achieve their objective and the department's ability to protect against it.

6. The *risk* component demonstrates a hierarchical rating of the assets for each type of attack as a result of the threat, vulnerability, and impact analysis. Each of the department assets is compared to every other identified asset to demonstrate their relative risk.
7. The *needs* component permits a department to review various security and recovery solutions that would serve to reduce the level of risk the department faces from a terrorist event.[13]

Threat

In this country, responding to terrorism is an experience limited to a very few emergency services departments. It should therefore be an area of concern for those departments that have not yet considered it as an issue. The range of terrorist threats to a department is identified by the types of weapons used or sought by terrorists. Emergency responders know them as Weapons of Mass Destruction, or WMD. Included in this category of weapons are: chemical, biological, radiological, and nuclear weapons, and explosives. In addition, an analysis of recent terrorist tactics and methods shows that more conventional types of weapons and tactics, associated with the "small unit type actions" displayed in the Mumbai attack, can also be devastating to emergency services. [14]

The likelihood of a department encountering any or all of these forms of attack is a variable driven by the full range of conditions and circumstances unique to each department and its location. A departmental liaison to, or membership in, a regional Fusion Center or a Joint Terrorism Task Force can serve as the source for current and realistic threat information.[15]

Note that the level of existing threat is entirely outside the control of a department when considering WMD's. The amount of threat from these types of weapons is controlled by, and exists solely within, the terrorist element itself and the actual prevention of WMD use is not normally within the capacity of local first responders. Unless the department is capable of neutralizing the terrorist organization itself, or changing the beliefs, objectives, means, or capabilities that drive their attack motivations, the department will not be able to "prevent" an attack. The terrorist organization always retains the option to change the location of its attack to another, "softer" target in order to satisfy its objectives. Thus, that attack is not "prevented," but only "deterred" onto another location.

Criticality

Every department has a mandate or reason for its existence. That reason may be found in enabling legislation, a charter, or mission statement. The initial process in doing a risk assessment answers the question, "What do we do?" The best answer is one that views the department mandate at a high level. For example, for a fire department the answer "We put out fires." is not as comprehensive or accurate as "We prepare for and respond to emergencies that threaten life and property." Opening the range of

possibilities in this manner facilitates thinking about the development of a list of critical assets.

Few departments have assets and resources that are not necessary to some aspect of the department mandate, but not every resource or asset is critical to the mission. The criticality element of the assessment allows a department to evaluate which of its assets are the most important ones for accomplishing its mission.

All departments function as networks of assets and elements that interact with each other, either operationally or administratively or both. It is the linkage and the frequency of linkage between these elements that can define the networked structure of the department and the criticality of those elements.

The terms used for describing the different types of elements in a network are "nodes", "links", and "hubs". A *node* can be a particular building, a piece or type of equipment, or part of a process, etc. The *links* are the elements and/or parts of a process that serve to connect nodes. This can be a physical, administrative, or operational "pathway" that connects or creates interaction between nodes. A *hub* is a node that multiple other nodes link to. The more links there are from other nodes to a particular hub, the more critical that hub becomes.[16]

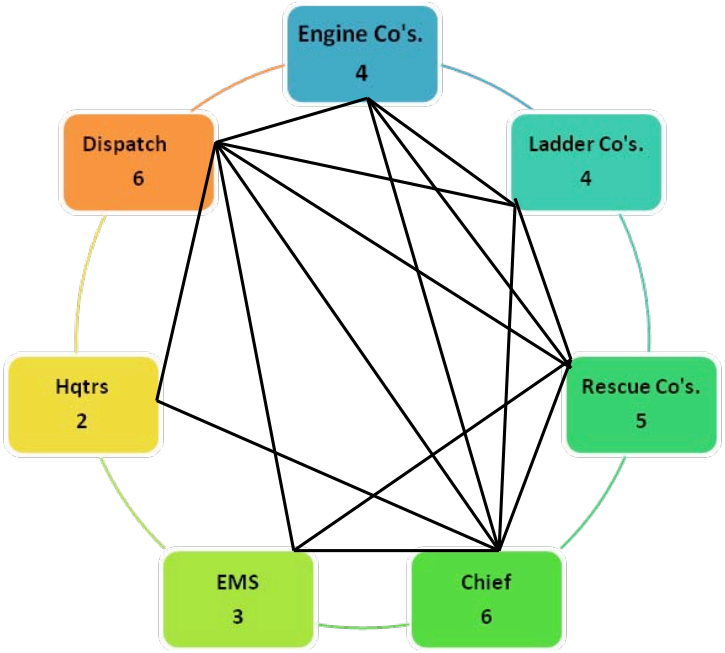


Diagram 1

In theory, the hub with the largest number of links is the most critical in the department network and each of the subsequent hubs have their hierarchy established in a similar manner. While network theory recognizes there are many factors available for use in this calculation,[17] for the purposes of this risk assessment discussion, Diagram 1 displays a notional example of a department's assets on a chart based on the number of

operational communication interactions between some of these elements in a department; many other criteria can also apply.

While each of a department's assets is "critical", it should be clear that each of them is not equally critical. Each critical asset's importance to the range of different factors that make up the department mandate is an indication of its position in a hierarchy of criticality.

These assets, owned and operated by the department, each make an important contribution to achieving the department mandate. Their final position in the hierarchy will reflect an analysis using a common set of factors that make each of them critical to accomplishing the department mandate. Such factors can include the number of casualties that will occur from the loss of this asset, the percentage of the department's ability to function that will be lost due to the loss of this asset, the cost of replacing the asset, etc., but these factors will not apply equally to each asset. Combining the ranked assets with these factors will result in a hierarchy of all the assets' critical relationship to the completion of the department mandate.

Vulnerability

An array of attack weapons and methods are available to the terrorists for them to potentially use successfully against any asset. Clearly, not every weapon would be appropriate for use at each site or against each asset, yet an asset may have a wide spectrum of weapons and tactics that can be used against it.

Note that the use of a particular type of weapon is influenced by many factors external to the department. The objectives of the terrorist element, their chosen means for achieving these objectives, and their capacity for having and using a particular type of weapon are all factors that would be considered. There must be a corollary between the objectives of the terrorist organization, their capabilities and methods, the importance of an asset in achieving (or preventing) their objectives, and the security conditions at the asset to deter the terrorist. Diagram 2 below provides a notional example of how these conditions result in the different types of threat, weapon(s), and attack scenarios that a terrorist might choose to use against an asset, depending upon the particular vulnerabilities of each of the critical assets of the department.

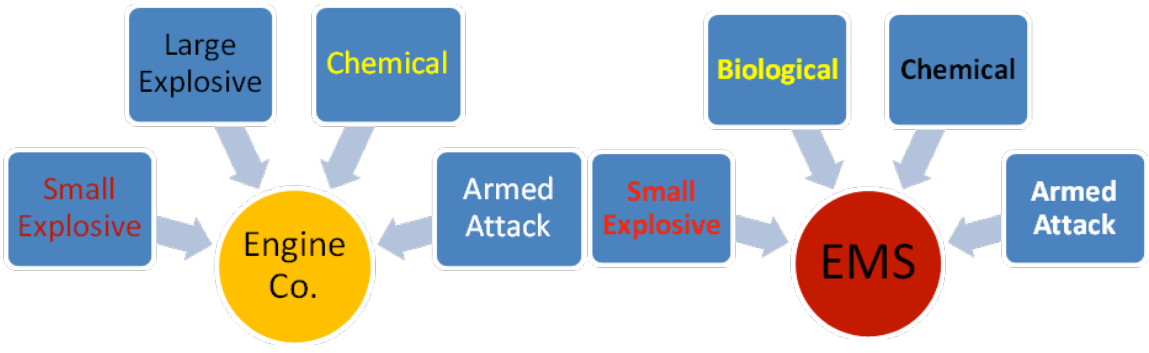


Diagram 2

As revealed above, each of the identified department assets can have a vulnerability to multiple, selected types of attack. Understanding vulnerability consists of knowing both certain specifics about the attack method verses the security conditions that exist at the asset. Some elements of an asset might serve to deter an attack – i.e. the security procedures in place at the asset are believed to be sufficient to deny terrorist access (fences, card readers, etc.) – and such an attack could be detected before it is completed because of other procedures (CCTV, lighting, etc.). There is also the probability that once the attack is detected, it could be interdicted before it is carried out. Other aspects of an asset might be so lacking in security that it would attract an attack. In short, it is necessary for a department to look at itself as the terrorist would in order to determine its vulnerabilities.

It is the difference between the offensive aspects of an attack and the defensive abilities of the asset that provides an indication of the likelihood of a successful attack. If an asset is highly vulnerable to a particular type of attack, and attacking it with a selected type of available weapon would serve the terrorist's objectives, then the probable vulnerability or likelihood of a successful attack at that asset might be high. Conversely, even if the asset is vulnerable but the terrorist element doesn't posses that type of weapon and/or attack capability, or attacking that asset would not serve the terrorist's objectives, then the probability of attack would be lower.

A department can be fully capable of deterring an attack through the introduction and use of security measures that counter specific types of attacks. It is of paramount importance that departments consider security measures to mitigate these types of attack in their planning procedures. It should also be noted that the department's planning must be sensitive to the potential that improperly selected and/or applied security measures may only serve to "deflect" rather than deter an attack. For example, if a department so hardens its administrative building that the terrorists attack a less defended operational building within the same department, then the department has succeeded only in "deflecting" rather than "deterring" attack. In this case it cannot be said that the attack was "prevented".

Response Capabilities

There are specific measures available for preparation for, defense against, and/or response to types of terrorist attack. The department's internal capabilities across a wide range of areas of expertise and resources will be required in the wake of such an attack to continue performing the department mandate. Organizational structure and leadership, the existence of operational plans and procedures, the level of training and expertise, the availability and use of equipment and or systems, and the number and type of personnel and their availability are all primary issues for appropriate response and recovery. The gap between the current readiness condition within the department and a desirable level of readiness in order to continue departmental functionality equates to a department's response needs. For example, if a department needs twenty SWAT trained officers when it currently has eight, or the department has one rescue company but also needs a Haz-Mat capability, such conditions reveal the gap between existing departmental resources and what the current threat environment requires them to have.

Some of the administrative and infrastructure elements of the department also contribute to its response readiness. These includes such things as the presence of administrative plans and procedures, the existence of alternate facilities, communication capabilities, the existence and continuity of vital information in databases, and a periodic use of training exercises. The combination of these operational and administrative elements can reveal the difference between current capabilities and terrorist incident response needs.

Impact

Impact (or consequence) can be described as the portion or fraction of an asset's criticality that would be lost to the department in each of the attack types previously described. This impact is balanced to a degree by determining what fraction of that impact could be reduced or mitigated due to the identified response and recovery capabilities of the department. The combination of these various elements (the percentage of criticality of the assets destroyed, the percentage mitigated by recovery capabilities, and the amount of impact mitigated by response capabilities) has a direct relationship to the overall consequence to the department from these attacks and, by extrapolation, to the surrounding community.

Relative Risk

Relative risk means that assets of different types, with different purposes and functions, being similarly threatened by multiple types of weapons and attacks, can still be measured in direct comparison to each other's level of risk exposure. This also means that all of a department's critical assets can be evaluated as a group.

These risk calculations can be plotted on a graph, where the vertical axis represents vulnerability (likelihood) and the horizontal axis represents consequence (impact), by placing a point on the graph for each type of attack at each critical asset. Those points close to the axis junction (lower left) have less vulnerability and/or consequence than those at a distance from it (upper right). In practice, the assets and attack type combinations proceeding diagonally on the graph up and to the right from the axis point represent the highest level of risk and require the most immediate attention to secure. Since all the assets and attack types are measured against the same set of threats, and each asset has a point on the graph for each type of risk it faces, the plot points display the relative risk between all the assets.

Using this method, it is possible for a department to know that, given its circumstances, the greatest risk may be to their communications center from a vehicle borne explosive, or to their EMS center from a biological weapon, or their headquarters from a chemical attack, or to their rescue company quarters from a man-carried explosive, etc. Each attack type and location will have a position (node) on the graph in direct risk-relationship to every other type of attack at each of the other assets. The below graph displays a notional example of a typical relative risk assessment diagram; an asset can have multiple points on the graph representing each type of attack it could face, while some types of attack appear multiple times against different assets.

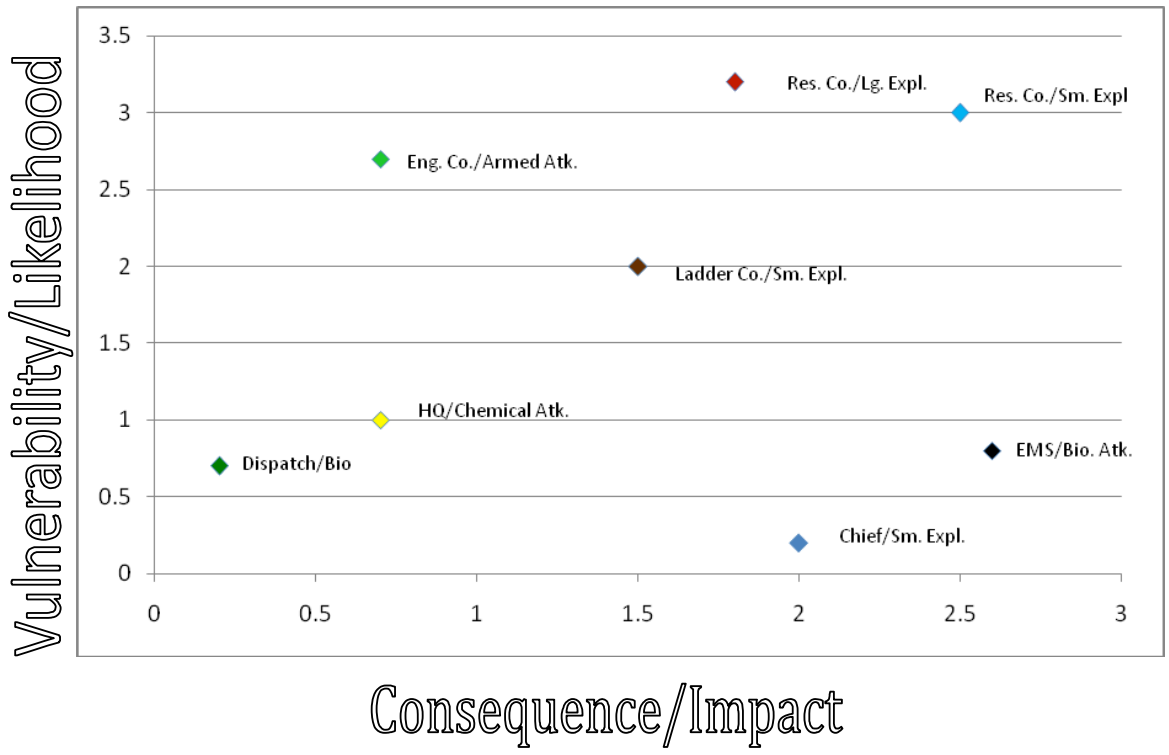


Diagram 3

Needs

Through extrapolation, Diagram 3 also informs department management and personnel of what corrective measures need to be taken in order to lower risk. Determining the reasons for a vulnerability rating suggests the lack of a defensive security measure (or a combination of security measures). Instituting such a security measure (or measures) would serve to lower an asset's vulnerability to a particular type of attack. For example, where a vehicle bomb attack is indicated, the installation of vehicle barriers might serve as a deterrent and installing a type of public access control system could reduce the possibility of a man-carried explosive being used against another asset. Installation of such security measures would lower the risk profile of the involved asset.

Reduction in vulnerability (the vertical axis) is frequently thought of as being achieved through installation of "site-hardening" physical security measures. While this is a logical way to reach the risk reduction goal, other means are also available and must be considered. For example, one of the elements of 'likelihood' is the target's attractiveness to the terrorist; changing that attractiveness is a means of reducing risk. Making a target too difficult to attack, or beyond the terrorist's weapon and resource capability, reduces the target's attractiveness and, therefore, "likelihood". Changes in established operational procedures can also serve to lower risk by making various aspects of the asset less vulnerable.

Risk can also be reduced by making changes in consequence (the horizontal axis). This is frequently done through duplication and/or dispersal of the asset. If destruction

of a particular asset represents a single potential point of failure in accomplishing the department mandate, then consideration can be given to duplicating that capacity and/or dispersing its functional purpose throughout multiple other elements or locations, in order to reduce that failure consequence. Measures that create duplication and dispersal of ability can extend the time during which an emergency service can continue to provide services in a crisis by ensuring a replacement or substitute capacity when a similar function is lost at another location. Note, however, that security measures which reduce consequence without changing the level of vulnerability of assets rely, in part, on the presumption that the terrorist element does not have the capacity to eliminate all of the vulnerable assets simultaneously or each in sequence. Thus, choosing mitigations that focus independently on reducing "likelihood/vulnerability" *or* "consequence/impact" alone can have the desired effect of reducing risk to the asset where they are applied; but a program that develops need-driven mitigations that reduce both these elements of risk (vulnerability and consequence), simultaneously and in coordination with each other, directly enhances overall security and supports the sustainability of the departmental services the asset provides.

Applied risk reduction measures that lower vulnerability can sometimes be dependent on various forms of technology. Departments must be sensitive to the degree of technological dependence created in addressing their risk reduction methods, particularly if the technology represents a single point of failure. If the technology fails or is overcome, the total consequence of the original vulnerability can occur immediately. The level of accrued technological dependency may not permit any time for initiating other measures to limit the full consequence.

In situations where technological dependency is acute, a program that trains personnel not to extend their operations to the extreme limits of the technology and/or provides alternate methods to achieve the objective, can serve to increase actual safety and available time to avoid the full consequences of any technological failure.

Whether the choice to reduce risk applies to vulnerability or consequence, or ideally both, it is important to remember that the mitigations and changes driven by the needs assessment should not be limited to physical and structural changes alone. Operational changes in routine functioning are often highly effective in reducing risk, usually involve less capital costs than physical changes, and can be applied more easily and often on a scale that varies according to the current local level of threat. It is often most effective to implement both physical and operational risk reduction efforts in a coordinated manner. It is in this area that changing response patterns as a result of specific terrorist conditions can be highly effective.

Return on Investment

Investments in counter-terrorism mitigations can be significant and as with all investments, must present a gain or positive return for the investor. The gain being sought in a risk assessment is the reduction of risk. It is that reduction which represents the return on this investment, and each mitigation must have a value in risk reduction with a direct relationship to the recognized threats. The cost of each mitigation method and/or a combination of mitigations, and their effectiveness and efficiency in gaining risk reduction per actual unit of cost, is a major issue for a department. By using pre-

and post-mitigation installation assessments, a department will be able to evaluate its overall security profile at any given time and the return on investment of its mitigations. It should be understood that the assessment profile and all aspects of risk respond to the nature of the threats, which can change over time. It is therefore beneficial for a department to periodically reassess its threat and risk condition.

Additionally, department management must consider the concept of "acceptable risk" in selecting which asset(s) are chosen, and in what sequence for mitigation improvement. Presuming that available funding in any given year will be insufficient to address the totality of mitigation needs, a department must choose how and where those funds will be expended. Logic would seem to dictate that the asset determined to be most at risk (see Diagram 3, Rescue Co./Small Explosive) would be the first asset to receive corrective measures, and each subsequent asset in the hierarchy would be addressed in turn according to available funding. Another method could be to collectively fund partial mitigation for a selected group of assets, or all assets simultaneously, thereby giving some protection to a wider group of assets rather than in-depth security to one. Regardless of which process is chosen, the gap between the optimum obtainable security condition desired, and that which current funding, technology or expertise permits, is the amount of 'acceptable risk' a department will have until conditions allow further mitigations to be applied or the threat itself diminishes.

Similarly, a department must guard against selecting a method of mitigation simply because it has the highest return on investment. Expending funds for that reason only, on an asset that holds a lower position on the risk assessment graph, leaves those higher ranked assets wanting for attention.

TRANSITION 2: Risk Assessment Informs Security Mitigations

Security Mitigations

The vast majority of calls that fire departments and emergency medical services respond to are accidental. That is to say, they are not intentionally caused. The exceptions of arson and other intentional criminal matters account for a select percentage of the total responses, but most departments consider such operational responses within their routine patterns. The idea that these emergency services may themselves be intentionally targeted is rarely considered or planned for. This is not to be confused with any existing plans for operating under dangerous conditions or in a contaminated zone; these plans envision *arriving at* an ongoing, unusual, or terrorist event wherein something else is the primary target. The concept being considered here is that of *emergency services being directly targeted and attacked* as part of a wider terrorist event. Departments have an awareness of time-delayed "secondary" explosive devices being planted for the specific purpose of impacting emergency responders upon arrival, but the intentional attacking of the services *prior to or concurrent with* a wider attack is not an event generally included in emergency planning.

There are numerous examples of terrorist attacks targeting security forces whose expertise could impede or deny the terrorists' attack objectives. Such actions as attacking command and control hubs, communications centers, hospitals, etc. that can

reduce the impact of the terrorist attack by rapid and effective use of a department's responding capabilities are such examples.[18] By neutralizing or minimizing that response capability the asymmetry of the attack shifts in favor of the terrorists.

Both captured intelligence evidence and past terrorist actions require that this intentional targeting potential be examined.[19] Causing death, injury, and destruction are some of the primary intentions of transnational terrorists. Terrorists have demonstrated that they can improve their effectiveness in those areas through the elimination or lowering of the response capabilities of local authorities.[20] Recent evolutions of such attacks, particularly in Mumbai, India, have clearly demonstrated that the terrorists were able to enhance the effects of their attacks through such means. Whether conducting pre-attack surveillance on emergency services, rehearsing attacks on responding vehicles, attacking police stations, commandeering emergency vehicles, or executing response commanders, there is ample evidence to indicate that such tactics are part of their overall planning.[21]

Emergency services must realize that they represent some of the most valuable and finite counter-terrorism resources in the country. This means that departments should highlight the need to secure their resources from attack and take the possibility of any diminished capability or capacity due to such situations into account in their policy development and response planning and budgeting.

Even if departmental resources are not targeted directly, multiple types of WMD terrorist attacks are capable of wide-spread injury, death, and destruction. Emergency services are not immune from such consequences. These types of attacks can seriously impact both on-duty and off-duty personnel, and equipment serviceability, simultaneously. Crisis planning considerations should examine the departmental response profile through a range of diminishing levels of personnel and equipment availability due to the direct impact of a particular type of attack on the resources of the department itself, or by its being effected by these WMD. There is a direct relationship between the number, and capabilities, of the remaining department resources following an attack, and the selection of which emergency operational functions are to be continued at which critical community locations. There is a "tipping-point" at which operations are unavoidably or intentionally diminished.[22] This point will vary from department to department. Note that a departmental capability should never be confused with its capacity. A department may have excellent training, equipment, leadership, and experience to address an event – even a terrorist event – but its ability to rapidly respond and sustain those operations over time or in simultaneous multiple attack scenarios is a measure of its capacity,[23] which can be dramatically reduced by WMD.

The above risk assessment process can identify which assets are most at risk from terrorist-type attacks and their current vulnerability profiles. In planning terrorist response operations, senior emergency management needs to consider actions and expenditures that will help ensure that their most valuable resources (frequently the ones most at risk) remain viable and available for use by the wider community during and after these emergencies.[24] Even a cursory review by senior management will often reveal that the entirety of a department's policies, practices, and particularly Standard Operating Procedures (SOP), have been created to function in a routine environment

and will therefore need to be completely reconsidered to ensure survivability in a terrorist attack. Physical site hardening of critical assets and the installation of access-limiting measures that create a secure zone in depth, as well as operational changes, are some of the basic steps that can be taken to help protect these resources. Such hardening is not limited to physical sites; it should include mobile resources as necessary. In every instance it is the selection of the correct mitigation or (more frequently) a combination of mitigations, chosen because they are directly mapped to a risk reduction need identified through the above risk assessment process, that will be the most effective in addressing security concerns.

TRANSITION 3: Security Ensures Resource Allocation for Terrorist Events

The above risk assessment process results in a department understanding the ways in which it is threatened by terrorism and which of its assets are most vulnerable to that threat. The process also identifies those assets that will need to be secured from those threats since they are the most necessary and critical for the department to carry out its mandate in the event of a terrorist attack. That understanding of all aspects of risk is necessary in order to examine and address a department's preparedness profile for responding to terrorism. One of the principle ways of determining preparedness is to understand the way a department allocates resources.

Resource Allocation

"What is our capacity to do what we do"?

For an emergency services department, the answer to this question is related to all the resources that attach to each of the department's critical assets, and all other assets, in order to accomplish the department mission. For example, a fire department may have twenty apparatus including pumpers, ladder trucks, ambulances, rescue vehicles, mobile command vehicles, etc. The number of them and the total number of personnel assigned to those operational functions, in addition to those in administrative functions, can give an indication of the department's response capacity. That distribution will reflect what local experience and practice has shown to be the appropriate number of resources necessary to meet the daily routine requirements of the department. Diagram 4 (below) demonstrates the possible assets and the number of emergency personnel distributed within a department.

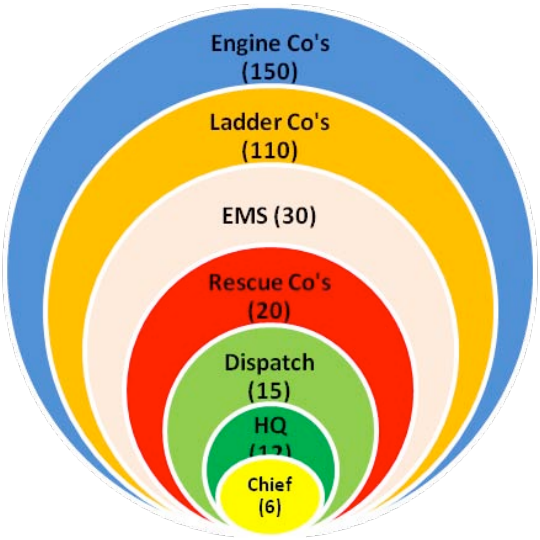


Diagram 4

"How do we accomplish our mission?"

The answers to this question generally involve training, command and control, response patterns, communication systems and data bases, liaison and mutual aid, etc. Knowing the answers to these questions permits a department to have an overarching view of its functional means and processes necessary to operate. Specifically, it will have an analysis of its daily, routine operations and how the department mandate is met.

"What resources, and in what numbers, will be needed to respond to each type of terrorist event?"

Diagram 5 (below) hypothetically lists an asset, the number of personnel assigned to that type of asset, and the types of WMD that asset will be called on to mitigate. (Diagram 5 is not intended to be comprehensive.)

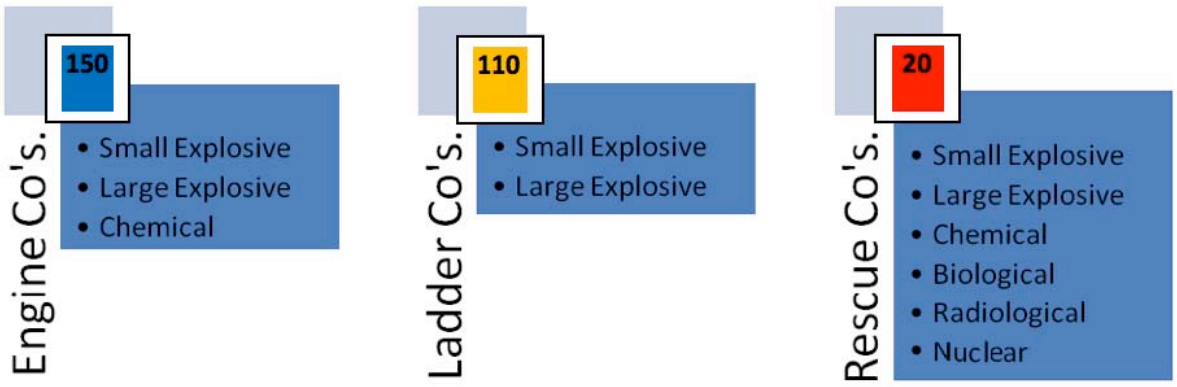


Diagram 5

Risk assessments (particularly in the response capabilities section) provide an analysis of critical issues and critical needs when operating in a *WMD* environment. The distribution of resources shown in Diagram 4 describes resource allocation for *routine* operations and functions.

As displayed in Diagram 5, the WMD response resource allocation needs are clear. The two diagrams (4 and 5) are dramatically different. In fact, the distribution of routine function resources (for example, personnel) may be nearly inversely proportional to the department needs in addressing the WMD terrorist threat. In Diagram 5, note that there are 150 personnel assigned to engine companies who can operate in response to three types of WMD attack, but only twenty rescue personnel available for addressing six types of WMD attack. Multiple, simultaneous attacks of this type would only serve to exacerbate this issue.

The reason for this disparity is that response to a routine matter and response to a terrorist/crisis event are two entirely different circumstances, requiring very different operational processes, abilities, and resources.

The expertise, equipment, and resources used most infrequently in daily operations will become some of the very elements in greatest demand during response to a terrorist event. Attempting to use the larger routine resources as a substitute for them during a crisis can/will result in great peril to those resources and an inadequate outcome for the conditions being addressed. This situation would be a crisis for the department.

TRANSITION 4: Terrorist Events Require Crisis Leadership Skills

The above description of a department's resources provides an indication of how it is prepared to respond to the full range of its mandated duties. But, as can be seen, those duties do not always consider the potential for terrorism within a department's response protocols. Similarly, the on-scene command and control of those resources may also not calculate the leadership issues – particularly the relationship between resource allocation, response patterns, and leadership present at a terrorism event.

Routine versus Crisis Response

Due to an emergency department's experience, training methods, management practice, and organizational structure and culture, the ability to recognize a crisis and to respond accordingly with methods specifically designed for a crisis (if such methods even exist) often develops too late in the course of the crisis to mitigate the issue. Unfortunately, for some the recognition does not come at all.

A crisis is often viewed is as a calculation of the size or scale of the event, but this is not always justified. For example, transmitting a fifth alarm for a fire, or calling up the police reserve, clearly signifies the occasion of a large-scale event. But this is not necessarily a crisis, inasmuch as the department has these existing methodologies and resources available to address the problem. In short, the department has a means in place to address large, but routine, matters. Conversely, a single police officer, suddenly engaged in a shootout with multiple armed subjects, is very much in a crisis status. Thus, size or scale alone is not always a legitimate measure for determining the presence of a crisis; there is a difference between routine – meaning something prepared for and

regularly addressed regardless of size – and a crisis, which is neither routine nor prepared for and can either evolve or be sudden and unanticipated.[25]

This ability to recognize the difference between routine and crisis conditions is a pivotal issue for emergency service leaders in a terrorist war environment.

Crisis Leadership

In studies of failure to manage crises, including those involving homeland security-type issues, Harvard's Kennedy School of Government has examined the crucial elements in decision making during situations that move from "ordinary" or routine, to "high consequence" or crisis conditions.[26] The point at which the routine (Status R), moves to crisis (Status C) is largely dependent on the amount of "novelty" in the situation and how quickly those in charge are able to recognize, and respond to, the novelty or newness of the situation. Status R is identifiable by its "familiar" elements and Status C by its "unfamiliar" ones. Individuals, institutions, and societies succeed or fail based on which set of elements is permitted to dominate the response in times of novelty or crisis.

Routine vs. Crisis Elements

Status R contains the following elements: a need for minor customizing; has standard operating procedures and clear objectives; has sufficient resources, policies, and laws; has sufficient training; has clear authority and organizational structure; is expert driven; has some unknowns; and plans are based on known threats.

Status C contains the following elements: it invalidates some standard responses; there is a mismatch between the problem and resources, policies, laws, and experience; it requires capability based planning; and it has "unknown unknowns."

Routine vs. Crisis Leadership

Status R leadership elements display: a familiarity with the condition; a substantive expertise with the issue; a consultative/directive style of leadership; demonstrated interpersonal skills ability; and a reliance on recognition-primed ("I've seen this before") decision making.

Status C leadership elements display: an expertise in multiple operations; a flexible "first responder" mindset; a strong personality; risk taking ability; a willingness to create a wide organization (a "sudden network"); rapid assessment of network abilities (evaluates resources); focuses the network (identifies what is important); decisiveness (takes command).

Recognizing Routine vs. Crisis Situations

A true crisis is characterized as an event which: has high stakes and high costs; is beyond existing resources; consumes available resources; has serious negative outcomes; entails a realization that a standard response is inadequate; and requires action that is urgent and imperative. There is a loss of control, the size and complexity of the situation is expanding, there is command and/or operational confusion, there is a lack of authority to act or too many authorities involved, it has high political and media attention, it is a unique occurrence or scale, it is beyond what has been prepared for, and there is a high level of uncertainty.

A "novelty" or crisis can also be characterized as a situation that changes from *categorized* to decentralized, *bureaucratic* to improvisational, *big picture control* to a possibility of risk, and from *familiar reliance* to a need for trust.

As the situation moves from Status R to Status C, the challenge is to not let the "R" people and/or methods maintain control according to routine practices, because the situation can no longer be overcome by using familiar methods. The main objective in overcoming a crisis is to apply creativity, improvisation, and rapid innovation – or prepared response patterns whose elements have that built-in crisis capacity as compared to routine responses.

The most common and systemic mistakes made by otherwise bright people in addressing crisis constitute cognitive failures which are most likely to occur under pressure. These mistakes are created by: over valuing one's own experience; believing in an illusion of experience (discounting what we haven't seen ourselves); and multiple forms of overconfidence, such as believing there is an understanding of the entire situation, all the facts are known, being able to make predictions, having a capacity to influence outcomes, and being able to control events.

Actions based on those types of cognitive failure are characterized by: continuing a commitment to an irrational action through escalation of that commitment; bounded awareness or focusing on the wrong things; over reliance on readily-available data; overconfidence; searching for data that confirms pre-conceived beliefs (a valid information bias); and an action orientation that has a preference to avoid risk (which in crisis only increases risk).

Routine vs. Crisis Indicators

Routine *(STATUS R)*	Crisis *(STATUS C)*
The situation is familiar	**The situation is a unique occurrence or scale**
Uses standard operating procedures	**Is beyond what has been prepared for**
Has clear objectives	**There is a high level of uncertainty**
There are sufficient resources	**The problem is beyond the existing resources and/or all resources are consumed**
The resources are the correct ones	**Resources do not match the problem**
The outcomes are expected and normal	**Has serious negative outcomes**
Authority and organizational structure is clear	**There is a lack of authority to act or too many authorities overlapping**
Is expert driven	**Experience is not equal to the task**
Plans are based on known threats	**Requires capability based planning**
Has some unknown conditions	**Has unknown unknowns**
Response needs minor customizing	**Invalidates some standard responses**
The threat level is normal	**There are "high-stakes" involved**
The cost is acceptable	**The cost is high**
Action time is normal	**Action is urgent and imperative**
Command is direct and obeyed	**There is command and/or operational confusion and a loss of control**
It attracts no or normal attention	**Has high political and media attention**
It can be contained with normal responses	**Has expanding size and complexity**

Diagram 6

What the generals were facing in the earlier warfare examples was a Status C situation which they were addressing with Status R process. Their actions represented a "cognitive failure" (as evidenced among other of the above indicators) by the fact that they were "continuing a commitment to an irrational action through escalation of that commitment." Reviewing the accounts of both battles and the nature of the wars in which they occurred, the descriptions of "crisis" and the failures to recognize the "novelty" of the situation that existed in the Harvard criteria are plainly evident, along with the failure of leadership to respond in an effective way partly due to their inability to recognize crisis.

Clearly, the British admiralty example is the opposite circumstance.

Routine vs. Crisis Leadership Skills

Routine (Status R)	*Crisis (Status C)*
Familiarity with the condition	**A flexible mind-set**
Has substantive expertise with the issue	**Expert in multiple types of operations and can rapidly assess network capabilities (evaluates resources)**
Has strong interpersonal skills and consultation/direction style	**Has a strong individual "take command" personality**
Reliance on "recognition primed" decisions	**Quickly recognizes the "novelty" of the situation. Is a risk taker and can focus the network (identifies what is important) and a willingness to create a wide organization (a "sudden network")**

Diagram 7

The principle hazard for emergency services in terrorist events (or other forms of crisis), in addition to the direct hazard of being targeted themselves by terrorists, is the failure to recognize the crisis condition for what it is, as rapidly as possible. Any command delay in switching from 'routine' to 'crisis' operations status can result in disastrous outcomes. Yet the very nature of emergency service response patterns and culture can aggravate this problem; i.e. departments do not traditionally have separate, prepared, and practiced "crisis" response protocols that the commander and operational personnel can switch to when the situation requires it.

Emergency services have well-established methods for managing large or expanding emergencies. This is most frequently done through sounding additional alarms, calling in mutual aid, applying the Incident Command System (ICS), etc.,[27] which is a universally accepted and practiced process. But a WMD crisis is not just another large emergency; it is a "novel" situation that must be immediately recognized and managed according to plans and response procedures designed specifically for these events. In fact, a routine plan (such as Mutual Aid or ICS) that facilitates an ever-expanding response and use of additional resources, might create the illusion of control and can serve to delay the critical command recognition that a crisis is occurring which requires a different type of response.[28] It is of primary concern that all departments develop such crisis awareness and terrorist/crisis-specific operational plans. This will serve to make

them more effective in a crisis in their own jurisdictions or when responding under mutual aid or ICS.

The discussion thus far has examined the nature of the threat, the consequences of an attack, and the need for changed response patterns to address those threats. However, the information developed also indicates that a department can do more than just "respond". It can also take measures to protect itself from being victimized by the terrorist attacks.

TRANSITION 5: These Issues are Addressed through Training and Plans

As can be seen from the above, for an emergency service operating in a terrorist environment, the relationship between threat, resources, leadership, and response patterns is an all important equation. The balance between these elements can be critical to the department successfully achieving its mandated objectives. That balance is gained by making the necessary changes to each of these elements in relation to the others, and it is within the department planning and training programs that the most significant and effective changes can occur and must begin.

Training Systems

Emergency services train their personnel to operate within a practiced and coordinated system and process designed to be highly effective and efficient. Significant amounts of time and money are allocated to ensuring that every member of the department is fully aware of his or her duty, and has the knowledge and means to execute those duties properly. The nature of emergency work is such that repetitive conditioning through training and exercises ensures that each member will respond to a situation in a manner that has been tested and shown to be effective in gaining the desired outcome. The training is often conditioned to the point of individual operators responding instinctively. This methodology is designed to create teamwork and organization that focuses all resources on achieving the desired outcome in the most effective and efficient manner. This orchestrated response pattern is nearly universal and contains within its normal parameters the capability to meet and address expanding emergencies. In short, training methods condition personnel to address situations that have known best practices available, regardless of the scale of the event.

These training programs are experiential at their core. Many years of analysis of what happened, what worked, and what proved to be the best solution has evolved into Standard Operating Procedures (SOP). It is absolutely mandatory that such methods be developed and applied in daily operations because they represent the collected knowledge of years of experience that result in the most effective and efficient means of responding to an event. These events that training addresses vary by location, frequency and scale, but the thing that remains constant is that, regardless of these dynamics, all are familiar events. The very fact that training protocols exist for these conditions is *prima facie* evidence that the condition is a known occurrence for which best practices have been derived through experience. The vast majority of all emergency services rely on the effective use of these inculcated response patterns by their personnel to carry out

the mandate of the department. Such training is at the core of effective emergency management practices for *routine* events.

Unfortunately, the SOP can also lead to response patterns in individuals and organizations that become more automatic and habitual rather than considered. It is this reliance on routine actions that can be a primary issue in growing a crisis into a disaster. Reliance on known event parameters, and a matching response pattern by a department and every individual in it, reflects the core strength of the organization and can also become its greatest weakness.

The longer the delay in recognizing that a crisis is occurring, and then changing response patterns accordingly, the worse the outcome can be.[29] It must also be understood that even if a leader recognizes the existence of a crisis, but has only routine resources and response processes available to use, that leader will be overmatched and forced to rely heavily on improvisation, which will meet with limited success and duration.

Therefore, the pivotal factors in addressing crisis are *situational awareness* (having knowledge of the totality of an event), the amount of *time* that has elapsed before crisis recognition is made, and having specific *crisis response plans available*. All these issues can be managed by training programs.[30]

Training Sources

Just as SOP are created by experience, the fact that only a select few domestic emergency services have first-hand terrorist operations experience precludes the ability of others to develop new response patterns from their own knowledge. Those departments that do have such experience most likely dealt with a singular event, which is certainly not sufficient to draw upon for response plan development for the full range of terrorist-type attacks. Limited experience can tend to isolate and focus departmental thinking to anticipate a repetition of what has happened to them previously, causing them to develop too narrow a plan.[31] It is therefore mandatory that terrorist-based response patterns be developed by accessing the wealth of information that has been gained as a result of decades of worldwide responses to these events.

While the attempted New York Times Square car bombing, in May 2010, initially appeared routine, several issues created a note of caution for responding units: Times Square is clearly a high value, iconic target location; the vehicle was hastily left in a marked pedestrian cross-walk rather than in a parking space; there were unusual "popping noises" coming from the vehicle; there was white smoke without heat; and the vehicle was immediately abandoned by the driver.[32] None of these factors individually might be sufficient to trigger a heightened awareness on the part of the responding units, but in the aggregate, where crisis training protocols are comprehensive, they serve to give warning that a possible terrorist event is underway. It is understood that initial responding units rarely have full information about the conditions they will encounter and can therefore be drawn into an environment they would otherwise avoid. That lack of information is one of the cautionary indicators of crisis that enhanced training can include.

As previously noted, one of the keys to successful crisis management is the ability on the part of the personnel involved to recognize that the environment they find

themselves in is in fact, a crisis.[33] It may seem odd to suggest that experienced individuals might not recognize the novelty of their situation, or that it is actually a crisis, but the historic military examples given previously are only representative of numerous such examples across the full range of human experience, including the emergency services. Inasmuch as modern terrorist objectives bring a form of warfare into the realm of the emergency services, it is imperative that those services be prepared to address and counter these events with training and preparations at a level, and on a scale, that have previously been thought of as matters confined to war and military leaders and decision makers.

Training Curriculum

Training for Crisis Leadership

Any crisis can also contain "routine" elements that will be familiar to an experienced leader. The presence of such elements can cause a cognitive failure, where the leader focuses on the wrong things (a bounded awareness) and develops a myopic view of the entire situation. The leader is in danger of making overly focused decisions that rely on "recognition primed" thinking, when in fact the entirety of the environment calls for decisions that cannot be judged by experience alone.[34]

Operational leadership training programs that rely on stress-inducing scenarios to test a commander's ability to acquire, distribute, and utilize ever-expanding resources, serve to accustom that individual to managing a wide range of disparate facts and details simultaneously.[35] It is essentially a test of the individual's ability to manage the growing minutiae of an incident. Such repetitive attention to the management of details can occur at the expense of overall situational awareness and unacceptably extend the time it takes to recognize that a crisis condition exists.

Inducing stress can be an effective teaching method, but it must be counter-balanced with a process that teaches the leader to regularly detach from issues of detail in order to rethink and re-evaluate the totality of the operation in order to recognize crisis situations sooner and to take appropriate action.

Alternatively, resources permitting, a secondary leader can be assigned the duty of continuously monitoring and evaluating the entirety of the situation rather than its minutiae, and serve as an assistant/advisor to the commander. Such a position would provide the commander with a second source of warnings, cautions, and critical advice in determining the existence, and managing, of the crisis.[36]

Providing Crisis Response Tools

At the heart of the matter is the fact that due to the lack of specific crisis response status training, let alone counter-terrorist training, even if emergency personnel do recognize that they are in a crisis, they are left with no other methodologies for response available to them other than those designed to address routine conditions.

Clearly, because of the culture of these organizations, their personnel are highly innovative and will quickly regroup and reorganize in a way that eventually develops a successful, if limited, path for them to follow. However, in the face of an enemy that has factored emergency service methods and capabilities into its attack plans, the terrorist overmatching of the department response capabilities may cause that innovative

response pattern to be ineffective or to come long after the terrorist's objectives have been met. In short, departmental innovations may come at a time when they can be applied to the "recovery" phase, rather than during the crisis management part of the event. Thus it is manifest that the amount of time expended to first become aware of the crisis situation, and second to apply alternative procedures to counter the crisis, are two critical issues in regaining control of the operating environment.

It is insufficient to train personnel to recognize the presence of a crisis, but not have crisis protocols and/or response patterns for them to utilize during the crisis. As noted above, such a situation will leave the leaders and other personnel relying on innovation and improvisation alone to address the situation. While emergency service personnel are often innovative by nature, the ability to innovate (which is different from improvisation) is a highly personal and singular matter. Given similar circumstances, or even separate parts of the same incident, an innovative response that is dependent on the variables of personal ability and preference can result in drastically different outcomes for the same conditions. In the absence of crisis protocols, opportunities for innovative and/or improvisational response will soon be overmatched by the growing crisis condition. Additionally, recognizing that improvisation requires spontaneous and rapid reorganization and instruction, significant modification of protocols, and the use of tools, equipment, and technology for purposes for which they were not intended, means small chance for success of continued and repetitive improvisation during a crisis.

Routine Training and Crisis Training

A training program that establishes an additional crisis response training course parallel to the routine matters course can start to address the modern form of terrorist warfare in its operational area. In essence it means providing instruction in two different forms of thinking and operating, based on threat recognition. Traditionally, emergency services do not teach multiple, alternative forms of operations and the departments' themselves are not organized, managed, or equipped to function along parallel tracks. This, however, is the very functional condition that effectively combating transnational terrorism has imposed upon emergency services.

The first step in establishing a crisis training regimen is to instruct all personnel to recognize the signs that differentiate crisis (Status C) from routine (Status R). It is then necessary to have a command and operations structure that is authorized and capable of immediately changing the department from routine to crisis operations and administration as soon as the crisis is recognized. Most importantly, it is necessary for the training and command entities to have established crisis policies, plans, procedures, and resources in place that can be substituted during crisis for the now inadequate routine methods.

This is not to say that routine procedures become discarded or obsolete; it is within the scope of the department mandate that an emergency service will continue to respond to other routine matters concurrent with the crisis occurring. However, the crisis use of available resources will severely impact the scale and ability of the department to respond to the routine matters, requiring significant modification to existing routine response patterns as well.[37] It is this requirement to maintain both forms of response in parallel that will have a significant impact on policy changes. The

intensity and level of threat will determine if a department uses dual, parallel response patterns for routine and crisis matters simultaneously, or chooses to use crisis response mode for all activities to counter the potential consequences of sudden terrorist events leading to injury and loss of department personnel in such an environment.

RESPONSE PLANNING

The modification of all of the elements of an emergency services department discussed thus far is driven by understanding the nature of the threat and the relationship of each of the departmental elements to the other. Changing all of those relationships in a balanced and cohesive manner, utilizing the sequence of transitions described above, will require a department to develop detailed plans based on the consideration of thoughts and issues about terrorism that may not currently be included in the overall management vision. Department leaders must consider a wide range of new and changed issues.

Planning Considerations

Simultaneously considering altered and/or random, non-traditional response patterns, set to specific types of events, can enhance the potential security of a department's and a community's valuable resources. A response pattern structured to meet current, factual conditions rather than future, presumptive environments, can result in both successful and acceptable outcomes within the dynamic created by these terrorist environments.

Similarly, a review of policies based on administrative and legal matters may reveal the need for additional authority or relief from certain other requirements, in order to fully function in this changed environment. Virtually every area of a department's functioning – from contracting to recruiting, equipment purchasing, supply management, communicating, housing, and promotions, etc. – can be modified to update and enhance a department's security and operational capabilities profile both during, and in the aftermath of, one of these incidents.

As the threat of terrorist activity increases, through various notification means we have come to recognize (such as the yellow to orange, orange to red, etc.) a department can order different types of operations. For example, "Secure Response Conditions" under "orange" conditions can mean changing response routes, responding only with police escort,[38] blocking private vehicles from transiting roads used by critical departmental assets, etc.

A further heightened threat level may result in a "Limited Service Response Condition" wherein departmental resources are retained away from critically hazardous or ongoing situations until such time as the immediate danger passes. This response can also serve to ensure the survival of those resources for use in protecting the wider community.[39]

Such overarching departmental policy and training alterations do not come easily. The realization that every aspect of a department culture will undergo some change is a significant concept to grasp and adjust to. It is also probable that those very individuals on whom this change-management task will fall are the same individuals who have the longest association with the reliability of the established routines. Conversely, they are also the individuals who have the greatest knowledge of the department and all its

networked aspects. They should therefore be the most capable of identifying and coordinating all the cause-and-effect relationships that a modification of one element will require in all the other elements.

The sequence of the risk assessment, threat-based resource allocation process, crisis leadership issue, and training needs alluded to earlier can serve as the pivotal guide in managing these terrorism-motivated departmental changes. As a department enters into this process it is worth noting the following items:

- A conceptual model for dual routine and crisis thinking and management can be found in the military practice of designating a "General Quarters" condition. All routine matters cease, all personnel change immediately from a routine to a crisis mind-set, and all operations, equipment, resources, and response patterns become crisis condition-based for the duration of the situation.
- Ensuring the security of critical assets before an incident will positively contribute to the availability and sustainability of those resources during and after a terrorist event and crisis.
- Planning for crisis by starting with current departmental conditions and resources and working to evolve into a crisis-ready format may not be efficient. Consider deciding on the desired departmental outcome or 'end-game' for operating in a terrorist-induced condition, and work backwards to determine what training, procedures, and equipment need to be developed in order to ensure the department's desired outcome. Also calculating potential departmental losses created by the terrorist event will help determine the priority and scope of subsequent operations and departmental capabilities.[40]
- Do not project personal or departmental standards of behavior onto the terrorists' planning and practices. Instead, rely on the stated objectives of the terrorists themselves to anticipate the issues that need to be addressed. Rather than trying to predict specifics, use the change in preparedness and the improved ability of the department to meet and counter the terrorist objectives as the measurement of reorganizational success.[41]
- It is of primary importance that each department member not only knows his or her individual responsibility in the crisis procedure, but also what is the intended purpose and outcome of the operations plan in total. This is done so that every member can continue to work to achieve that outcome despite any mishaps or plan failures caused by the terrorists. This allows leadership initiative to surface during crisis.
- Do not plan to counter what the terrorists *are going to do* – this is a presumption based on knowledge of their past actions. Absent any specific knowledge of actual plans, departmental thinking and planning from this basis seriously limits the potential to create operations and security measures that can be highly effective against terrorist attacks. In essence, this is "planning for the last war" and is an example of a hindsight bias. Instead, plan for what the terrorists *are capable of doing*, which is based both on their past actions and current capabilities, using knowledge provided by the department's intelligence agency partners. Such

thinking will keep the department current with the latest threat, and ensure that mitigations and plans serve to match or overmatch the terrorist abilities, thereby reducing departmental assets' target attractiveness.

CONCLUSIONS

Traditional emergency services are operating in the front lines of combating and responding to terrorism. The response protocols used by these departments are based on routine emergencies and are insufficient to meet the direct threat of terrorist incidents. In order to understand and meet the current level of threat, these departments must re-examine conditions, security, and response capabilities through a series of steps beginning with a comprehensive risk assessment. Emergency services departments must ensure the security of their personnel and critical assets, re-define the allocation of resources, prepare for crisis leadership, and develop training methods and response patterns that reflect the nature of the current threat environment. These elements must be viewed as a continuum of inter-related parts of the same problem, rather than individual, independent issues. Creating threat-based response patterns will challenge all the assumptions on which current routine-based response patterns exist.

Command personnel charged with developing these protocols must resist the temptation to fall back on what has been done previously under routine response conditions. In fact, many of the protocols developed to respond to a terrorist threat will seem to be the antithesis of the very culture of the department itself and may be met with significant resistance both internally and externally. All the parties involved must understand, be trained, and be prepared to operate in both routine- and crisis-status situations that are different, because a terrorist crisis condition *is* different from the daily, routine condition. The current reality of the terrorist threat and departmental risk exposure requires that a prepared emergency services department make these changes.

By starting with an understanding of the current terrorist threat, and using the knowledge gained in each step of the above processes to inform the successive steps, a department will overcome the parochial approach to developing its response patterns. A department can become informed and transformed to counter the terrorist threat, protect its personnel, fulfill its mandate, and continue to serve the community it protects in this new terrorist environment.

Robert T. Mahoney is a retired FBI agent who served as the national manager for all FBI Special Operations Groups, assistant legal attaché for terrorism in London, and acting assistant special agent in charge in New York. He was in the World Trade Center on September 11th and a supervisor in the FBI Crisis Command and Recovery Center thereafter. After retiring from the FBI, Mahoney was a team leader in the development of the WMD Terrorism Threat and Vulnerability Assessment process for Critical Infrastructures, and general manager of security programs for the Port Authority of New York. He holds a master's degree in education and another from the Naval Postgraduate School in national security studies. Mr. Mahoney may be reached at r.mahoney@manageemergencies.com.

[1] United States Congress, *Homeland Security Act of 2002*, Public Law 107, 107th Cong. (November 25, 2002), 6 USC.101, Sect. 2, http://fl1.findlaw.com/news.findlaw.com/wp/docs/terrorism/hsa202.pdf

[2] The White House, *Homeland Security Presidential Directive 8*, *National Preparedness* (Washington, DC: U.S. Department of Homeland Security), 1 (2.d), http://www.dhs.gov/xabout/laws/gs_1215444247124.shtm#1

[3] S. W. Sears, *Landscape Turned Red* (New York: Houghton Mifflin Company, 1983).

[4] S.L. A. Marshall, ed., *The American Heritage History of World War I* (New York: American Heritage Publishing Company, Inc., 1964).

[5] R.K. Massie, *Dreadnought* (New York: Random House, 1992).

[6] National Consortium for the Study of Terrorism and Responses to Terrorism, *Global Terrorism Database* (University of Maryland, College Park, 2009-2010)2010, july 8), www.start.umd.edu/gtd/search/results.aspx?page=1&casualties_max=&target=3&charttype=live&chart=overtime&ob+GTDID&od=desc&expanded+yes#results-table

[7] A. Rabasa et al., *The Lessons of Mumbai* (Santa Monica, CA: RAND Corporation, 2009).

[8] The National Commission on Terrorist Attacks Upon the United States, *The 9/11 Commission Report: Final Report of the National Commission on Terrorist Attacks Upon the United States* (New York: W. W. Norton & Company, 2004), 150.

[9] R. Windrem, "Al-Qaida's NYC Surveillance Video Release," *MSNBC,* June 15, 2007, http://www.msnbc.msn.com/id/19254592/ns/nightly_news/print/1/displaymode/1098

[10] Rabasa et al, *Lessons of Mumbai;* S. Gale, L.A. Husick, and L. Rabinow, *E-Notes Messages from Mumbai: Terrorism and Policy Implications* (Foreign Policy Research Institute, January 2009), 1-2, http://www.fpri.org/enotes/200901.galehusickrabinow.mumbai.html.

[11] Fire Department, City of New York. (2010). *Textbook Response at Times Square Car Bomb Incident,* Supplement No. 23 to *Department Order No. 35*, 2.1.1 (New York: New York City Fire Department, 2010).

[12] Ibid., 10.

[13] U. S. Department of Homeland Security, *Risk Management for Special Needs Jurisdictions* (Washington, DC: Office of State and Local Government, Coordination and Preparedness, Office for Domestic Preparedness, n.d.)

[14] U. S. Department of Homeland Security, *Attack on Pakistan Police Academy Highlights New Terrorist Emphasis on Small-Arms Tactics* (Washington, DC: Office of Intelligence and Analysis, 2009).

[15] Bureau of Justice Assistance, *Fusion Center Guidelines-Developing and Sharing Information in a New Era* (Washington, DC: U. S. Department of Justice, Office of Justice Programs, 2006).

[16] T.G. Lewis, *Critical Infrastructure Protection in Homeland Security* (Hoboken, NJ: John Wiley & Sons, 2006).

[17] Kimberly I. Shoaf, Hope A. Seligson, Samuel J. Stratton, and Steven J. Rottman, *Hazard Risk Assessment Instrument* 1st ed. (Los Angeles, CA: UCLA Center for Public Health and Disasters, January 2006).

[18] National Consortium, *Global Terrorism Database.*

[19] Windrem, "Al-Qaida's NYC Surveillance Video."

[20] U. S. Department of Homeland Security, *Ambush-Style Tactics Used Effectively Against Sri Lankan Cricket Team in Pakistan* (Washington, DC: Office of Intelligence and Analysis, 2009).

[21] Rabasa et al., *Lessons of Mumbai,* 21, 22.

[22] B.A. Jackson, K.S. Faith, and H.H. Willis, *Evaluating the Reliability of Emergency Response Systems for Large-Scale Incident Operations* (Santa Monica, CA: RAND Corporation, Homeland Security and Defense Center, 2010).

[23] Fire Department, City of New York, *Terrorism and Disaster Preparedness Strategy* (Brooklyn, NY: Fire Department, City of New York, 2007).

[24] McKinsey & Company, *McKinsey Report – Increasing the FDNY's Preparedness* (New York: FDNY, 2002).

[25] N.N. Taleb, "Learning to Expect the Unexpected," *New York Times*, April 8, 2004.

[26] Author's notes from Leadership in Crises course at Kennedy School of Government, Harvard University, April 2007.

[27] G.A. Bigley and K.H. Roberts, "The Incident Command System: High Reliability Organizing for Complex and Volatile Task Environments," *Academy of Management Journal* 6 (December 2001): 1281-1299.

[28] District Fire Chief M. McNamee, interview with author, July 23, 2008, Worchester, MA.

[29] Ibid.

[30] R. T. Mahoney, "Deciding Who Lives: Considered Risk Casualty Decisions in Homeland Security" (master's thesis, Naval Postgraduate School, Center for Homeland Defense and Security, December 2008), 186.

[31] Gale, Husick, and Rabinow, *E-Notes Messages from Mumbai.*

[32] Author's notes from FDNY Battallion Chief's Command Course, Fire Department of New York, June 2010.

[33] Deputy Fire Chief V. Dunn (ret.), interview with author, June 26, 2008, 20.

[34] Author's notes, Leadership in Crises.

[35] FDNY "Battallion Chief's Command Course".

[36] Ibid.

[37] McKinsey & Company, *Increasing the FDNY's Preparedness.*

[38] Rabasa et al., *Lessons of Mumbai,* 11.

[39] McKinsey & Company, *Increasing the FDNY's Preparedness.*

[40] Jackson, Faith, and Willis, *Evaluating the Reliability of Emergency Response Systems.*

[41] N.N. Taleb, N. N., *The Black Swan* (New York: Random House, 2007).

Homeland Insecurity: Thinking About CBRN Terrorism

Albert J. Mauroni

As the U.S. government has seen a change of administrations, there is an opportunity for a constructive review of how the Department of Homeland Security (DHS) has addressed the threat of chemical, biological, radiological, and nuclear (CBRN) terrorism in terms of policy development and execution to date. Our current homeland security approach to CBRN terrorism seems to have its basis in the incidents of 9/11 and the U.S. anthrax attacks in October-November 2001. However, our history of homeland defense goes back to 1941 (at least); to understand from a policy perspective how the government ought to address domestic CBRN terrorism, we need to put it all in context.

This essay examines the issues of how DHS has prepared for chemical, biological, radiological, and nuclear terrorism incidents. DHS should address these threats in a consistent and holistic manner, but instead the federal government has developed singular hazard-based approaches to each threat. DHS has not assessed its efforts to address CBRN terrorism or identified where DHS could improve, and as a result we see merely the continuation of previous initiatives. The essay concludes with some recommendations on how DHS could improve this area with better policy practices.

Words Are Important

The term "WMD" was the word of the year in 2002, but quickly fell into abuse as a term of political rhetoric and comedic punch lines. It was originally developed in 1948 by the United Nations as an accepted arms control term to describe the nation-state use of nuclear, biological, and chemical weapons. But today, the term means different things to different people and agencies. For that purpose, I'm going to take some time to define my terminology.

The military defines WMD as nuclear, biological, or chemical weapons that can cause a "high order of destruction." I would add to this definition that the intentional use of these weapons needs to cause mass casualties, defined as more than one thousand injured or dead, during a single incident. I disagree with the FBI's use of the Title 18 U.S. Code definition of WMD because of its deliberate lack of reference to the scale of the incident. To the Department of Justice (DoJ) lawyers, any amount of CBRN or explosives, no matter how small, constitutes a WMD. Even innate devices or hoaxes can have WMD aspects.

The presence of mass casualties is a key aspect of the WMD incident, but "mass casualties" is an undefined and nebulous phrase. In general, people use the term to describe a situation in which there is one more casualty than the number of available

hospital beds in the local area. Because we want to focus on the federal response, we need to quantify that number to understand what federal actions are adequate. The Department of Health and Human Services (DHHS) chose the number of 1,000 injured or dead people for the trigger for its Metropolitan Medical Response Forces.

In my mind, the term "WMD" is only useful as an arms control term. It is often used by international agencies and government officials to discuss a particular class of unconventional weapons. However, the United Nations wanted to keep the term open to other forms of technology that might equal nuclear weapons in the scope of their destructive force, so I'm not against consideration of high-yield explosives, directed energy lasers, or other weapons that could *realistically* cause mass casualties. Ricin and botolinum toxin, often used in small amounts for assassinations, are not WMD. Airplanes used to cause mass casualty events are not WMD. Pipebombs and grenades are not WMD.

There is a distinction between nuclear, biological, and chemical (NBC) weapons and CBRN hazards. This is probably more of an issue for specialists than for laypersons, but again, words are important. The term "NBC weapons" should cause one to take into consideration that a nation funded its top scientists and engineers with millions of dollars and built numerous facilities to develop and test special weapons that had definable characteristics and expected outcomes. The military developed operational specialists who could use these weapons on the battlefield for the purpose of causing measurable operational effects. This is where we got our nerve agents, our anthrax and smallpox weapons, and nuclear missiles and bombs.

These weapons were not developed casually, nor are they "immoral." They were developed because they could, in fact, kill large amounts of people or disrupt operations, causing an advantage for the side using them. That's what military forces do. The immorality comes in when the weapons are causally used and noncombatants suffer as a result, just as with any weapon system. Nonetheless, the world community has developed arms control treaties to regulate the use of these unconventional weapons, and the U.S. government has agreed to comply with these treaties.

One needs to be careful about how we use the term "chemical weapons." The military has always been careful to note the difference between munitions with chemical components, such as riot control agents, herbicides, and incendiaries like napalm, and toxic chemical munitions, like sarin nerve agent and mustard agent. Again, this is because of arms control agreements intended to guide nation-states during wartime. It is not against international law to use tear gas, herbicides, or flame munitions.

CBRN hazards, on the other hand, reflect a more general threat in which certain physical compounds could harm individuals through direct exposure, whether inadvertent or deliberate. The key here is that CBRN hazards do not have to be used in great quantity or to result in mass casualty events to be a concern to the public. It

benefits us, however, to narrow down the definition of what CBRN hazards are. There are literally tens of thousands of potential chemicals that could harm an individual through direct exposure. Even water has a material safety data sheet. The serious threats include toxic inhalation hazards like chlorine and phosgene, not chemicals like mercury or sulfuric acid. Anti-plant or anti-animal diseases are not so much a concern as are a limited number of pathogens and toxins that are particularly contagious or lethal to people. There is a short list of radioactive material, such as highly-enriched uranium, plutonium, and cobalt that cause people significant concern.

I don't like the term "CBRNE" because that's an antiterrorism term, not a WMD term. The military police and emergency responders within the DOD antiterrorism community started using "CBRNE" in the late 1990s because of numerous terrorist incidents such as the bombing at Khobar Towers, the Oklahoma City bombing, and the Aum Shinrikyo's Tokyo subway incident. But the antiterrorism community really doesn't worry about the "CBRN" as much as they do the "E." When it comes to assigning resources and time to the most credible threats, the more probable threat of explosives wins over CBRN hazards every time.

THE EVOLUTION OF HOMELAND SECURITY

There's a good publication within DHS that describes the history of civil defense and its morphing into what we now know as homeland security.[1] I don't intend to go through the long linage of that effort, except to note two things. First of all, it's not a static history. Different administrations viewed civil defense/homeland defense in different ways, and they moved around the responsibilities from office to office. This is a natural part of policy development and maturation, where people can assess how the programs are going and where they need to be. That's something that I've hoped would happen more within DHS since its inception in 2003, and I'm not sure that this assessment has really taken place.

Second, there has been a change in the focus as to what the federal government's responsibilities are with respect to addressing civil defense/homeland defense roles. Initially, the federal government saw its role strictly as providing a response to the intentional use of military weapons against U.S. cities and noncombatants. First it was the fear of German and Japanese bombers and missiles hitting U.S. cities on the coast. Then it was the threat of Soviet bombers and missiles. But the congressional response was not to spend great deals of money on this threat. Over time, the state and local officials were not as concerned about the possibility of external attack as they were the power of Mother Nature. Congress, influenced by those state and local officials, decided it was more important for the federal government to respond to states and locals

affected by natural disasters and accidents rather than external threats. That balance was rudely jarred after 9/11, and we have yet to re-establish a more balanced view.

Using Public Policy Methodologies

There are policy analysts, such as Charles O. Jones, who have developed methodologies to examine how the federal government addresses specific issues, whether these functions are appropriate, whether they are being adequately executed, and whether the people in charge are addressing the challenges that are presented. Homeland security and national defense are two important public policy issues, and yet it seems rare to see any honest, intellectual assessment of the particular projects the government is executing.

Using the Jones model outlined in "An Introduction to the Study of Public Policy,"[2] there are four specific players involved in any public policy issue. There are the decision-makers at the top ranks of executive agencies who are responsible for developing rational policy for areas under their mandate, such as the DHS under secretaries and assistant secretaries. There are the technical agencies that have to implement an aspect of these public policies, such as FEMA or the Coast Guard or Fire Services. The state and federal politicians are never quite comfortable with wide, sweeping actions, so they implement policies in small increments rather than addressing reforms in bold strokes. Finally, there are the reformists who demand immediate actions despite legal or financial challenges. The activists for homeland security exist on both the right and the left, especially on issues such as missile defense and border control.

This model can assist in identifying the challenges in how DHS is executing its responsibilities for addressing CBRN terrorism. For instance, on occasion, one might find the policy-makers (rationalists) directing agencies (technicians) on how to do their jobs in great detail rather than developing policy issues (which is hard). And because those policy issues need to be laid out before the challenges are addressed, the subordinate agencies end up making policy directives that are ineffective because the technicians don't have a view of the entire policy issue from a higher level. Congress ends up being influenced by activists and create grand initiatives, but only incrementally fund them. And the challenges pile up.

Seeking National Guidance

The recently released *National Security Strategy* defines its homeland security approach as addressing a number of significant challenges.[3] There are the generic "threats" to American interests, the emphasis over maintaining our borders and to stopping the transit of "hostile actors" who are either bringing illegal trade into our country or who are intent on causing harm. The ever-present focus on terrorism is plain, but less so the emphasis on natural disasters and whatever "other hazards" entails. The

National Security Strategy provides the basis for developing public policy for homeland security.

We can argue about what homeland security is and isn't, but it should be clear that it is a broad area covering multiple issues and overlapping concerns where the public might expect the federal government to play a role. In responding to natural disasters and catastrophic incidents, there was the Federal Response Plan to explain how the federal response will address state and local emergencies. This was followed by the National Response Plan, and now we have the National Response Framework and National Incident Management System. Deliberate CBRN hazards and WMD incidents are one subset of the overall national response framework, but we do spend an awful lot of energy discussing these very low-probability, high-consequence events.

There are a number of national strategy documents that address CBRN terrorism concerns. I don't intend to go into each one, but these documents have been the basis for explaining how our nation will execute its plans and develop capabilities for particular aspects of CBRN terrorism response. The federal government does not often distinguish between the approaches of how the military addresses adversarial use of NBC weapons on the battlefield from how terrorists use CBRN hazards against noncombatants. This is a serious flaw. We don't lack for top-level guidance, but determining what one can do given unclear guidance, budgetary limits, and limited areas of responsibility, can be challenging.

As an example, Presidential Policy Directive 2, a national strategy to "counter biological threats" just came out in January 2010. It purports to address all biological threats, whether natural or deliberate, under a sweeping architecture of efforts. At a recent meeting, one person stated that the only difference between naturally-occurring infectious diseases and biological warfare agents was "intent." Such a statement could quickly lead to miscommunications as to who's in charge of what and whose funds ought to be used to address the problem. This casual approach doesn't help to identify the roles and responsibilities for responding to bioterrorism within the federal government.

U.S. GOVERNMENT STRATEGIES TO ADDRESS CBRN TERRORISM

When we examine federal responses to CBRN terrorism, there is a tendency to confuse what the DOD does to protect its forces from NBC weapons and what DHS does to support state and local responses to CBRN incidents. This hasn't been helped by the confusing, high-level guidance in the *National Strategy to Combat WMD*, which was released in 2002.[4]

We've seen a deliberate change of philosophy in how the federal government addresses CBRN terrorism before and after 9/11. Before 9/11, it was a law enforcement exercise that DOD supported as requested. After 9/11, it became a military responsibility

to pre-empt the terrorists, with less attention as to the adequacy of civilian response. But due to a lack of clarity over roles, missions, and responsibilities, we see a continued debate over who's supposed to do what to whom in both areas. We talk about using a "whole of government" approach to CBRN terrorism, often focusing on the efforts of DOD, DHS, and DHHS (and other federal agencies). But this also commits the sin of blurring the difference between military operations and homeland security.

Overall, there are many responsibilities across the government when it comes to addressing domestic CBRN terrorism. No one should be surprised by the long list of involved federal agencies. The broad responsibilities are pretty well known – it's the inter-agency coordination and actual implementation that's the challenging part. There are a lot of people doing different things, and it's sometimes hard to put the pieces all together. This article will focus on the DHS responsibilities and programs, but certainly, the discussion could continue as to other federal agencies that are involved in CBRN terrorism response.

Counterproliferation versus Counterterrorism

There is a National Counterterrorism Center (NCTC) and a National Counterproliferation Center (NCPC). Both address WMD issues, but from differing perspectives. The counterproliferation community largely focuses on nation-states and the means of producing WMD materials and technology, and works long-term policy initiatives. The counterterrorism community focuses on tracking violent extremist groups who may be seeking WMD materials and technology and their activities operating outside of nation-states. Both communities are looking for similar hazards, but from different perspectives, using different agencies and different funding. They don't work as well together as they probably should, but that's because they have different agendas. There is a gap.

There are those people who believe we should force the two communities to work more closely together – that we ought to eliminate the gap between the agencies. I don't agree. While the two communities use similar intelligence sources and may be looking at similar regions in the world, they are fundamentally different. I don't believe in the popular assumption that terrorists are actively working with "rogue nations" to exploit WMD materials and technology. The evidence isn't there. Nation states invest heavy amounts of people and funds to develop specific unconventional weapons, and if they were to give or sell them to terrorists, one of two things could happen – either the weapons would be traced back to them, or the weapons might get used someplace where the nation state regrets.

Terrorists get their material and technology where they can, from the local economy. They don't have the time, funds, or interests to get exotic. That's what we see, over and over again. The NCTC noted that, in 2008, there were approximately 11,800 terrorist

attacks resulting in more than 54,000 deaths, injuries, and kidnappings. Nearly all were caused by armed assaults, bombings, suicide attacks, kidnappings, and other conventional forms of assault.[5]

Early Efforts to Address CBRN Terrorism

In 2003, DHS began developing its CBRN terrorism response efforts by basically copying the DOD's CBRN defense concept. This included recommending the use of plastic sheets and duct tape for homes and businesses to provide "shelter in place" collective protection and the use of point detectors to identify lethal levels of chemical, biological, and radiological hazards. There were two major problems with this approach. First, the threat of CBRN hazard exposure to people at home (or even businesses) was about near zero, and second, the low probability of a CBRN hazard being used on any one day during the year at any one particular site within the United States was practically zero. It was not a sustainable strategy if one demanded eternal vigilance at all locations with the goal of eliminating all threats. And of course, the U.S. government wasn't protecting all potential terrorist targets.

The Homeland Security Planning Scenarios are ridiculously unrealistic in portraying the expected threats to the homeland. Of the fifteen scenarios, eleven are CBRN-focused, and not just typical CBRN hazards but significant quantities of military warfare agents such as anthrax, smallpox, sarin nerve agent, and mustard agent. They are "worst-case" scenarios, which are good for leadership exercises where you want to encourage interagency communications or to identify whether policies or resources are a limiting factor, but they are lousy for making resourcing decisions. Worst-case scenarios rely on movie-theater plots that maximize the threat only because that's the best way to get a maximum number of senior leaders within multiple agencies at the federal level involved to play in a short, annual national exercise. The 10-kiloton nuclear scenario is particularly ridiculous, but let's wait on that discussion.

As a result of these plans, we've inflated the stature of foreign terrorists into twelve-foot *ubermensch*. The term "non-state actor," a phrase that is routinely used around Washington, DC, applies to a larger cast of villains, including private militias, insurgents, criminals and drug smugglers, anyone who is basically working outside the government and conducting illegal activities. The concern focuses on those foreign (transnational) violent extremist organizations who generally receive some kind of basic military training so that they can use automatic rifles and grenades.

The basic approach used by terrorists and insurgents is to seek out and use low-risk, easily-acquired weapon systems. Any weapon that can be improvised using available and accessible materials is good; any weapon that can be bought on the open market and easily used is good. CBRN materials don't fit that niche. The reason why terrorists are interested in CBRN hazards is because so many senior leaders keep vocalizing how

afraid they are of this particular threat. Before 9/11, the interest was not as strong (and the senior leader rhetoric about "WMD threats" wasn't, either).

While terrorists are interested in CBRN hazards, they can't get the dangerous precursor materials, they don't have any training in handling or dispersing these hazards, and they don't understand the particular effects on their targets. So we see some scattered use of industrial chemicals, some production of ricin toxin from castor beans, a few grams of radioactive material stolen from a facility – not exactly mass casualty threats. As terrorists attempt to develop more sophisticated weapons in an effort to create mass casualties, their machinations become more public and it actually becomes easier to catch them.

Chemical Terrorism

Chemical terrorism has been downplayed recently, ironically because it doesn't cause enough casualties for high-consequence scenarios. Chemical terrorism remains the most likely form of CBRN terrorism, if one looks at the relative ease of obtaining industrial chemicals from the economy and low threshold of training and equipment required. Still, people focus on the nerve agents as the "likely" threat, not because they're available, but because they're the most lethal. Actual cases show terrorists seeking available industrial chemicals rather than making nerve agents, with one exception. Aum Shinrikyo had millions of dollars, facilities, trained chemists, and years of practice to make its sarin nerve agent. Most terrorist groups lack those resources.

I'm not a proponent of the DHS Chemical Facility Antiterrorism Standards, where the department looks to identify all chemical storage facilities and to make their owners assess the security of their chemicals. All this does is cause incentives to industry to move the chemicals somewhere else. Instead of focusing on the major producers, DHS diminishes its efforts by trying to cover tens of thousands of small facilities and anyone using a chemistry kit. It becomes a paperwork drill where no one addresses the really tough problems.

The toxic inhalation hazards, such as chlorine and phosgene, represent the most challenging terrorist threat, but that doesn't stop DHS from listing sixteen pages of "chemicals of interest."[6] Even then, getting cylinders of chlorine gas in the United States is not as easy as it used to be. Many water treatment plants have converted to alternatives to chlorine gas. Most toxic chemicals have colors or smells that cause people to take preventive measures prior to succumbing to their effects. But in the end, we know how to address hazardous material incidents, right? So why is this so difficult to address?

The railcar discussions are particularly amusing, in that there is so much concern about a hazmat derailment within a major city. So the answer is to divert hazardous materials around a city, right? There are two things wrong with that – the secondary

rails are less well maintained, and so represent a greater safety risk. And legal issues with regulation of interstate rail transport get in the way.

We're driven in the chemical industry to use this mentality of limiting exposure to the general public to "as low as reasonably achievable" or ALARA. This approach results in promoting "worst-case" EPA plume analyses that use minimum levels of incapacitating exposure as guidance for area effects, overestimating the actual impact of such incidents. We need to be serious about the probability of "high-consequence" events and what can be done to address them. DHS should focus on providing installation security assessments and identify ways to assist industry rather than being watchdogs.

Biological Terrorism

Bioterrorism is the flavor of the year, thanks to a recently-released government report titled "World At Risk" by former senators Bob Graham and Jim Talent.[7] Hollywood and fiction novels have done their best to ensure we all believe that a contagious virus without any cure is being secretly developed in a government lab and will wipe out civilization as we know it. We have a very long history on the treatment of natural diseases, and with the rise of biological warfare the difference between addressing deliberate and natural disease outbreaks gets very blurry. Some people say that, merely because there is greater access to information and technology related to natural biological diseases, there is a corresponding increasing chance of a bioterrorist incident. This isn't necessarily so.

One requires a large amount of biological warfare (BW) agent to successfully cause mass casualties, and these agents can't be made in a bathtub. You can't go to Wal-Mart stores to obtain dangerous biological assays or to Home Depot for equipment to grow biological material. Bruce Ivins was successful because he had a full laboratory suite and starter material available to him, plus decades of experience in handling anthrax.[8] But while the dangerous agents are hard to make, the diversity of the biological threat complicates the development of particular solutions. That isn't to say that we haven't made a good faith effort.

There are at least a dozen top BW threats, but under Project Bioshield, we have vaccines for only two of them. Maybe in another ten years, we'll have a few more vaccines, but certainly not twelve. For the 270 cities in the United States with a population of more than 100,000, only thirty-odd cities have Project Biowatch detectors. It's a very expensive project to sustain against a wide variety of potential threats. But this isn't just a medical issue, although the medics have assumed the spokesperson role.

Let's look at the "whole of government" approach to public health. DHS coordinates the Biowatch effort and the National Biosurveillance Integration Center effort. It's not a lot of money. DHHS has more than $80 billion a year invested into public health (not

including nondiscretionary spending). This includes the work at CDC. The DOD has its Defense Health Program funded at $40 billion a year. This includes all the military hospitals and TRICARE program, in addition to medical surveillance and treatment on the battlefield. The Department of Veterans Affairs department handles the health care of former military and is slightly bigger than the active duty health affairs efforts at $41 billion a year, but that's not a big surprise.

Then there's the DoD combating WMD community. While two-thirds of its $15 billion annual budget is spent on missile defense and special operations efforts, there are some funds spent on medical countermeasures and responses to biological warfare agent use. And finally, the international community plays a role through numerous non-governmental agencies as well as international health organizations. There are lots of players addressing different aspects of this huge area we call "public health."

By the estimates of the Center for Biosecurity at the University of Pittsburgh, there is roughly $5-6 billion a year spent on "biological defense," depending on how one defines that project. The FY2011 budget calls for about $6.5 billion. The "whole of government" challenge is managing all these efforts without disrupting anyone's rice bowl and still keeping cognizant of the bioterrorism threat, in addition to other public health concerns of infectious diseases, drug safety, and other health concerns.

People like to quote the total federal investment of $58 billion in biodefense projects over the past ten years to discuss the efforts made in this one specific area of CBRN terrorism. It's a misleading number, since many of the projects address multiple or tangential goals, not just domestic bioterrorism. However, the question should not be, is this too much money, but rather, how well is the money spent toward achievable goals? And we don't really know, because no one has established the end state against which we ought to be planning.

In January 2009, I presented a paper on behalf of the Project for National Security Reform, examining the progress we've made since the "Biodefense Strategy for the 21st Century" was released in April 2004.[9] Overall, the framework of the strategy is good. It identifies all the aspects required to respond to domestic bioterrorism and assigns responsibilities to the right federal agencies. In fact, it is unique in that there is no equivalent chemical or rad/nuclear framework (and that ought to be a concern). The problem is that no one has assessed how well the agencies were performing, if they were going in the right direction or required rebalancing, or if the end state was achievable given the available resources and personnel.

My research revealed that there are significant limitations on the progress made over the past five years. In particular, it was not apparent that there was any direct day-to-day federal oversight of CBRN terrorism response measures. Both the National Security Council and Homeland Security Council were consumed with daily emergencies and

meetings, and there was little to no oversight of what executive agencies were doing and if more funds or guidance were needed.

The generic terrorist threat is often referenced without any specific understanding of specific group motivations or activities. Al Qaeda has stated intentions to use CBRN hazards, but this has not led to the actual development of any specific capabilities. While the Proliferation Security Initiative has equipment for rad/nuke interdiction, there are no technologies to support biological interdiction. We're blindly attacking the tools instead of the terrorists.

The lack of any effort to harden critical infrastructure, notably with collective protection filters and CB agent detectors, surprised me. While integrating improved collective protection systems into existing buildings can be done, it's not an area that you see implemented. It seems like a relatively easy solution, but it seems that people would rather spend the money on military intervention or medical response rather than general protection.

I already mentioned the lack of vaccines and medical countermeasures for biological agents. The challenge was, and continues to be, that Big Pharma has no incentive to get involved in researching these specialized medical countermeasures. It's too expensive, it's not profitable, and it could lead to lawsuits if the drugs are incorrectly used. The government's offer of indemnity isn't winning any friends.

Bioforensics remains a tough challenge, considering the number of different strains of biological organisms. I don't know how many anthrax strains there are, for instance, but information on specific biological organism strains was helpful in narrowing down the Amerithrax suspect to a domestic source. The Biowatch effort should not be acceptable to any serious analyst. False positives aside, we'll never get adequate coverage for the entire United States, or even a majority of the nation's major cities, because it is too expensive to run 24/7 and to test all the samples in a lab. Even with the proposed Gen 3 biowatch detector, which doesn't exist right now, DHS plans to roughly double its monitors to cover sixty cities. Using point detectors for national special security events makes sense. Biowatch doesn't.

DOD has an impressive amount of personnel standing by for responding to a CBRN incident. At last count, it was approaching fourteen to fifteen thousand people ready to respond to assist state and local emergency responders. Although they might be useful for addressing the consequences of a chemical or radiological terrorist incident, they're not much help for biological terrorist incidents – especially a "no-notice" attack – other than offering a presumptive identification that the "white powder" threats isn't anthrax.

Radiological and Nuclear Terrorism

Radiological terrorism gets people excited because, even though the nature of radiological hazards hasn't changed in more than six decades, there's something about

radiation that spooks us. The term "dirty bombs" has a sinister sound. But of all the terrorist CBRN hazards, radiological devices (RDD) are certainly not WMD. We have never had an RDD incident to date, and yet so many people like to worry about the loose or available radiological isotopes that could be grabbed up by terrorists.

I'm very critical about the approach to addressing radiological terrorism. It's no surprise that the easiest way to reduce our risk in this area is to secure all the radiological material that industry uses and to place it in one location that could be guarded. Instead, because of NIMBY politics, the decision was made to close down a $9 billion nuclear material repository and to maintain the status quo of storing nuclear material in "temporary" storage near more than 120 nuclear facilities across the nation.

The idea of placing radiological monitors at every airport, sea port, and border crossing is, again, a concept that DHS adopted from the DOD. There's no question that the radiological dosimeters and monitors work when presented with an isotope. It's just that using these detectors at the thousands of possible entry points, considering the huge and constant flow of personnel and cargo, is a really stressful and expensive operation. We do not have reliable, cheap detectors that can be integrated into the process of screening people and cargo without negatively impacting our economy.

Getting past the actual implementation of such a vast network of detectors, let's look at the real 800-pound gorilla in the room. Some people fear that al Qaeda is going to somehow obtain a nuke from Pakistan, disable the safety mechanisms, and transport it to a U.S. city. Some fear that al Qaeda will build a crude nuclear bomb, using technical expertise and material through the global economy. The scenario of a 10-kiloton nuclear blast is what causes people to "lose sleep," allegedly. And yet, if you examine the facts, it's not likely at all that this is a credible scenario.

I strongly recommend Brian Jenkins' book *Will Terrorists Go Nuclear?*[10] and Michael Levi's book *On Nuclear Terrorism*[11] for anyone who's interested in an objective discussion on this topic. In short, nations with nuclear technology or materials need to consider whether the bomb will be traced back to them, and where the bomb might be used. It might not be in the United States, it might be in a neighboring country. The number of people who would need to be engaged to get/build a bomb and move it to the United States, let alone engineer a successful detonation, would make this a complex operation that would be visible to law enforcement and the intelligence community. We have no compelling evidence that any nation has provided a terrorist group with chemical or biological weapons – why on earth would they provide a terrorist group with nuclear weapons? It doesn't make sense.

The "high-altitude EMP blast" scenario is particularly outlandish, suggesting that a terrorist organization would be able to move a ballistic missile to the coast of the United States and set off a megaton nuke 200 miles over the country just to collapse the electronic infrastructure and turn America into a pre-industrial society. There are better

odds that an asteroid the size of Texas might collide with a major city within the United States. Resiliency is the answer – it would be simple to harden critical infrastructure points and maintain spares to stop this scenario from occurring. The argument here actually masks a separate debate over the continued development of a comprehensive (and very expensive) national missile defense effort.

Bottom line, we're already petrified that al Qaeda is going to nuke America, even lacking any evidence that it has one or could get a nuclear weapon. So why does al Qaeda need a nuclear bomb? It already has accomplished its purpose of terrifying the country. And yet, we see the unfolding of this massive "Global Nuclear Detection Architecture" that's designed to ensure our politicians can sleep well at night. We could cite the statistics – the hundreds of ports, the thousands of miles of border, the "second line of defense" – and ask is this the most effective way to address the challenge of a terrorist rad/nuke incident?

The scope of the global architecture keeps growing. In addition to the major air and sea ports and border crossings, the DHS Domestic Nuclear Detection Office has proposed going after all the smaller air and sea ports that cater to private vessels. And then there's the idea of populating the major cities and interstate roads between cities with radiological monitors. Is this a sustainable plan? Is it really effective, considering the limits of radiological detection technology? I would argue, no. The false alarms and cost of maintaining such a nation-wide system are prohibitive, considering the very low probability of occurrence and other options available to the national security community.

The GAO is actually very reserved in its criticism in this area.[12] It focuses on the lack of a strategic plan with measurable actions rather than on the feasibility of the concept itself, because the GAO strongly believes in strategic planning in any area of government. But let's be clear, this is a losing proposition. It is security theater, designed to make us feel good about doing something against a threat that people feel, in their gut, is an unacceptable challenge, despite the lack of any credible possibility of it occurring.

This is the least probable threat, granted one with an extremely high-consequence event if it is successful. Increasing the effort to focus on the origins of the rad/nuke material, in addition to good old-fashioned law enforcement and intelligence work, would be a far more effective solution than developing a network of detectors that focus on a particular hazard that could be easily shielded. To truly be effective, we need to develop a strategy that is guided by resources and that can be sustained throughout the year.

Let's assume that, worst case, a nuclear bomb is smuggled into a major U.S. city. Let's not pick New York City, that's been debated enough. But say a nuke goes off in Atlanta or Chicago or Seattle. Let's assume that the terrorists had a functional bomb that yielded

a 10-kiloton blast, not a crude device that resulted in a 1-2 kiloton fissile. Certainly thousands of Americans would die and a city would be irrevocably damaged. But would the United States stop, falter, collapse as a nation? No. A single nuclear terrorist event is not an existential threat to such a massive country. It can be managed, and given all the effort already in place to prevent such an incident, it's not what ought to be keeping us up at night.[13]

DOD Efforts to Respond to CBRN Terrorism

The DOD became involved in the discussion of federal response to CBRN terrorism in the late 1990s because Secretary of Defense William Cohen wanted his technical specialists to be involved in any federal response to a CBRN terrorist incident. Since everyone believed the threat was NBC weapons, DOD was of course the subject-matter expert. We already had a limited capability with the Army's Technical Escort Unit and the Marine Corp's Chemical-Biological Incident Response Force (CBIRF), the latter developed after the Aum Shinrikyo incident in 1995. So Cohen started with the concept of WMD Civil Support Teams to advise and assist state and local emergency responders. Congress really liked that idea, and now we have fifty-seven teams deployed across the U.S. states and territories.

That wasn't good enough, so DOD designed a Chemical-Biological Rapid Response Team, using various Army, Air Force, and Navy technical specialists, and later designed a "Guardian Brigade" in 2005. The National Guard decided to help with seventeen CBRNE Emergency Response Force Packages (CERF-P), which placed a CBIRF-type organization in every FEMA region (with some extra units for redundancy). The Bush administration pushed for a more robust capability using active duty forces, identifying the need for three large CBRNE Consequence Management Response Forces (CCMRF) to address multiple, simultaneous mass casualty events, but the strains of combat operations in the Middle East were significant, so that idea collapsed. As an alternative, the National Guard may provide additional response capability by creating ten Homeland Response Forces (HRF), one in each FEMA region.

The development of DOD response forces assumes that the states and local emergency responders will become overwhelmed by a high-consequence WMD event within forty-eight to seventy-two hours, and that gradual waves of federal troops are required to reinforce the response to that incident until it is concluded. So DOD comes in if a state governor requests federal support, if DOD is seen as necessary to that support, and if the DOD secretary approves it. However, if a high-consequence event never occurs, is this really a necessary capability? It is more likely that state and local emergency responders will be able to address the majority of CBRN terrorist incidents (short of that 10-kiloton event), given adequate training and preparation. It's an awful lot of manpower standing around, waiting for the firehouse alarm that may never ring.

As an example of DOD's own inherent challenges in addressing "homeland defense" with military chemical-biological (CB) detectors, let me offer this case study. Shortly after 9/11, DOD leadership was concerned that terrorists were going to attack U.S. military installations with CB warfare agents. There was no clear intelligence to support this, but it was a gut feeling based on the belief that terrorists liked mass casualties and domestic military installations were the top targets. It wasn't exactly a solid piece of analytical work.[14]

In 2002, DOD had more than 650 military bases and installations across the globe, but because of financial implications, the Office of the Secretary of Defense decided that it would provide funds to develop CB defensive measures for 200 of these bases, the majority of which were within the continental United States, at a cost of $5 million each. In addition to the one billion dollars for the project, there was another half-billion dollars allocated for training installation responders. This would provide a number of chem-bio detectors (no radiation detectors) tied into the emergency ops center, some protective gear and medical countermeasures, hazard plume software and warning sirens, and training and concept development. This was supposed to provide a basic level of protection for the installation.

The effort began in 2004, and within the first two years only one base received enough gear that might constitute an adequate antiterrorism capability. Most of the bases only received limited gear for the emergency responders, rather than receiving a full antiterrorism capability. In 2006, half of the billion dollars was funneled off for a new program aimed at developing "silver bullet" vaccine shots for "broad spectrum" biological threats. The main failure lay in the inability of the antiterrorism and CB defense communities to implement an integrated, all-hazard "CBRNE" operational concept for military installations and bases. The antiterrorism community didn't view CBRN hazards as a significant threat, and didn't appreciate having specialized equipment forced onto them.

CONCLUSIONS

Homeland security is not a new issue. It's encouraging that we have advanced education now and interagency discussions on how we all can address the threat of domestic CBRN incidents, from the state and local level through the federal level. But we need serious reviews of the policies that are in place and to use that "risk-based" management approach to ensure that we are spending our funds wisely. We continue to view WMD or CBRN hazards as the threat – that's a myopic focus. We need to look at the process by which terrorists develop their tools and understand that it is by defeating the terrorists that we can stop the CBRN threat. When you take a realistic look at the threat and what

terrorists can actually do – outside of a television show like *24* – it's not a difficult thing. We can do this more smartly.

There is a fundamentally better approach to developing a federal response to domestic CBRN incidents, but we need to start by stopping the loose use of the term "WMD." It only confuses the discussion and presents an unachievable goal that obstructs serious discussion. We need to clearly separate the concepts of how militaries defend against NBC weapons and how emergency responders address terrorist CBRN hazards. These are very different concepts. We should not act as if a terrorist group has the capability to do as much damage as a nation with an active WMD program. Although the military threat is similar to the terrorist threat in terms of physical composition, the scope of the incident and required concepts and equipment are entirely unique. We have to develop a sustainable, effective solution that can be employed throughout the year to protect untrained noncombatants.

We need to address the mass casualty definition to allow more informed discussions on possible approaches to realistic scenarios. My suggestion is to develop a three-part framework based on the expected number of casualties:

- Type A: 100 – 1,000 casualties (Oklahoma City bombing)
- Type B: 1,000 – 5,000 casualties (9/11 incident)
- Type C: 5,000 – 50,000 casualties (nuclear weapon incident)

By better defining the consequences of a terrorist incident, we can develop focused initiatives that can be measured against easily understood scenarios. Similarly, the Homeland Security Planning Scenarios have to be changed to reflect realistic and probable threats, not "worse-case" scenarios. By using the scenarios as the basis for national-level exercises, we risk the danger of overestimating the actual need for unique and specialized resources that may never be employed within our lifetimes. We should not lose sight of the fact that the majority of incidents requiring federal response to state and local emergency responders will be for natural disasters and industrial accidents rather than WMD.

In developing policies that try to protect everything, we protect nothing. We need to develop strategies that are guided by resources, recognizing that there are multiple homeland security threats that all have to be addressed. It actually is a question of "if, not when" we ever see a CBRN terrorist incident that results in mass casualties. We need a sustainable, effective approach, which requires us to stop overhyping the threat. It's not September 12, 2001, anymore. We need to realistically assess the challenge and all possible threats – natural and man-made – and calmly, rationally, develop a plan that doesn't bankrupt the annual operating budget. None of us have enough money to

provide perfect protection for everyone throughout the year, and there are better things to spend money on – like retirement plans.

Al Mauroni is a senior policy analyst with more than twenty-four years experience in Department of Defense chemical, biological, nuclear, and radiological (CBRN) defense policy and program development. He served as a U.S. Army chemical officer for seven years before leaving active duty in 1992. He holds a master's degree in administration from Central Michigan University and a bachelor's degree in chemistry from Carnegie-Mellon University. He is the author of six books (the latest of which is titled Where Are the WMDs?) *and more than two dozen articles. Mr. Mauroni can be contacted at mauronia@yahoo.com.*

---

[1] U.S. Department of Homeland Security (DHS), "Civil Defense and Homeland Security: A Short History of National Preparedness Efforts," (September 2006), http://training.fema.gov/EMIWeb/edu/docs/DHS%20Civil%20Defense-HS%20-%20Short%20History.pdf.
[2] Charles O. Jones, "An Introduction to the Study of Public Policy," (Harcourt, 1984).
[3] The White House, *National Security Strategy* (May 2010) http://www.whitehouse.gov/sites/default/files/rss_viewer/national_security_strategy.pdf.
[4] The White House, *National Strategy to Combat Weapons of Mass Destruction* (November 2002), http://www.state.gov/documents/organization/16092.pdf.
[5] National Counterterrorism Center (NCTC), *2009 Report on Terrorism* (Office of the Director of National Intelligence, April 20, 2010), http://www.nctc.gov/witsbanner/docs/2009_report_on_terrorism.pdf.
[6] See the DHS webpage on CFATS at http://www.dhs.gov/files/laws/gc_1166796969417.shtm.
[7] Bob Graham, et al, *World At Risk: The Report of the Commission on the Prevention of WMD Proliferation and Terrorism* (Vintage Books, 2008), http://www.preventwmd.gov/report/.
[8] Federal Bureau of Investigations (FBI), "Amerithrax Investigation," http://www.fbi.gov/anthrax/amerithraxlinks.htm.
[9] See Project on National Security Reform, "Progress of 'Biodefense for the 21st Century' – A Five-Year Evaluation," Project on National Security Reform (January 2009), http://otherwmds.blogspot.com/2009/03/biodefense-monograph.html.
[10] See http://willterroristsgonuclear.com/.
[11] See http://www.cfr.org/publication/13915/on_nuclear_terrorism.html.
[12] U.S. Government Accountability Office, "Nuclear Detection: Domestic Nuclear Detection Office Should Improve Planning to Better Address Gaps and Vulnerabilities," GAO-09-257 (January 2009), www.gao.gov/new.items/do9257.pdf.
[13] See also Robert C. Harney, "Inaccurate Prediction of Nuclear Weapons Effects and Possible Adverse Influences on Nuclear Terrorism Preparedness," *Homeland Security Affairs* V. No. 3 (September 2009), http://www.hsaj.org/?fullarticle=5.3.3.
[14] Al Mauroni, "CBRN Defense of U.S. Military Installations and Facilities," *Scribd.* (August 2005), http://www.scribd.com/share/upload/10460697/1d19xw96qz3oiaqq48pw.

Natural Security for a Variable and Risk-Filled World

Raphael Sagarin

INTRODUCTION

Fish don't try to turn sharks into vegetarians. Living immersed in a world of constant risk forces the fish to develop multiple ways to live with risk, rather than trying to eliminate it. The fish can dash away from the shark in a burst of speed, live in places sharks can't reach, use deceptive coloration to hide from the shark, form schools with other fish to confuse the shark, it can even form an alliance with the shark, and all of these things may help the fish solve the problem of how to avoid getting eaten by the shark. But none of these adaptations will help the fish solve the general problem of predation, and they don't need to. The fish doesn't have to be a perfect predator-avoidance machine. Like every single one of the countless organisms it shares a planet with, the fish just has to be good enough to survive and reproduce itself.

The world in which we spend our daily lives is also full of risk. Acts of terrorism that seem to come out of nowhere. Wars that have carried on too long and show little progress toward resolution. Catastrophic failures of supposedly fail-safe oil rigs. Intensifying natural disasters fueled by global changes in climate. A distribution of food that leaves billions undernourished and millions of others facing an obesity epidemic. A cyber infrastructure that we've become increasingly dependent upon that also has become increasingly vulnerable to catastrophic attack. New diseases and new mutations of old diseases that threaten to become global pandemics. The major threats society faces today are ominous and complex interplays of human behavior and environmental change, global politics, and local acts of cruelty or carelessness, historical accidents, and long-simmering tensions. Some of these threats have plagued us as long as we have been human and yet we've made little progress against them, others are becoming more dangerous in synergy with rapid climatic and political changes, and still others are just now emerging.

Yet the responses we been offered or forced to accept by the experts we've entrusted to solve these problems often seem frustratingly ineffective, naïve, or just plain ridiculous. When increased body screening of airline passengers was implemented after 9/11, Richard Reid attempted to destroy an airliner with a bomb in his shoe. When shoes began to be screened in response to Reid's attack, al Qaeda plotted to use a liquid explosive attack. When liquids were banned, Umar Abdulmutallab used a powdered incendiary hidden in his underwear in an attempted attack. A wall constructed between parts of the U.S. and Mexico border at a cost of between $1 million and $10 million per mile, slows down illegal immigrants by an estimated twenty minutes, even in its most fortified areas.[1] And on a tiny island in the tiny town of Beaufort, North Carolina there is a tiny outpost of the National Ocean and Atmospheric Administration (NOAA) that studies fish populations and coastal ecology. There is little reason to suspect this outpost is on any terrorist's list of desirable targets. Yet when the NOAA coastal scientists wanted to renovate and add some space a few years back, they were forced by the Department of Homeland Security to install enormous Wal-Mart style parking lot lights on their facility as a required security measure. This was ironic, since the scientists

working at the lab know full well that nighttime light pollution is a major threat to the ecology of the same coastal marine environments that they are paid by taxpayers to study.[2]

The most famous line of the 9/11 Commission report was that 9/11 represented a "failure of imagination,"[3] and this was certainly an apt description of the security situation up until 9/11. However, now that we imagine almost anything to be a threat to our security, a more pernicious problem faces all of our security systems: a failure of adaptation. Adaptation is the process of changing structures, behaviors, and interactions in response to changing conditions in the environment. *Adaptability* is the capacity to adapt to these changes – something that despite an unprecedented amount of attention, financial resources, and human lives sacrificed in the name of security since 9/11, has still largely eluded us.

Fortunately, we have at our disposal a vast storehouse of largely untapped knowledge that could guide us in developing adaptable security systems. It is a massive set of proven solutions (and teachable failures) to the very same problem that unites all of the threats we face – that is, how to survive and thrive in a risky, variable, and uncertain world. Remarkably, this database is completely unclassified and accessible to anyone. The solutions I'm referring to are all contained in the staggering diversity of life on earth – millions of individual living and extinct species, and countless individuals within those species – which have been developing, testing, rejecting, and replicating methods to overcome the challenges of living on a continually changing planet. These organisms have been experiencing security challenges and developing solutions since long before any presidential administration or Congress has developed their security agenda, since long before 9/11 finally woke most of us to the new post-cold war reality, since long before industrialization pushed our biogeochemical cycles into chaos, and long before humans ever walked the earth. Indeed, the 3.5 billion-year history of life imbues biological systems with more experience dealing with security problems than any other body of knowledge we possess.

And because we ourselves are biological creatures, our own species' evolution (and the modern manifestations of that evolutionary process) is not only an integral part of this natural database, but perhaps the most important set of data to consider. This means that in addition to the ecologists, paleontologists, virologists, and evolutionary biologists who have something novel to contribute to our security debate, so too do anthropologists, psychologists, soldiers, and first responders who have extensive behavioral observations of people and societies under the stress of insecurity in an uncertain environment.

I have been working with exactly these types of people for the last five years, primarily through my working group on "Darwinian Security" at the National Science Foundation-funded National Center for Ecological Analysis and Synthesis (NCEAS) in Santa Barbara, CA, and through interactive discussions with participants in several programs at the Center for Homeland Defense and Security (CHDS). The ideas developed in these lively discussions have been further honed in presentations to security think tanks and academic institutions, in corporate seminars and discussions with elected officials, and through response to our edited volume, *Natural Security: A Darwinian Approach to a Dangerous World* (University of California Press, 2008).

We have found that there is an increased openness among biologists to apply ecological and evolutionary ideas beyond biology, and receptiveness among societal institutions to incorporate biological knowledge into practice in, for example, using ecosystem analysis to study the global financial collapse. While there have been attempts to copy designs from nature to apply to security concerns (for example, designing submarine hulls based on the hydrodynamic shape of a tuna), and applications of biological models to studies of conflict, our approach considers key questions across the broad spectrum of security concerns and seeks insight from natural patterns and dynamics (Fig. 1). It is from this rich store of human knowledge that I present the general rules, specific examples, and pertinent applications of naturally-inspired security that can be implemented in the analysis, planning and practice of security in society.

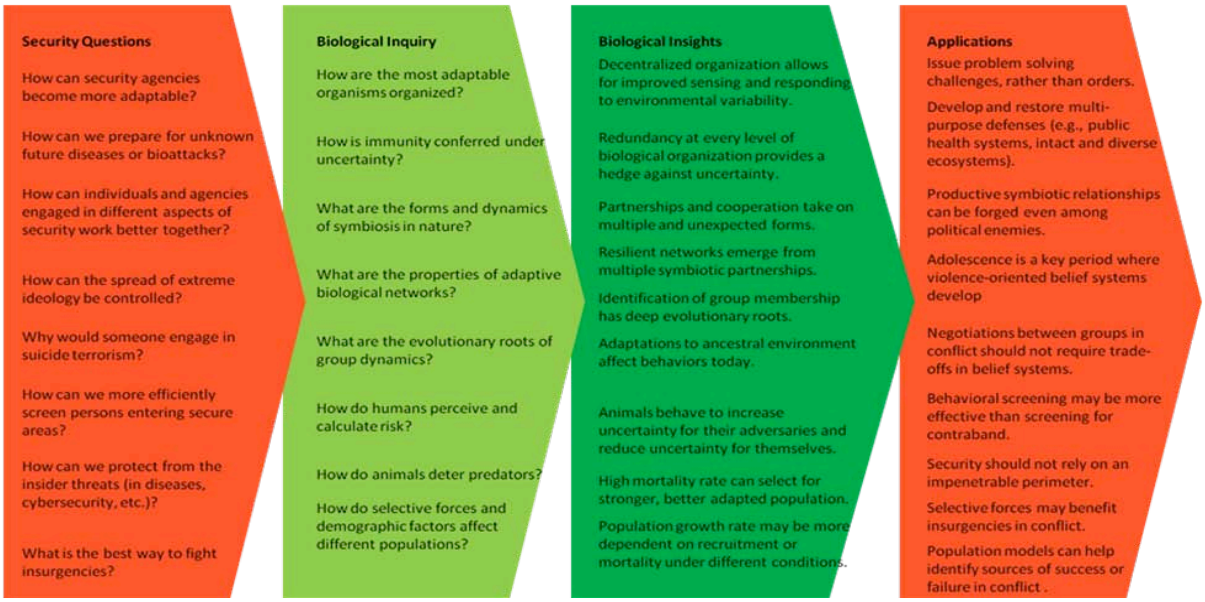


Figure 1: Naturally Inspired Security. Applying natural security is a reiterative process that begins with security questions in society and uses natural history-based inquiry to find analogies and models, which can then be applied to society. Applications can then be further refined with more detailed societal questions and biological observations. Examples given are illustrative, not exhaustive.

BASIC PROPERTIES OF NATURAL SECURITY SYSTEMS

Since we have incredibly limited communication with all but one species of the millions of natural security experts, how can we tap their knowledge? In some cases, we will have just the raw data to observe and work with – the remarkably diverse ecosystems, organisms, cells, and molecules that inhabit the earth. Still more knowledge can be gleaned from ancient observations of nature made since the earliest human societies, from painstaking natural history and evolutionary biology conducted over the 150 years since Darwin's revolutionary *On the Origin of Species*, and from the most cutting-edge biological research on protein folding, genome mechanics, and network analysis that

have massaged these raw data into stories and models and theories about how biological organisms survive and thrive on a dangerous planet. What emerges from this vast and growing field of study are a few simple themes that are essential in understanding how to translate natural security to societal security.

First, patterns in nature appear similar across different levels of biological organization. By levels of biological organization I mean the progression from molecules to DNA to cells to bodies of individual organisms to populations of those individuals to communities of those individuals interacting with individuals of other species to ecosystems which include the species, habitats, chemical and energetic interactions between them all in a given area. What is remarkable is that similar patterns – for example, using non-centralized organization to sense and respond to the environment – appear at each level of this organization. This *nested* quality of biological systems arises from their *recursive* character, meaning that the rules and patterns occurring at one level are not just similar to those at the next level, but essential in defining what happens at the next level. All of this is a good sign for applying biology to security in society because it suggests that biologically-guided solutions successfully implemented at one level (say, within a single office in FEMA) will be applicable at a completely different level (e.g., throughout the Department of Homeland Security). It also invalidates the excuse that we can't change security policy unless our highest levels of government change. I argue that we can start at any level of society in instituting more adaptable security systems and, if we align our incentives correctly, these ideas can easily (in fact will almost inevitably) spread up and down different levels of organization in society.

Second, complex natural patterns and processes arise from very simple building blocks. The four basic molecules of DNA code for a vast diversity of organisms that live in completely different ways and deal effectively with vastly different challenges. Moving up the levels of biological organization, natural selection, which has molded millions and millions of species into their forms today, is an incredibly simple process requiring just three simple building blocks: variation between individuals, environmental conditions that favor (or select) certain variants over others, and a means to reproduce those variants that are better suited to the environment. At yet a higher level, the simple process of individual organisms trying to survive and reproduce ends up producing networked ecosystems that are complex and resilient. Accordingly, natural security isn't about rising to the complexity of the security threats we face by designing a hugely complex system with flow charts and acronyms and multi-variate statistical outputs. It's about finding simple processes that impart our security systems with the adaptability to deal with a wide range of threats.

Third, biological evolution doesn't plan, design, or set goals of perfecting an organism. Evolution proceeds by solving survival problems as they arise, resulting in organisms that are not perfect, but "good enough" to survive and reproduce themselves. Likewise, in society we do not need to design perfect solutions to security problems – when we try to, they inevitably waste enormous amounts of resources while at best only marginally improve our security. We do need to define what is "good enough" and recognize that, as in natural systems, that definition will change continually through time.

Fourth, good ideas in evolution are often easy to spot because they appear nearly exactly the same across many different kinds of organisms. Although the DNA codes for millions of different organisms, the basic structure of the molecule and the process by which it replicates itself is the same across much of the living world. Heat shock proteins, which go around the body repairing damaged proteins, are both present and nearly identical in almost all organisms on earth. Thus, the biologically inspired ideas I propose here are not just stab-in-the-dark guesses that happened to work out well for a snail or a soybean plant somewhere, but time-tested billion-year-old solutions that have worked out in the coldest, highest, darkest, hottest, most predator-full and water-starved places on earth.

Fifth, good ideas in evolution are often the things that evolved independently multiple times. Eyes, for example, are a good solution for finding your way around in a complex world, but there isn't one common type of eye that evolved billions of years ago and that we all share. This security solution arose independently several times in different types of organisms. Octopuses have incredible eyes that serve the same kinds of functions as our eyes, but they are unique to octopuses. This phenomenon, called *convergent evolution*, is evidence that evolution is not about taking one design and plopping it down all over, but about solving problems particular to a given organism in a given environment. Here I propose ideas for security that mimic natural solutions, but they may also have been explored by other people or organizations who didn't make any reference to nature at all. I consider these coincident solutions to be examples of convergent evolution – different people trying to solve the problem of how to be ensure security in society and coming up with similar solutions.

Sixth, under the lens of natural history, humans are special, but not that special. There are a number of adaptations we have – such as advanced cognition and language – that both set us apart from most other species and create a lot of the complex security threats we face, but we are, in the end, just another species that evolved through time to deal with security challenges in our environment. With over a billion people facing chronic nutrition shortages,[4] and a host of old and emerging diseases that threaten to turn into human pandemics, we are undoubtedly still subject to the pressures of natural selection. Moreover, the way we have evolved has changed our environment enough to force us to adapt further. This cuts several ways for us – we are extremely adaptable, but we also may have changed our world and way of living faster than some parts of us can evolve. Some of our adaptations, which first arose in societies and on a planet completely unlike that in which we live today, can get us into trouble now.

Finally, and most important, change and variation rule everything in nature. As Darwin mused during his long journey on the *Beagle*, "where on the face of the earth can we find a spot, on which close investigation will not discover signs of that endless cycle of change, to which this earth has been, is, and will be subjected?"[5]

Darwin was referring to geology, the task he was primarily assigned during his fateful journey, but variation and change were very much at the heart of his subsequent biological studies. He felt it was essential to understand even the most minute variations – such as the microscopic differences between anatomies of the many species of barnacles that he cataloged in an enormous two-volume treatment[6] – to understand that "mystery of mysteries" of where life comes from. The simple lesson from this is that no

effective security solution can be deployed and not modified or changed with time, because everything around it will be changing.

These basic tenets of evolution provide the outside parameters for developing an adaptable approach to security, but careful study of nature reveals general trends and patterns that can be used to provide specific guidance for applying nature's lessons to security in society.

SPECIFIC PROPERTIES OF NATURAL SECURITY SYSTEMS

Adaptable Organization

The most adaptable and successful organisms, though wildly diverse in appearance and behavior, are all organized in a similar manner. Universally, they avoid the trap of centralized, top-down control by giving wide ranging power to multiple independent sensors to observe and respond to environmental change and threats.[7] Organisms have done this by evolving specialized organs, developing highly sensitive sensory mechanisms, specializing functions into differentiated clones, and organizing nerve cells into networked clusters operating closest to the environmental interaction.

By contrast, many of our security responses trend towards increased centralization. The most prominent security response after 9/11 was to create the massive Department of Homeland Security (DHS), which quickly displayed its shortcomings during and after Hurricane Katrina, the response to which represented the worst post-9/11 security breach in the United States. A common question during and after Katrina was "Where was FEMA?" – referring to the Federal Emergency Management Agency, which was ostensibly in charge of disaster relief efforts. Because it is a bureaucracy, the best way to find FEMA is by looking at the "Org" chart of its parent organization, DHS, at the time of Katrina (Fig. 2). FEMA is literally buried in a huge stack of blocks, all representing their own enormous bureaucracies – such as the Coast Guard and the Transportation Security Administration (TSA) – all required to run decisions up the chain of command to the secretary of Homeland Security and, consequently, all vying for the secretary's attention.

An organization like this might work fine in carrying out a planned set of tasks that continue routinely day after day. It's like an early circuit board with a finite number of pathways through which the energy of decision-making can pass. But security problems are such precisely because they are not routine; they are highly variable and unpredictable. If one of the organizations inside one of those boxes needs to do something completely different than normal – as FEMA needed too after Katrina – it has little recourse to do so.

That's not to say that some organizations didn't demonstrate some amazing responses to Katrina. The United States Maritime Administration, a branch of the Department of Transportation that maintains and contracts a fleet of ships to make vessels available during wars and national emergencies, quickly set up shipboard spaces that the various security agencies used as command centers. And of course, many individuals within all of the agencies, as well as individual citizens, improvised all sorts of effective responses to the hurricane.

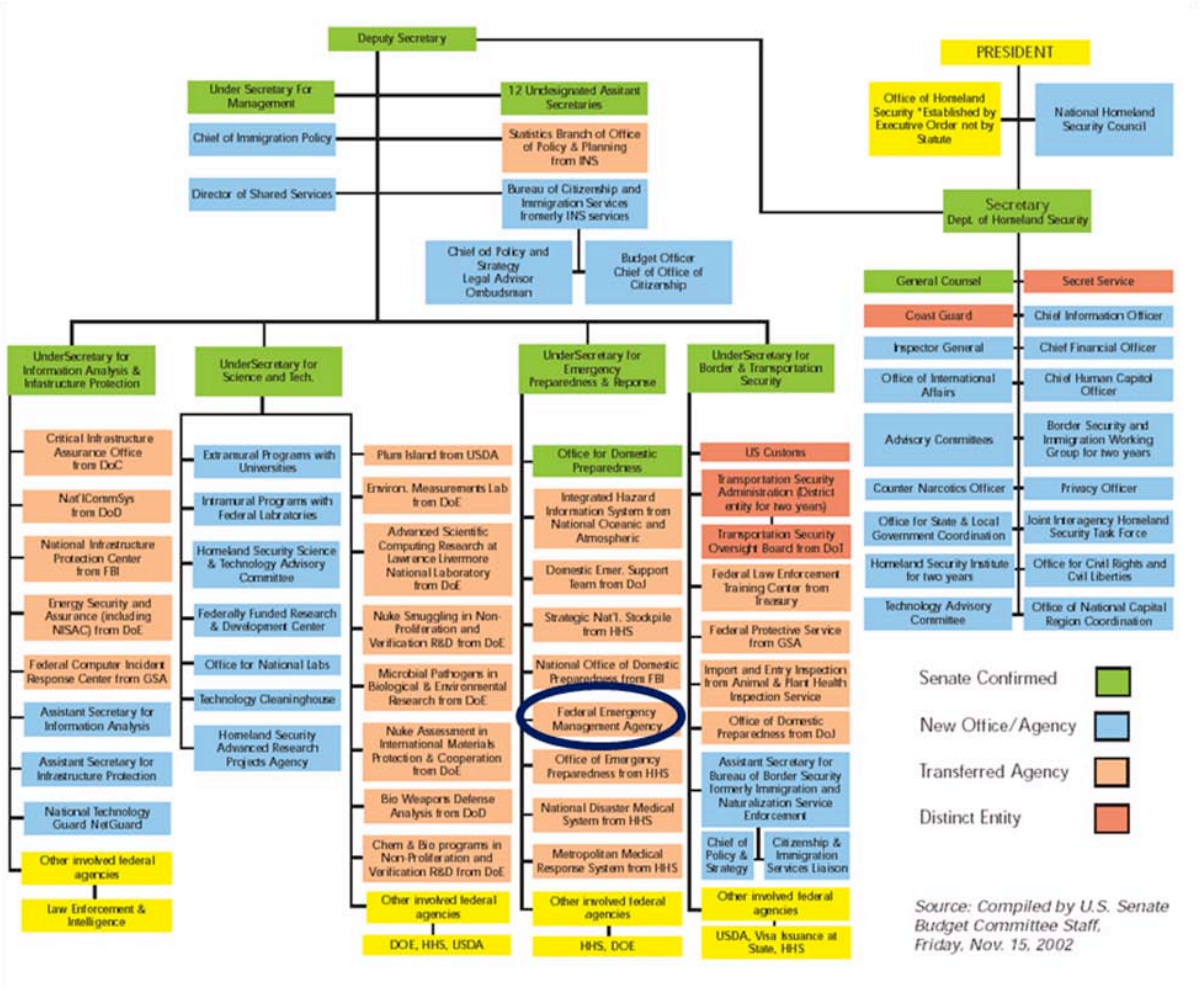


Fig. 2. Organizational chart for the Department of Homeland Security. FEMA is circled in dark blue. Source: U.S. Senate Budget Committee Staff, Nov. 15, 2002.

It is often assumed that the stack of boxes leading to one central controller is the natural and inevitable way an organization develops. And people working within such an organization often assume that there is no way to change that system of organization without destroying the entire organization itself.

The first assumption is, in fact, completely false, as proven by most successful biological organizations on earth. And challenging the second assumption, which is beginning to happen in societal organizations throughout the world, is the key to turning non-adaptable *organizations,* like DHS, into adaptive *organisms* that truly do keep us safer. Indeed, independent of our biological perspective, a number of sources have recognized the adaptability of decentralized organization in the context of business,[8] social activism,[9] and international governance.[10]

Even large entities have learned to develop adaptable, distributed organization structures. Google, Inc. uses a decentralized system for encouraging development of

many of its products, which are then tested by billions of independent internet users.[11] For example, Google Flu Trends analyzes search behavior by internet users, specifically focused on flu-related search terms such as, "flu symptoms" and "flu remedies" under the assumption that more people will search such terms when flu is becoming more prevalent. Google Flu Trends show remarkable similarity to official U.S. Centers for Disease Control and Prevention (CDC) flu trend reports (which are compiled and published by CDC from doctor and hospital surveys) with one major exception: Google Flu Trends are available one to two weeks prior to the release of centrally controlled CDC data.[12]

Adopting an adaptable organizational system does not require a complete reorganization of our security bureaucracies. Almost any organization can inculcate adaptable systems by shifting from giving commands to issuing challenges – essentially open contests to solve a clearly stated security problem. Most security practice today is designed by a small number of experts and implemented through a central authority issuing orders to civilians (e.g., surrender your bottled water to TSA officials in airports) or contractors (e.g. design an aircraft that does X for Y amount of money). By contrast, challenges essentially create adaptable security organizations by encouraging multiple independent agents to find the best solution to a problem, then rewarding the most successful agents, and in the best cases, repeating the challenge to replicate and improve on the best designs from the previous iteration.

Even complex challenges can be successful at low cost and in relatively short time frames. For example, in 2002 the U.S. Defense Advanced Research Projects Agency (DARPA) presented an open challenge to a diffuse population of civilian groups to create autonomous vehicles that could navigate an obstacle course. The first iteration of this "Grand Challenge" in 2004 was fraught with failure. But groups learned from one another, and independently modified the wide variety of first-generation designs, selecting out poor performers and replicating successful components, resulting in high success in the second year which encouraged DARPA to issue yet more complex challenges in subsequent years. The most recent DARPA challenge (to find ten weather balloons scattered around the United States) was solved within a few hours by activating thousands of independent observers on the internet. [13]

Harnessing Uncertainty

A decentralized organizational structure works because it allows organisms to deal with uncertainty. Uncertainty that is created by variation lies at the core of a wide range of security concerns. Organisms in nature actively exploit uncertainty and turn it to their advantage by creating uncertainty for their adversaries and reducing uncertainty for themselves. Predators create uncertainty by stalking from hidden vantage points, but when possible, prey reduce this uncertainty by vocally or behaviorally signaling the presence of predators – a strategy that both warns fellow prey about the threat and indicates to the predator that the element of uncertainty has been removed.[14] To be effective the signaling must be directly tied to immediate threats. For example, ground squirrels will make vocal signals to bird and mammal predators (which can hear) but switch to "tail flagging" displays to deter snakes (which cannot hear), and will additionally heat their tails only when encountered by particular snakes (pit vipers) that can sense infrared signals.[15] By contrast, when organisms in a community make

constant alarm calls regardless of the immediacy of the threat they only increase uncertainty for other members of the group, who must waste resources determining if the alarm is true or false.[16] Analogously, the U.S. National Threat Advisory, which has remained at level "orange" for aviation since August 2006,[17] is not aimed at deterring a particular threat and does little to reduce uncertainty among innocent travelers. We can vastly increase the uncertainty for our adversaries by just doing a small amount of random things every day in our security procedures. Currently we waste enormous resources to screen 100 percent of the people passing through security with little benefit. Laying aside the fact that this doesn't even work to find the things we are looking for (knives, guns, explosive materials, and 6 oz. tubs of strawberry yogurt, all have which have been brought through security in recent years without detection),[18] it also gives us almost no extra protection from real attackers.

A low frequency of random screening (as opposed to a high level of screening equally applied to all) can deter someone who wants to evade detection.[19] This is particularly true in the case of a terrorist attack because there is a very high cost of failure in such a plot, as there is for any predator. A lioness hunting an antelope must have very little uncertainty that her attack will be successful because if she fails, she has not only wasted energy and gotten hungrier, but she has also left her pride hungrier as well. A terrorist who gets caught not only fails to achieve the goal, but also puts his entire organization at grave risk of being discovered or counter-attacked. Indeed, this aversion to uncertainty drove several delays of the 9/11 attacks and may have led senior al Qaeda leaders to abort the attacks on 9/11 had they known one of the secondary operatives had been arrested.[20]

What is attractive about randomizing security procedures is that it can actually drastically reduce the amount of time we waste in security lines (by screening much less than 100 percent of people for most things) while reducing the likelihood of an attack. These multiple benefits are not just serendipitous – natural security systems create positive feedback loops. For example, increasing uncertainty for a predator reduces the need for constant vigilance by the prey organism, which can then spend more resources on eating or mating or other needed security strategies. The Transportation Security Administration (TSA) has been experimenting with randomization and uncertainty in its 2010 Surface Transportation Security Priority Assessment, about which it testified that "random screening teams are among DHS' most effective deterrence and detection tools for countering terrorist threats,"[21] as well as through its Screening of Passengers through Observation Techniques (SPOT) behavioral detection program which deploys trained TSA agents to search for characteristic signs of stress and deception among passengers. Behavioral recognition has the advantage of returning control of uncertainty to the population it is trying to protect because it can be conducted from hidden vantage points or video. As a head behavioral screener at Dulles Airport (one of 161 airports where behavioral screening was initially deployed by TSA)[22] remarked, "The observation of human behavior is probably the hardest thing to defeat. You just don't know what I am going to see."[23] Nonetheless, the scientific basis for behavioral detection has not been well established,[24] and the efficacy of layering discrete behavioral screening with other levels of verbal and non-verbal intent detection systems is currently being investigated.[25]

Learning Through Evolution

A main reason that security walls and contraband screening don't work against attackers is that they quickly learn what the barrier is and how to get around it. This problem has been recognized by cyber security experts who have recently acknowledged that forty years of attempts to make "perfect" systems protected by firewalls have only led to an increasingly vulnerable cyber infrastructure.[26] One simple and effective cyber attack that has been successful in deliberate simulations and actual attacks involves physically scattering virus-infected USB drives in a parking lot and letting employees with security clearance inadvertently introduce the virus behind the firewall when they insert the drives into their workstations.[27]

Even in relatively simple organisms, learning sets off a continual process of escalating threats and adaptive defenses. Birds learn that certain color patterns in spiders indicate the presence of poison and they avoid those patterns. Through time, other non-poisonous spiders develop the color patterns of the poisonous types and thus avoid being eaten themselves; a selectively induced learning passed down through generations. Even the process of how animals learn is not immutable. That is, animals have some basic capacity for learning, but they can learn in accelerated ways depending on the environment they are put in. Monkeys, which are generally considered to have the learning capacity of a human two-year-old, can be trained in experimental settings to learn like a nine-year-old, including understanding a sense of their own self as a unique entity interacting with and affecting the world around them.[28] The capacity for learning reminds us that no security adaptation should be assumed to be a safe and everlasting solution, because there is always the potential for an adaptable enemy to learn how to overcome it.

A more formalized way to look at natural learning is through the framework of adaptation by natural selection. Examining the changing security environment in a Darwinian context that breaks down the three components of adaptive evolution – variation, selection, and replication – provides insight into how individuals and institutions learn from experiences with environmental threats. These factors may explain why the insurgents have been relatively successful against coalition forces in recent conflicts. Johnson argues that the nearly invariant ratio of insurgents killed or captured per U.S. soldier killed or captured throughout the Iraq war may be attributable to stronger selection pressure exerted by the more powerful side (the U.S.),[29] which leads to faster adaptation among insurgent fighters, strategies, and technologies. This selection works on a more variable population of insurgents, who both come from more diverse origins than U.S. forces and utilize a wider range of tactics than U.S. forces, which are constrained by standard procedures, international conventions, and other norms.

Ground observations support this analysis as the average time for insurgent fighters to adapt to new tactics, techniques, or procedures of U.S. troops is reported by counterinsurgency officers to be about fourteen days; insurgents apparently have learned to identify the signs of troop rotation and step-up attacks immediately following the arrival of new troops.[30] This rapid adaptation is a well-appreciated problem. U.S. Secretary of Defense Robert Gates remarked at a congressional hearing in March 2007 that "as soon as we ...find one way of trying to thwart their efforts, [the insurgents] find a technology or a new way of going about their business"[31].

Humans' ability to learn is advanced relative to most other species and accelerated through a high degree of parental care, symbolic language, and communication networks that allow us to learn from environmental threats without actually experiencing them.[32] In addition to creating a more threatening environment, learning can also greatly aid our security. For example, until 9/11 the normal response to a plane hijacking was to put up no resistance as hijackers made demands that were eventually negotiable and lethal threats were unlikely to be carried out. But on the same day that terrorists began using passenger planes as weapons of mass destruction, humans used networked technology to share information about the change in hijackers' tactics and passengers on one hijacked plane immediately adapted a more active defense, risking their own security to protect a larger (and largely unrelated) group of humans. Subsequent airborne attack attempts by Reid and Abdulmutallab were similarly stopped by passengers.

Using Symbiosis to Extend Adaptability

All organisms are constrained in their adaptability at some point, but they can utilize symbiotic relationships to extend their inherent adaptive capacity to exploit new resources and environments. Symbiotic relationships are diverse and ubiquitous in nature, including relationships between species – such as predatory fish and much smaller fish – that would appear to have no reason to cooperate. Where these relationships appear cooperative in humans or other organisms, there is still debate over whether they: are codified through positive feedback, must be enforced by punishment, are conducted with the expectation of reciprocity, or arise in response to genetic relationships between kin.[33] Regardless of the underlying mechanism, individual symbiotic relationships can confer multiple benefits to the larger environment. Studies on monkeys and apes show that when individuals are forced to begin a cooperative relationship (to help one another get food, for example), conflict overall between the animals is reduced.[34] Small coral reef fish known as wrasses set up "cleaning stations" where large fish can have their parasites cleaned off, provided they don't eat the smaller fish. The large fish in this symbiosis are not only less aggressive to their cleaning partners, but towards all other fish on the reef as well.[35]

Cooperation among humans is far more complex than that among fish or monkeys, but the same surprising diversity of symbiotic relationship characterizes successful partnerships that diffuse security risks. New types of symbiotic partnerships between the most unlikely of collaborators are developing and ameliorating potential security crises around the globe. My colleague Terence Taylor, for example, has helped incubate symbiotic partnerships between Israelis, Palestinians and Jordanians,[36] as well as practitioners from five traditionally hostile countries on the Mekong River, all working together to identify and neutralize disease outbreaks on whatever side of borders they occur. Several features of these cooperative networks should be recognized. First, the networks have demonstrated success even beyond the feat of getting members of mutually hostile nations to work with one another. Network practitioners were quietly allowed into notoriously restricted Myanmar to do their work days, not weeks, after the catastrophic cyclone there. Second, these networks weren't mandated by high levels of government or through international treaties, but have emerged from the ground up as local, adaptive responses to a real need to protect regional food supplies and human

health from pathogens that know no borders. Third, the networks were not designed to tackle the much larger and complex issues of creating peace between their member states, though they very well may be an opening to further peace agreements. Finally, the networks greatly expand the capacity of any individual member state, giving them a built-in impetus to continue; without the network, each individual state would not only be powerless over outbreaks in neighboring states, but would also be much less capable of tackling diseases within its own borders.

HUMAN FACTORS

Complex human behaviors also appear at the origins of many security problems. Taking a natural history approach to human behaviors, which involves looking at both their evolutionary roots and their commonalities across human groups, can provide valuable insight into their present manifestations. Seemingly irrational behaviors, such as radical fundamentalist belief systems, make more sense when viewed in the context of an evolutionary bias toward forming strong group identity in opposition to outsiders,[37] a bias that has evolutionary origins long predating humans.[38] Villarreal argues that human belief systems are simply the evolved manifestation of self recognition systems that have helped nearly all organisms maintain their autonomy since the earliest interactions between bacteria and viruses. Belief systems can spread through relationship networks. These human networks also share key characteristics with biological networks such as ecosystems, food webs, and social insect relationships.[39] In particular, they show resilience which emanates from many individual components engaged in improving their own fitness. Many successful terrorist networks were found to originate through adolescent friendships developed in radical mosque-sponsored soccer leagues.[40] Although human belief systems have diversified, they show common features across societies – for instance, adolescence as a nearly universal period when ideological, religious, and other beliefs are either abandoned or solidified.[41] These three aspects of belief systems – their deep evolutionary roots, their network-reinforced resilience, and their universal features – suggest that they can't be eliminated entirely, but that alternative pathways provided for adolescents (e.g., soccer clubs sponsored by secular or non-radical religious groups) may be effective in diffusing their most dangerous expressions.

Nonetheless, applying Darwinian ideas to human society inevitably raises ethical issues. Biological evolution is often a tinkering process of trial and error and many individuals die under natural selection. Most societies don't ethically accept the notion of sacrificing individuals to improve security, although engaging in armed conflict implicitly carries some aspects of this (and accordingly raises ethical deliberations). But biologically inspired security systems will not be perfect mimics of nature and they do not have to be beholden to the same forces of selection that operate on natural organisms. We can deliberately select the aspects of natural security systems we would like to incorporate, devise artificial tests of their efficacy, and selectively reproduce only those systems that demonstrate improvements. Already, realistic amateur and professional probing has been used to test the efficacy of security systems, but the results have not necessarily been used to select for better systems. For example, the fallibility of systems that attempt to screen contraband carried by people entering secure

buildings and airport gates was revealed in tests well before Abdulmutallab smuggled incendiary material onto a plane,[42] but the response to both the simulated and actual failure of contraband screening systems has been, in part, to appropriate *more* resources to them.

This equation of human societies rewarding security failures stands in stark contrast to how the rest of the living world deals with failure. In the natural world, failed experiments are eliminated through the process of natural selection, while successful adaptations are rewarded and replicated through survival and relatively higher reproduction. We focus far less on success than on failures in society. For example, the U.S. Coast Guard was roundly criticized for its performance after the relatively small 40,000-gallon Cosco Busan oil spill in San Francisco, but its admirable performance in containing and cleaning 9 million gallons of oil spilled after Hurricanes Katrina and Rita was almost completely ignored.[43] In fact, the massive Townsend after action report on Katrina identified seventeen "Critical Challenges," 125 recommendations, and 243 action items, covering everything from search and rescue to transportation infrastructure to human services, but none of them addressed oil spill cleanup, the one unqualified success after Katrina.[44] At the time, the oil spilled from Katrina was one of the largest oil spills on record, approximately two-thirds the size of the Exxon Valdez spill. Yet so forgotten were the oil spills caused by Katrina that by the time of the 2008 presidential campaign, Republican candidate Mike Huckabee was able to argue publicly that "not one drop of oil was spilled" due to Katrina.[45]

Both the engineering literature and the "organizational learning" literature place a strong emphasis on learning from failure. David Garvin, a leader in studies of organizational learning, argued that BP capitalizes on "constructive failure" which he defined as a failure that provides the critical learning components of "insight, understanding, and thus an addition to the commonly held wisdom of the organization."[46] The image of BP as an organization to emulate was shattered in April 2010, when BP's Deepwater Horizon rig exploded and led to an ecological and economic catastrophe. No doubt, the BP disaster will provide the company with all the components of "constructive failure" as Garvin defined them, but at a cost of greater than $1 billion to the company and with the uncertain economic and environmental impact on the Gulf of Mexico, it's hard to see this kind of learning from failure as something to aspire to.

In part, this discrepancy lies in the selective forces at work or not. In nature, selection is cleanly parsed out in life and death. In society, the selective agents are not so sharp. In both statute and practice, BP was allowed to operate without the necessary backup systems and safeguards;[47] there was no pressure to improve performance in this part of their operations. We would like to think that our congressional representatives could do a better job of rewarding better performance among security and safety agencies, but the complex politics of congressional appropriations (which are often more closely tied to seniority of representatives than the merits of the funded projects) have created an enormous disconnect between performance and reward that is not likely to be repaired soon.

It is often news media that plays the strongest selective agent. After the Cosco Busan spill, images of hundreds of frustrated San Francisco volunteers waiting to clean up oiled birds, but held back by Government bureaucrats, were rolled on national media.

These kinds of images result in calls to Congress and demands for investigations. By contrast, the Coast Guard's work on the post-Katrina and Rita oil spills hardly made newsworthy footage relative to images of people stranded on the roofs of their flooded houses. Because so much of the selective force on government agencies, especially when it comes in the form of media attention, focuses on mistakes (cost overruns, terrapin-like foot dragging, and botched responses), adapting based on success is not something that can be instilled from the top down. We cannot (and would not want to) order media outlets to only report good news.

Accordingly, the onus is on operatives at much smaller levels of government – battalion commanders, local police chiefs, and bureau heads – to identify successes, even if they were just one part of an operation that mostly failed, and to reproduce them. Sometimes this will mean promoting the people responsible for the success. Sometimes it will mean allocating more of a budget to activities that demonstrated success. But even where these local agents lack the power or resources to dole out these material rewards, they do have a very powerful and very inexpensive resource at their disposal. They can reproduce successes by teaching others in their field how to adopt their successful activities. This kind of teaching and learning is best facilitated through small informal networks of practitioners. For example, the armed forces have used intranets, such as NCOcorps.net, to give soldiers in Iraq and Afghanistan a forum to share information about successful practices as experienced by troops in the field.[48] This peer-to-peer training turns out to be an invaluable resource to new soldiers who come into combat with much less experience, and therefore much less adapted, than the insurgents that they will be fighting. Indeed, this method of replication brings us full circle back to the adaptability of decentralized organizations, as illustrated in the following case study of improvised explosive device (IED) attacks in Afghanistan and Iraq.

A CASE STUDY: IED Attacks in Iraq and Afghanistan

The case of IED deaths in Iraq and Afghanistan illustrates several points relevant to natural security. The issue of IED came to most civilian's attention in a dramatic fashion on December 8, 2004, during a televised visit between Secretary of Defense Donald Rumsfeld and National Guard soldiers preparing for deployment in Kuwait. To the cheers of the soldiers assembled, Specialist Thomas Wilson, a thirty-one-year-old Tennessee National Guardsman, pointedly asked the secretary why he and his fellow soldiers were being forced to rummage through garbage dumps to find armor to strap on to their vehicles, which provided inadequate protection in the combat zone. Rumsfeld was initially taken aback, then tartly retorted "you go to war with the Army you have."[49]

The terse exchange belied a critical difference in *adaptability* between soldiers like Specialist Wilson and a large security organization like the Department of Defense. For the troops on the ground, the process of adapting began soon after the invasion of Bagdad. They "went to war with the Army they had" (to paraphrase Rumsfeld), and it worked brilliantly for a while. With superior firepower, training, and air superiority, even the most feared of Saddam Hussein's forces virtually collapsed in front of the advancing coalition force. But as the old regime collapsed, the ground became rich for

any number of new threats to sprout up. The threat environment radically changed. Suddenly, thousands of soldiers, independently as individuals and linked through the units they fought with, were observing that hidden improvised explosive devices (IED) were becoming their biggest threat to security. Whereas the DoD had planned for a war against AK-47s, Scud Missiles, and weapons of mass destruction, soldiers on the ground began to see their enemies as random trash piles, sudden fender benders in downtown traffic, and cell phones; hiding, distracting from, and detonating IED. By the time Wilson was so incensed as to dare breach military protocol to give a superior officer a dressing down, 266 of his colleagues had been killed due to IED.[50] (Fig. 3)

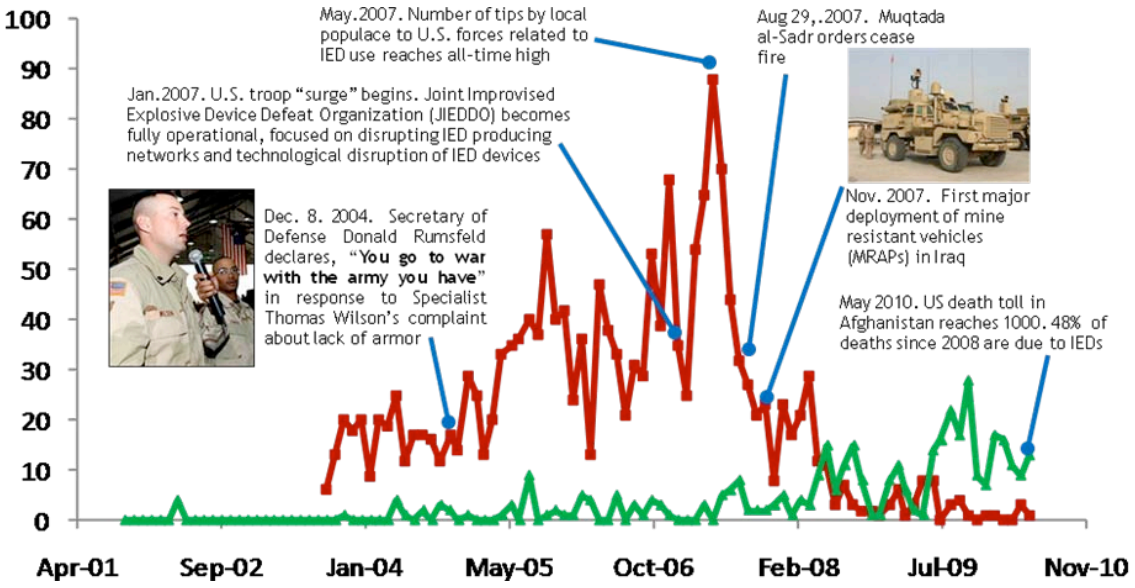


Figure 3. Deaths per month of U.S. troops in Iraq (red) and Afghanistan (green) and associated security related events. Data source: www.icasualties.org.

The soldiers adapted the best that they could, welding metal plates to their vehicles, blocking up culverts to eliminate the most obvious niches for bombers to use, and learning to identify the signs of hidden bombs in otherwise unremarkable debris. But their ability to adapt was limited by forces beyond their control – by the equipment they were given, by the available scrap metal, by the rules of engagement that they were ethically and legally bound by – and the casualties mounted.

By contrast, the Department of Defense had virtually unlimited resources, especially after 9/11 when no politically-minded congressperson or senator would ever turn down a military appropriation request. What the DoD lacked was adaptability. Even as Specialist Wilson and his comrades were frantically tracking the rapidly changing tactics of insurgents, the DoD was slowly churning away on weapons systems and fighting procedures that had been dreamed up long ago in places far away from the streets of Baghdad and Fallujah. Rumsfeld's retort to Wilson revealed a centralized view where small numbers of intellectuals design a battle plan and the accompanying technology years in advance, *and that's what you go to war with*. Moreover, even to bring the

idealized technological solutions to deal with the threats theorized by DoD experts, the Department was bound by a ponderous top-down procurement system in which a small number of large contractors submitted bids for development of weapons systems that inevitably ran over budget and beyond the estimated timeline. Even after congressional outrage from the exchange between Wilson and Rumsfeld fueled calls to speed up production and deployment of mine-resistant ambush-protected vehicles (MRAP), they did not arrive in Iraq in until November 2007 – nearly three years later. By that time, an additional 1,589 of Wilson's colleagues had been killed in IED attacks.

The DoD solution certainly arrived too late to save their lives, but also too late to even deal with the original threat. A rapid downward trend in IED attacks and deaths was already well on its way by the time the MRAP arrived in Iraq. This downward trend can largely be linked to the successful fostering of two sets of symbiotic relationships in Iraq. First, General Petreaus authorized a shift in strategy towards engaging local populations to break up IED-producing networks, which resulted in increasing numbers of tips to soldiers about IED operations. Second, an inter-service partnership between ground soldiers and electronic warfare experts that devised methods to disarm wirelessly detonated IED greatly reduced the effectiveness of the remaining IED.[51]

The lesson here is that adaptation is primarily forged out of behaviors and relationships that can respond to a changing environment, not out of material solutions. Indeed, the MRAP that arrived too late in Iraq were ready just in time for a renewed offensive in the long-simmering war in Afghanistan. They have undoubtedly saved the lives of soldiers who were hit by IED, but they certainly haven't led to a decline in IED attacks or deaths, and may in fact have attracted more IED attacks. This is because the environment of Afghanistan is much more rugged than that of Iraq, making most of the country downright impassable to 14- to 24-ton vehicles like the MRAP.[52] Taliban operatives in inexpensive second-hand Toyota pickup trucks (probably the most adaptable vehicle ever built) could operate at will without interference from the lumbering U.S. forces. The few roads in Afghanistan that were MRAP accessible quickly became targets for IED attacks (which had been only a minimal threat up until this point) so that travel became a cumbersome affair, sometimes taking all day to move twelve kilometers or so.[53] In fact, after only two years of deployment, nearly half of the 16,000 MRAP produced (at a cost of $500,000 each) are being put on "inactive status".

What does this tale of differential adaptation tell us? First, adaptation requires leaving or being forced from your comfort zone and into a place where you observe and experience new threats to your security. Second, adaptation takes resources, but resources don't guarantee adaptation. Third, parts of an organization can be adaptable even if the organization is non-adaptable as a whole. Fourth, an adaptation developed for a given threat in a given environment may be useless, or even counterproductive, in a different environment.

LESSONS FOR AN ADAPTABLE FUTURE

It is important to recognize that the untapped secrets of natural security systems are not classified in any way. Rather, they are laid out in the structure of fossil and living organisms, in fragments of DNA, and in the observable behaviors of the organisms themselves. Translating ideas from nature into usable security solutions in society

requires sensitivity to both how humans and human societies are different from other evolutionary systems, but also their common roots and analogous dynamics. Overall, the goal of a natural security system is to help society live with risks, rather than waste resources trying to eliminate them, by developing and maintaining adaptive security systems. An analysis of biological security systems suggests that a cascading set of interrelated strategies can provide the best means for dealing with the variation and uncertainty in nature.

In society, a cascade towards adaptive security can be initiated by giving more power to individual agents to sense and respond to threats. These agents could be individual people in a community, or individual offices, agencies, or states responsible for discrete aspects of a larger security mission. They do not operate completely independently, but rather are empowered through problem-solving challenges issued by an agency that has the resources or power to implement solutions. Multiple agents devising and testing a variety of security systems will provide greater likelihood of finding efficient solutions, redundancy to hedge against poor solutions, and potential for more rapid adaptation if selection pressures (such as budgets or media coverage) can be aligned to reward successful adaptations. Symbiotic partnerships between these agents can then extend their utility by bringing new skills and perspectives into emerging problem solving networks.

Given the vast diversity of life, we have only scratched the surface of potential lessons from nature for security in society. For example, biologists understand that organisms in nature inherently accept that risk is inevitable in the environment and, through selection, manage to balance the costs and benefits of developing new adaptations. But we have little ability to predict why certain types of adaptations will arise in a given place or time, which could then reflect on how society could optimally manage a portfolio of emerging and existing risks. Getting closer to this understanding may involve a deeper appreciation (using appropriate biological models such as the immune system and host-parasite interactions) of how particular adaptations take place in a range of situations – are they the product of escalation through repeated direct interactions, a response to chronic stress, or a generalized response to cope with a potential range of natural variation? Additionally, focusing on rapid adaptation and rapid feedback cycles – such as occur with retroviruses which manage to hijack the adaptive machinery of the immune system and use it against the host body – could be enormously important as a model for understanding how radical ideas are now rapidly spread peer-to-peer using simple messaging between previously unlinked terror groups. This same model could be adapted to aid with the likely need to adapt rapidly to climate change. Finally, my group has largely focused on evolutionary successes, but the history of life is replete with apparently well-adapted organisms that went extinct. What are the conditions under which even organisms that sense the environment well and reduce their own uncertainty go extinct and what can this tell us about our own failures? This reminds us of a sobering basic tenet of natural security: those who embrace the process of adaptation survive and thrive, those who don't, go extinct.

Raphael Sagarin is a marine biologist and research scientist at the Institute of the Environment at University of Arizona. Dr. Sagarin's work on using biological evolution as a guide for improving societal security systems began during his tenure as a Geological Society

of America Congressional Science Fellow in the office of U.S. Representative (now Labor Secretary) Hilda Solis. His research has appeared in Science, Nature, Conservation Biology, Foreign Policy *and other leading journals. He received his doctorate from the University of California, Santa Barbara in 2001. Dr. Sagarin may be contacted at* rafe@email.arizona.edu.

---

[1] "Migrants Finding Ways to Climb 18-foot-tall Border Fence," *Arizona Republic*, November 15, 2008, http://www.tucsoncitizen.com/ss/related/102700.

[2] See, for example, NOAA Technical Memorandum NMFS-SEFC-278 (NOAA Scientific Publications Office), http://spo.nwr.noaa.gov/.

[3] National Commission on Terrorist Attacks Upon the United States, *The 9/11 Commission Report* (Washington, DC: 2004). Several major news organizations and private blogs from different political persuasions used the "failure of imagination" line in their headlines or leads in coverage following the release of the report, including: National Public Radio, http://www.npr.org/911hearings/; *Perrspectives*, http://www.perrspectives.com/blog/archives/000010.htm; Radio Free Europe Radio Liberty, http://www.rferl.org/content/article/1053987.html; *The Christian Science Monitor*, http://www.csmonitor.com/2004/0723/p01s03-uspo.html; CNN.com, http://www.cnn.com/2004/ALLPOLITICS/07/22/911.report/index.html.

[4] Food and Agriculture Organization of the United Nations, *Hunger in the Face of Crisis* (New York: United Nations, 2009).

[5] Charles Darwin, *Voyage of the Beagle* by Charles Darwin, with a new introduction by David Quammen (Washington, DC: The National Geographic Society, 2004).

[6] Stott, Rebecca, *Darwin and the Barnacle* (New York: W.W. Norton & Company, 2003).

[7] Geerat Vermeij, *Nature: An Economic History* (Princeton, NJ: Princeton University Press, 2004).

[8] Ori Brafman and Rod A. Beckstrom, *The Starfish and the Spider: The Unstoppable Power of Leaderless Organizations* (New York: Penguin Group, 2006).

[9] Paul Hawken, *Blessed Unrest: How the Largest Movement in the World Came into Being and Why No One Saw It Coming* (New York: Viking Press, 2007).

[10] Jean Francois Rischard, "Global Issues Networks: Desperate Times Deserve Innovative Measures," *The Washington Quarterly* 26, no. 1 (2002): 17-33.

[11] Bala Iyer and Thomas H. Davenport, "Reverse Engineering Google's Innovation Machine" *Harvard Business Review* (2008): 58-68.

[12] J. Ginsberg, M. H. Mohebbi, R. S. Patel, L. Brammer, M. S. Smolinski, and L. Brilliant, "Detecting Influenza Epidemics Using Search Engine Query Data," *Nature* 457, no. 7232 (2009): 1012-U4.

[13] These results can be found at https://networkchallenge.darpa.mil.

[14] D.T. Blumstein, "The Evolution, Function, and Meaning of Marmot Alarm Communication," *Advances in the Study of Behavior* 37 (2007): 371-400.

[15] Aaron S. Rundus, Donald H. Owings, Sanjay S. Joshi, Erin Chinn, and Nicholas Giannini, "Ground Squirrels Use an Infrared Signal to Deter Rattlesnake Predation," *Procedings of the National Academy of Science* 104, no. 36 (2007): 14372-76.

[16] D.T. Blumstein, L. Verneyre, and J.C. Daniel, "Reliability and the adaptive utility of discrimination among alarm callers," *Proceedings of the Royal Society of London Series B-Biological Sciences* 271 (2004): 1851-1857, doi:10.1098/rspb.2004.2808.

[17] Data available at http://www.dhs.gov/xabout/history/editorial_0844.shtm.

[18] John Nance, "Has Airport Security Improved Since 9/11 or Not?" *ABC News*, October 31, 2006, http://abcnews.go.com/Technology/story?id=2618488&page=1; Jeanne Meserve, "Airport screeners failed to find most fake bombs, TSA says," *CNN*, October 18, 2007, http://www.cnn.com/2007/TRAVEL/10/18/airport.screeners/index.html.

[19] S.E. Martonosi and A. Barnett, "How Effective Is Security Screening of Airline Passengers?" *Interfaces* 36, no. 6 (2006): 545-52.

[20] National Commission on Terrorist Attacks Upon the United States, *The 9/11 Commission Report* (Washington, DC: 2004), referring to the arrest of Zacarais Moussaoui.

[21] United States Department of Homeland Security, "Statement of David Heyman, Assistant Secretary for Policy," in *Senate Committee on Commerce, Science, and Transportation* (2010), http://commerce.senate.gov/public/.

[22] A full list of these airports is available at http://www.tsa.gov/press/where_we_stand/training.shtm.

[23] Doug Mills, "Faces, Too, Are Searched at U.S. Airports, " *New York Times*, August 17, 2006.

[24] United States Government Accountability Office, "Efforts to Validate TSA's Passenger Screening Behavior Detection Program Underway, but Opportunities Exist to Strengthen Validation and Address Operational Challenges" (Washington, DC: GAO, 2010).

[25] J.K Burgoon, D. P. Twitchell, M. L. Jensen, T. O. Meservy, M. Adkins, J. Kruse, A. V. Deokar, G. Tsechpenakis, S. Lu, D. N. Metaxas, J. F. Nunamaker, and R. E. Younger, "Detecting Concealment of Intent in Transportation Screening: A Proof of Concept," *IEEE Transactions on Intelligent Transportation Systems* 10, no. 1 (2009): 103-12.

[26] William A. Wulf and Anita K. Jones, "Reflections on Cybersecurity.," *Science* 326 (2009): 943-44.

[27] Industrial Control Systems Cyber Emergency Response Team, "USB Drives Commonly Used as an Attack Vector against Critical Infrastructure" (U.S. ICS-CERT, 2010), http://www.us-cert.gov/control_systems/pdf/ICS-CERT%20CSAR-USB%20USAGE.pdf.

[28] Laura Spinney, "Tools maketh the monkey," *New Scientist,* October 11, 2008, 42-45.

[29] Dominic D. P. Johnson, "Darwinian Selection in Asymmetric Warfare: The Natural Advantage of Insurgents and Terrorists" *Journal of the Washington Academy of Sciences* (Fall 2009): 89-112.

[30] Air National Guard Maj. N. Lipana, personal communication with the author.

[31] P. Eisler, "Insurgents Adapt Faster Than Military Adjusts to IEDs," *USA Today*, July 16, 2007.

[32] J. Henrich and R. McElreath, "The Evolution of Cultural Evolution," *Evolutionary Anthropology* 12, no. 3 (2003): 123-35.

[33] E.I. Svensson, "Understanding the Egalitarian Revolution in Human Social Evolution," *Trends in Ecology & Evolution* 24, no. 5 (2009): 233-35; K. Sigmund, "Punish or Perish? Retaliation and Collaboration among Humans," *Trends in Ecology & Evolution* 22, no. 11 (2007): 593-600.

[34] John Horgan, "The End of War," *NewScientist*, July 4, 2009, 38-41.

[35] K.L. Cheney, R. Bshary, and A. S. Grutter, "Cleaner Fish Cause Predators to Reduce Aggression toward Bystanders at Cleaning Stations," *Behavioral Ecology* 19, no. 5 (2008): 1063-67.

[36] A. Leventhal, A. Ramlawi, A. Belbiesi, and R.D. Balicer, "Regional collaboration in the Middle East to deal with H5N1 Avian Flu," *British Medical Journal* 333 (2006): 856-858.

[37] M.E. Hochberg, "A Theory of Modern Cultural Shifts and Meltdowns," *Proceedings of the Royal Society of London Series B-Biological Sciences* 271(2004): S313-S316, doi:10.1098/rsbl.2004.0172.

[38] Luis P. Villarreal, "From Biology to Belief," in Raphael Sagarin and Taylor Terence, eds., *Natural Security: A Darwinian Approach to a Dangerous World* (Berkeley, CA: University of California Press, 2008), 42-68.

[39] E.G. Leigh and G. J. Vermeij, "Does Natural Selection Organize Ecosystems for the Maintenance of High Productivity and Diversity?" *Philosophical Transactions of the Royal Society of London Series B-Biological Sciences* 357, no. 1421 (2002): 709-18; Simon A. Levin, "Ecosystems and the Biosphere as Complex Adaptive Systems," *Ecosystems* 1 (1998): 431-36.

[40] House Appropriations Subcommittee on Homeland Security. *The Making of a Terrorist: A Need for Understanding from the Field* (Washington, DC: March 12, 2008).

[41] Richard Sosis and Candace S. Alcorta, "Militants and Martyrs: Evolutionary Perspectives on Religion and Terrorism," in Raphael Sagarin and Taylor Terence, eds., *Natural Security: A Darwinian Approach to a Dangerous World* (Berkeley, CA: University of California Press, 2008), 105-24.

[42] "Airport insecurity," *The Seattle Times* , July 11, 2004); M.L. Goldstein, "Preliminary Results Show Federal Protective Service's Ability to Protect Federal Facilities is Hampered by Weaknesses in its

Contract Security Guard Program" (Washington, DC: United States Government Accountability Office, 2009).

[43] Coast Guard Lt. Rhianna Strickland in personal comments to author, Febrary 2009.

[44] The White House, *The Federal Response to Hurricane Katrina Lessons Learned* (Washington, DC: 2006).

[45] "Fox News contributor Mike Huckabee falsely claimed 'not one drop of oil was spilled' during Hurricane Katrina," *MediaMatters,* July 27, 2008, http://mediamatters.org/research/200806270005.

[46] D.A. Garvin, "Building a Learning Organization," *Harvard Business Review* 71, no. 4 (1993): 78-91.

[47] M.Turnipseed, R. Sagarin, P. Barnes, M. C. Blumm, P. Parenteau, and P. H. Sand, "Reinvigorating the Public Trust Doctrine: Expert Opinion on the Potential of a Public Trust Mandate in U.S. and International Environmental Law," *Environment* 52, no. 5 (2010): 6-14.

[48] Information available at http://www.ncocorps.net/more/army_nco_site.htm.

[49] "Troops grill Rumsfeld over Iraq," *BBC News,* December 8, 2004, http://news.bbc.co.uk/2/hi/middle_east/4079201.stm; "Rumsfeld gets earful from troops," *Washington Post,* December 8, 2004, http://www.washingtonpost.com/wp-dyn/articles/A46508-2004Dec8.html; "Soldiers must rely on 'hillbilly armor' for protection," *ABCNews.com* (n.d.), http://abcnews.go.com/WNT/story?id=312959&page=2.

[50] IED casualty figures are drawn from www.icasualties.org.

[51] Major Noel Lipana, Air National Guard, personal comments to author, September 2009.

[52] Andrew Feickert, "Mine-Resistant, Ambush Protected (MRAP) Vehicles: Background and Issues for Congress," Congressional Research Service, ed. (Washington, DC: Library of Congress, 2008).

[53] Reporter Nir Rosen, personal comments to author, January 29, 2010

More is Better: The Analytic Case for a Robust Suspicious Activity Reports Program

James E. Steiner

In his March 2009 testimony, Gregory Nojeim warned Congress of the potential danger to civil liberties posed by the government's suspicious activity report (SAR) program. But Nojeim, director of the Project on Freedom, Security, & Technology, raised another concern – that "the security 'bang per byte' of information gathered may be diminishing. While 'stove piping' was yesterday's problem, tomorrow's problem may be 'pipe clogging,' as huge amounts of information are being gathered without apparent focus."[1] In concluding his testimony, Nojeim recommends:

> The Subcommittee should test whether SAR reporting is both effective and efficient in preventing terrorism…. SAR reporting may or may not be the best way to collect the 'dots' that need to be connected to head off terrorist attacks; whether it is or is not should be tested. Because the SAR reporting system will result in the collection of so much information about innocent activities, it seems that it would be good to know at the front end that the results are likely to be worth the risks.[2]

A subsequent CRS study, in November 2009, endorsed Nojeim's suggestion questioning the need for a data-intensive program and made a similar recommendation: "Congress may be interested in how a future SAR Program Management Office intends to address this problem – specifically, which agency or agencies will be responsible for quality control of SARs [sic] to prevent system overload from irrelevant or redundant ones."[3]

This article acknowledges the progress made in protecting civil rights – an area of legitimate concern – but rejects categorically the call to reduce or limit the size of the SAR program. Two analytic requirements for the collection of more rather than less information through the SAR process are presented, to increase the probability of identifying pre-operational terrorist activity and to improve the efficiency and effectiveness of critical infrastructure protection regimes. In statistical analysis, more is better.

The SAR Program and Process

Since 2007, the U.S. homeland security, law enforcement, and intelligence communities have formally recognized the usefulness of SAR in counterterrorism. The U.S. government defines a SAR as "official documentation of observed behavior that may be indicative of intelligence gathering or pre-operational planning related to terrorism, criminal, or other illicit intention."[4] The primary impetus for the federal government's National SAR Initiative (NSI) is intelligence support to law enforcement, although officials from the critical infrastructure (CI) protection world have recognized that SAR can help them improve their performance.

Law enforcement has been collecting SAR (or something similar, such as field interviews of suspicious individuals) for decades. The NSI program endeavors to formalize a nationwide, uniform process for evaluating and recording this information and then making it available to appropriate personnel and organizations through the

Information Sharing Environment (ISE). The SAR concept and the NSI were both originally developed to provide direct support to law enforcement. Here is the typical process in brief: law enforcement intelligence analysts receive and evaluate all new SAR. In those relatively rare cases where a single SAR is both credible and actionable, the information is embedded in a short analytic report and provided directly to law enforcement for immediate counterterrorism action. These leads go to the local Joint Terrorism Task Force (JTTF), which has first right of refusal in terrorism cases. If the JTTF chooses not to follow-up, the lead is passed to state or local police for action. The figure below illustrates the Notional SAR Process in detail.[5]

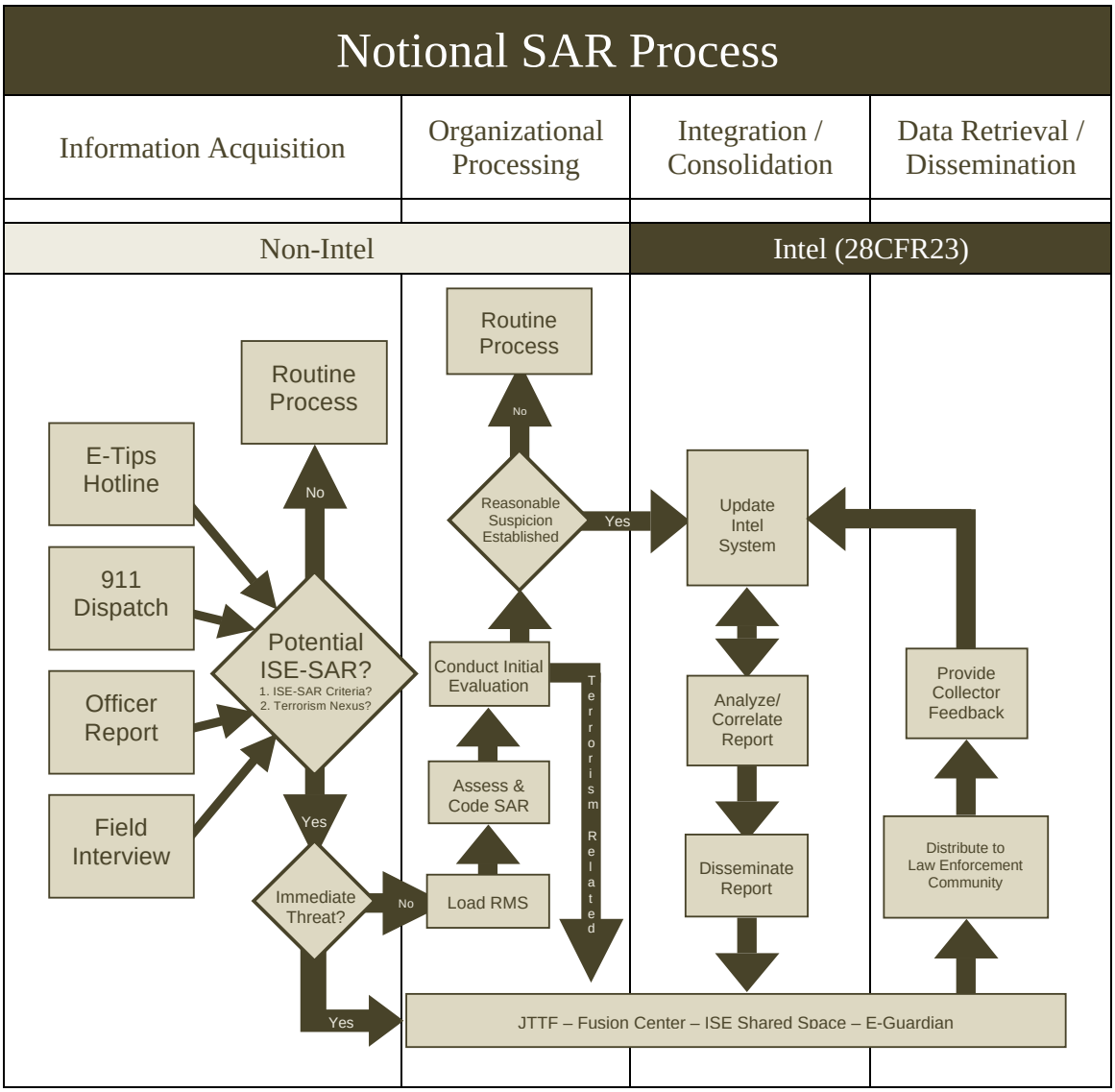


Figure 1. Notional SAR Process

This graphic has a familiar feel since it shows the traditional intelligence cycle as applied to suspicious activity reports. It begins with collection (information acquisition), moves to the (organizational) processing of that information, then on to analysis (integration/consolidation) and ends with final dissemination (and data retrieval) of the SAR and SAR-based analysis to the law enforcement customer (JTTF). Although not shown clearly, the cycle is completed through the "feedback to the collector" function in the last column of the graphic.

SAR originate from a wide variety of sources, including law enforcement officers, public and private sector security, and the public through "phone in" calls to hotlines, and are reported to a large number of federal, state, local, tribal, and territorial law enforcement organizations. From an intelligence perspective, the lack of direct control over some of these intelligence sources results in exceptional difficulty in assessing the quality of SAR. The NSI/ISE leadership is acutely aware of this problem as highlighted in the original "Nationwide Suspicious Activity Reporting Initiative Concept of Operations":

> A standard reporting format is a key element of the effective implementation of a SAR program. A standardized report provides a mechanism for the efficient transition of the suspicious activity from the line-level officer to the agency management. This process will ensure that the suspicious activity is being collected and reported correctly and will regulate the reporting procedures across the agency.
>
> Additionally, in order to identify local, regional, and national trends in crime and terrorist precursor activity, a common national set of data collection codes needs to be adopted to ensure seamless sharing and analysis of suspicious activity. This national standard of codes will ensure that patterns of criminal behavior are identified and handled properly. The establishment of these codes needs to be the result of evaluation and determination that the activities to be collected are likely precursors of terrorist activity."[6]

If anything, this focus on SAR quality (a necessary condition for using SAR in the analytic process) has increased as seen in the extensive treatment dedicated in the "Final Report: Information Sharing Environment – Suspicious Activity Reporting Evaluation Environment."[7]

Legitimate Civil Rights Concerns

Coming from a civil liberties perspective, Nojeim is most concerned about the range and number of collectors and the fact that despite a plethora of "quidelines" for collecting, handling, and storing SAR, the *collection guidelines "fail to provide adequate guidance"* (emphasis added).[8] This legitimate issue raised by Nojeim was directly addressed by the NSI/SAR leadership in developing their January 2010 report on the NSI-SAR Evaluation Environment. In fact, no less an organization than the ACLU has provided kudos to the NSI SAR leadership, its efforts, and its results:

> The ACLU released a report criticizing these SAR programs in July 2008. In response, ISE program manager Thomas E. McNamara and his office worked with the ACLU and other privacy and civil liberties groups, as well as the LAPD and other federal, state and local law enforcement agencies, to revise the ISE SAR functional standard to address privacy and civil liberties concerns.

> The revised ISE guidelines for suspicious activity reporting, issued in May 2009, establish that a reasonable connection to terrorism or other criminal activity is required before law enforcement officers may collect Americans' personal information and share it within the ISE…. The revised ISE functional standards also make clear that behaviors such as photography and eliciting information are protected under the First Amendment, and require additional facts and circumstances giving reason to believe the behavior is related to crime or terrorism before reporting is appropriate. These changes to the standard, which include reiterating that race, ethnicity and religion cannot be used as factors that create suspicion, give law enforcement all the authority it needs while showing greater respect for individuals' privacy and civil liberties. *We applaud the willingness of the ISE Program Manager to engage constructively with the civil liberties community and to make significant modifications to the functional standard to address the concerns presented* (emphasis added).[9]

So far, so good. The civil liberties community and the SAR leadership agree that privacy issues are being addressed through guidance on how to handle such information.

Criticism Beyond Civil Liberties

Unfortunately the ACLU also picked up and repeated Nojeim's concern over the sheer *volume* of SAR, implying that a smaller program would be better in terms of program efficiency and effectiveness. In other words, these civil rights advocates and organizations are now evaluating the analytic merits of intelligence officers having more or less data available to do their job, a subject well beyond their civil liberties expertise.

Specifically, the ACLU continues:

> This overbroad reporting mandate is not just constitutionally questionable; it's also counterproductive. *These orders, if taken seriously by local law enforcement, can yield only one outcome: an ocean of data about innocent individuals that will overwhelm the investigative resources of the authorities* (emphasis added).[10]

In fact, this final conclusion is both naïve and incorrect. Intelligence analysts actually need an "ocean of data" concerning suspicious activity (but NOT the personal identities of those engaging in such activity) to successfully apply sophisticated statistical analysis techniques that have the potential to discern between benign activity and true terrorist precursor activity, thereby reducing the investigative load. Similarly, analysis of comprehensive data on suspicious but benign behavior near critical infrastructure is the first step in developing security programs to protect that infrastructure.

Why Analysts Need a Massive SAR Database

Figure 2 lays out a simplified representation of intelligence-led SAR support to law enforcement. As shown by the two arrows leading to law enforcement actions, there are two ways SAR-based intelligence reaches police authorities. The direct approach was discussed above and is straightforward. In the rare cases where a SAR is a clear indicator of threat, the SAR information moves quickly and directly from the intelligence realm to law enforcement for investigation.

The "indirect" method is fundamentally distinct from the direct method. In the indirect case, each new SAR is processed and evaluated by both intelligence and critical infrastructure analysts to determine whether there are *non-obvious* reasons for law

enforcement follow-up. To accomplish this task, the analysts must determine whether the new SAR is an anomaly when compared to the results of "pattern analysis models."

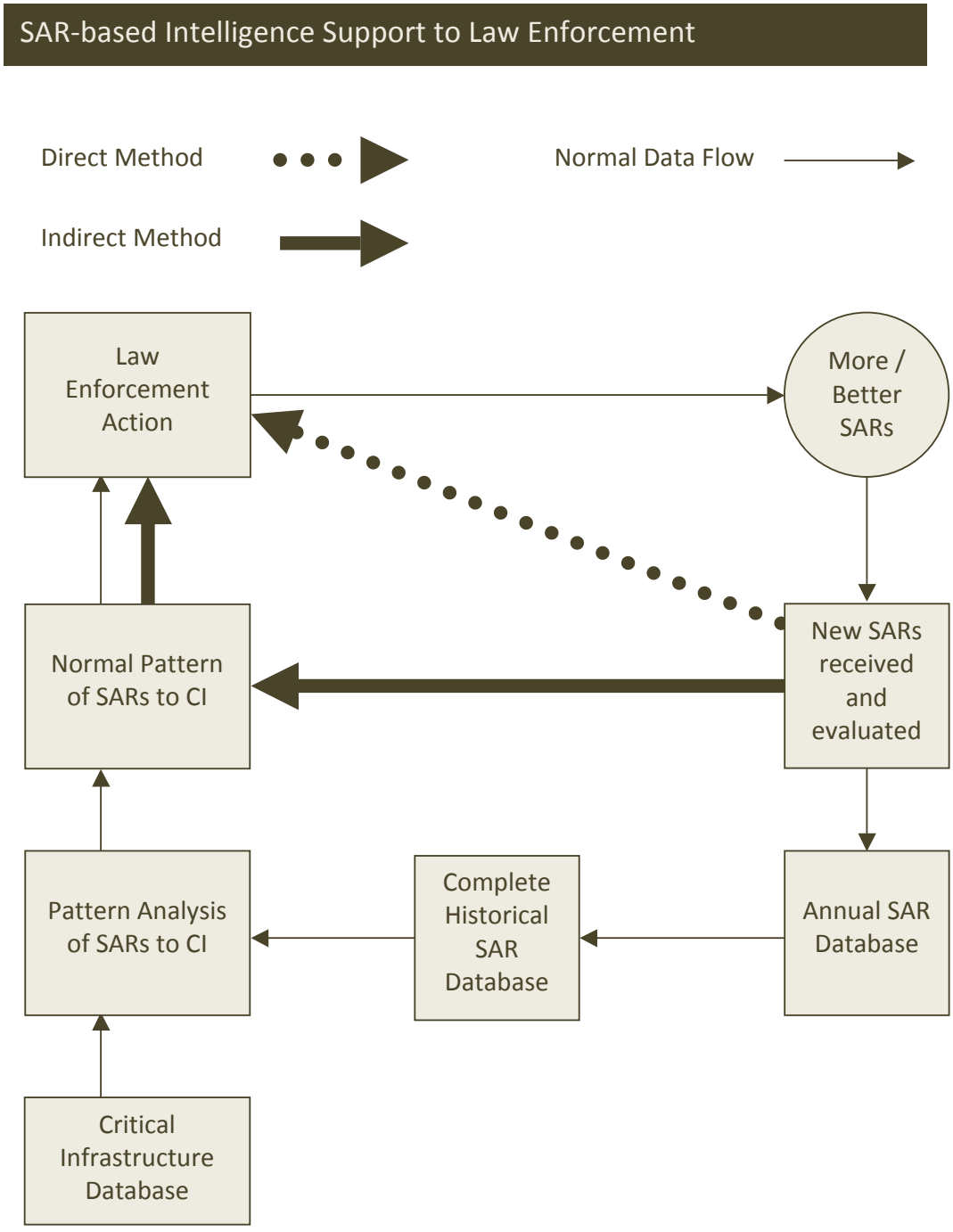


Figure 2. SAR-based Intelligence Support to Law Enforcement

Here is a brief summary of how such models and their results are generated. First, intelligence analysts format and evaluate all new SAR (a major task as noted above) and add them to the "complete historical SAR database." This database is then used with a similar (in that both are geo-rectified) database that holds information on critical infrastructure (CI) to feed the pattern analysis models, which, in turn, yield the "Normal Pattern of SAR" for each element of the CI. Critical Infrastructure analysts are responsible for generating the CI Database, which contains GIS and other information on each facility. Now for a closer look.

The Theoretical Foundation of the Indirect Approach

Given the obvious problems with using SAR as "intelligence," a number of professional intelligence officers have resisted spending scarce resources collecting and analyzing them. In the foreign intelligence world, a significant premium is placed on recruiting well-placed, reliable sources that can report raw intelligence that addresses specific collection requirements. Obviously, there is an effort by domestic law enforcement to utilize similar human sources (confidential informants) and technical collection (court approved wiretaps) to collect high-grade information. In the foreign arena, our intelligence agencies have been successful in collecting significant information on terrorist groups, their numbers, leaders, tactics, and techniques. This reporting has been used extensively in preparing analyses (target studies) at both the tactical and strategic levels. But within the U.S. domestic theatre, there just have not been many specific, credible reports on planned terrorist attacks within the U.S. since the 9/11 attacks. Although few in numbers, specific, credible intelligence reports have been critical in preventing terrorist attacks and both intelligence and law enforcement are actively seeking to acquire more such information.

On the other hand, there have been tens (possibly hundreds) of thousands of domestic suspicious activity reports collected in the U.S. by state and local law enforcement since 9/11. Statistically, the probability of any single SAR being an indicator of an actual terrorist plot is so small that it is insignificant. But the greater the number of SAR, the greater the overall probability that at least a few real indicators of threat exist within the total body of SAR reporting.

Most domestic intelligence practitioners characterize the counter-terrorism problem as separating the signal (the very rare true indicator of a terrorist threat) from the noise (the huge number of meaningless or benign SAR). For example, in 2009-2010 the FBI reports that of the 3,400 SAR entered into its system,[11] only fifty-six of these (less than 2 percent) merited an actual investigation.[12]

The indirect approach for using SAR to identify true threats harnesses the power of statistics and analysis to solve the signal/noise problem. Here is an example of the technique. Let's say there are 100 widget factories in the country and that we think (based on credible, specific intelligence regarding terrorist intent) that there is a near-term plot to attack one such factory. The challenge is to identify which particular widget factory is being targeted. Our understanding of how terrorists plan an attack tells us that operatives are likely to conduct at least a few surveillance operations before an attack. Further, we have collected a large number of SAR at or near the 100 widget factories over the past nine years – let's say 90,000 – roughly 100 SAR per plant per year. Obviously, if we are very lucky we will be able to identify the four or five of these 90,000

SAR that are true terrorist surveillance and immediately notify law enforcement and critical infrastructure protection to take appropriate actions.

But the likelihood of being so fortunate in identifying the actual SAR that are strong indicators of the targeted factory by examining each of the 90,000 relevant SAR is remote.

We have a much better chance of identifying a real indication of a threat if we characterize the challenge as defining the "normal" laydown of SAR at a widget factory with enough specificity to enable us to recognize a situation or SAR that is not normal. For example, if we can use our complete data set of SAR to develop a reliable expected pattern of SAR on any given target or area, then a significant deviation from that pattern is by definition an anomaly that deserves further investigation.

This approach is grounded in the "Law of Large Numbers."

In probability theory, the Law of Large Numbers (LLN) is a theorem that describes the result of performing the same experiment a large number of times. According to the law, the average of the results obtained from a large number of trials should be close to the expected value, and will tend to become closer as more trials are performed.

For our widget factory, here is how the LLN might work in action. We take the full dataset of 90,000 SAR on widget factories and *if* this total number of SAR is large enough and *if* every facility is collecting and reporting SAR in a uniform and consistent fashion, then we should be able to develop a model which will tell us if there are an unusually large number or type of SAR at any given widget plant. We can do this because quantitative methodologists, working with intelligence and critical infrastructure analysts, can now construct a model that defines the normal pattern of SAR for each unique widget plant. This model actually forecasts the number and characteristics of SAR expected at each widget plant during a particular time period and a statistically significant deviation from this expected value would constitute an indicator of unusual (and possibly terrorist) activity. Obviously, from the LLN we know that the larger our complete database of SAR, the more reliable our "expected value." Note that intelligence analysts do not require any personal information on those conducting the suspicious activity to conduct their analysis.

While theoretically feasible, the practical problems involved in constructing and maintaining a SAR database in which there is consistency and uniform treatment of the collection and coding of the data (SAR) might well be impossible to overcome, at least in the near term. For example, the data set on SAR must be huge, relatively consistent, and comprehensive to enable robust analysis. One need only consider the fact that there are over 18,000 local, state, and federal law enforcement organizations within the U.S. collecting and reporting SAR to begin to understand and to size the obstacles to full and effective implementation. On the other hand, the cost of overcoming these difficulties and uncertainties must be counterbalanced against the potential payoff of preventing a successful terrorist attack, either by direct law enforcement action or through improved critical infrastructure (CI) protection.

SAR Support to Critical Infrastructure (CI) Protection

The second argument for a robust SAR program is its largely unrecognized role in CI protection. The DHS website states:

> CI (Critical Infrastructure/Key Resources) is an umbrella term referring to the assets of the United States essential to the nation's security, public health and safety, economic vitality, and way of life. CI is divided into 18 separate sectors, as diverse as agriculture and food, emergency services, and cyber networks. [See below.]
>
> Because this critical infrastructure provides our country with the enormous benefits, services and opportunities on which we rely, we (DHS) are very mindful of the risks posed to CI by terrorists, pandemic diseases and natural disasters. At the Department of Homeland Security, we know that these threats can have serious effects, such as cutting populations off from clean water, power, transportation, or emergency supplies.
>
> Secretary Napolitano is working to raise awareness about the importance of our nation's critical infrastructure, and strengthen our ability to *protect* it [emphasis added]. The Department oversees programs and resources that foster public-private partnerships, enhance protective programs, and build national resiliency to withstand natural disasters and terrorist threats.[13]

The 18 DHS Defined Critical Infrastructure Sectors	
Agriculture & Food	Emergency Services
Banking & Finance	Energy
Chemical	Government Facilities
Commercial Facilities	Information Technology
Commercial Nuclear Reactors, Materials, & Waste	National Monuments & Icons
Critical Manufacturing	Postal & Shipping
Dams	Telecommunications
Defense Industrial Base	Public Health & Healthcare
Drinking Water & Water Treatment Facilities	Transportation Systems

Figure 3. DHS Defined Critical Infrastructure Sectors

The National Infrastructure Protection Plan (NIPP) sets forth a comprehensive risk analysis and management framework and clearly defines critical infrastructure protection roles and responsibilities for DHS and other federal, state, local, tribal, and private sector CI partners. The NIPP provides the coordinated approach used to establish national priorities, goals, and requirements for infrastructure protection to ensure that funding and resources are applied effectively. The goal of the NIPP is to

build a safer, more secure, and more resilient America by enhancing protection of the nation's CI to prevent, deter, neutralize, or mitigate the effects of deliberate efforts by terrorists to destroy, incapacitate, or exploit them; and to strengthen national preparedness, timely response, and rapid recovery in the event of an attack, natural disaster, or other emergency.[14]

Just as in the intelligence support to law enforcement case, intelligence support to CI protection goes well beyond SAR-based information. National, homeland security, and law enforcement intelligence organizations all produce and disseminate reports on terrorist techniques, historical terrorist targets and tactics, and many other studies to help those responsible for protecting CI. In fact, such studies are used to develop and validate sets of indicators of pre-operational activity. But SAR-based intelligence also has an important role to play.

The central player in bringing intelligence to bear on CI protection at the national level is the DHS Homeland Infrastructure Threat and Risk Analysis Center (HITRAC) which conducts integrated threat and risk analyses for CI sectors. HITRAC is a joint fusion center that spans both the Office of Intelligence and Analysis (I&A) – a member of the Intelligence Community – and Infrastructure Protection. As called for in section 201 of the Homeland Security Act, HITRAC brings together intelligence and infrastructure specialists to ensure a sufficient understanding of the risks to the nation's CI from foreign and domestic threats.[15]

HITRAC, partnering with the National Infrastructure Simulation and Analysis Center (NISAC), has the mandate to lead in the development, testing, and evaluation of SAR-based models of "normal patterns" of SAR at CI. As noted above, HITRAC is unique in bringing together intelligence and critical infrastructure analysts at the national level. It also has been aggressive in working with state-level CI protection organizations and fusion centers to develop intelligence support to CI protection. On the other hand, NISAC has the sophisticated expertise needed to conduct statistical modeling. In fact, NISAC is a congressionally-mandated modeling, simulation, and analysis program.[16] The Center already prepares and shares analyses of CI including their interdependencies, consequences, and other complexities, so moving on to model the relationship between SAR and CI is a natural extension.

We can now move on to Figure 4, which displays the role of intelligence based on SAR in improving CI protection. Intelligence analysts are responsible for developing, updating, and improving the "complete historical SAR database." Similarly, critical infrastructure analysts are responsible for bringing their sector-specific expertise to bear in developing and maintaining a GIS-rectified CI database. These two teams of analysts, working in tandem, operate the models that yield a picture of the "normal pattern of SARs [*sic*] to specific CI facilities". This understanding of what constitutes a normal versus an abnormal situation at sector specific potential targets can then be used by the CI analysts to develop a more effective *protection* regime at that facility. Finally, in the process of advising CI stakeholders and partners, the CI analysts will encourage them to gather more and better reports of suspicious activity – a positive feedback loop strengthening the SAR process.

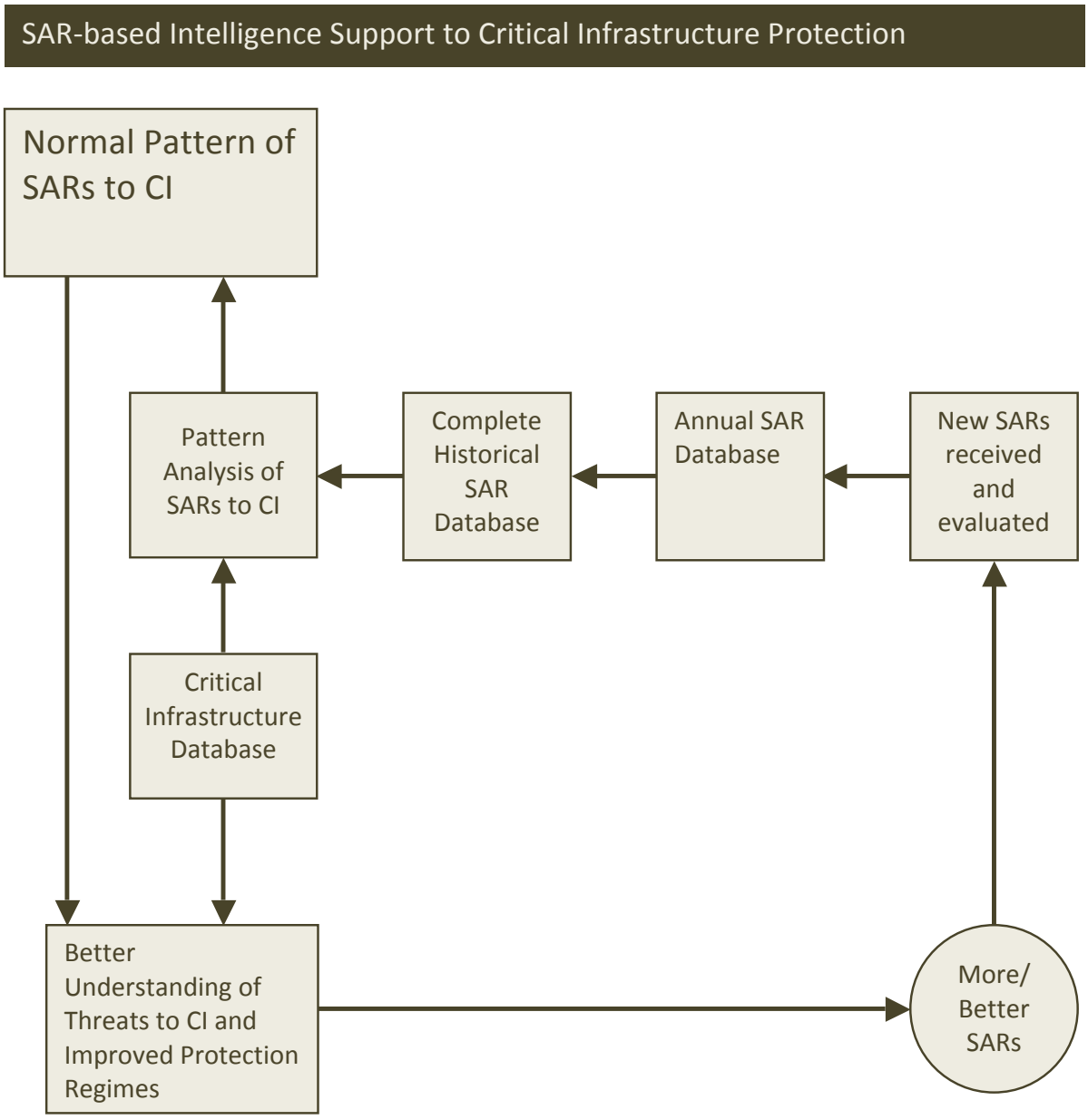


Figure 4. SAR-based Intelligence Support to Critical Infrastructure Protection

RECOMMENDATION

This paper has presented two SAR-based, data-intensive analytic techniques that have the *theoretic* potential to improve our counter-terrorism efforts by warning of terrorism activity and by assisting in the development of better CI protection regimes. Civil liberty activists point out the potential dangers to our privacy posed by a massive, national SAR program. They also question the effectiveness and efficiency of such a SAR effort.

Before national policymakers decide which way to go on this issue, it seems reasonable to conduct a validation test to determine whether or not the theoretic value-added of a robust SAR program can be proven in the real world. Such a validation program would begin with selection of a representative sample of the most important target sets (i.e. mass transit systems, bridges, dams, etc) and a concerted effort to collect a comprehensive data set of "suspicious activity" for this sample. Analysts from both the critical infrastructure and intelligence disciplines, supported by quantitative methodologists, would then be tasked to develop models of "normal" suspicious activity for each sample facility. If the models simply are not sensitive enough to detect simulated precursor terrorist activity or to provide insights into ways to improve protection of these facilities, then it is reasonable to constrain the SAR program. But if the models can do the job and actually are shown to constitute a unique, intelligence-driven capability to prevent terrorist attacks or at least to better protect our critical infrastructure, then further debate is in order before we simply discard that capability.

Dr. James E. Steiner is public service professor at Rockefeller College (SUNY Albany) where he teaches graduate courses in the craft of intelligence, with emphasis on intelligence analysis for homeland security. Dr. Steiner has more than forty years of experience conducting, leading, managing, teaching, and evaluating intelligence. After retiring in 2005 from a thirty-four year career at CIA, he taught intelligence analysis at the FBI Academy at Quantico. From 2006-2009 Dr. Steiner was an advisor both to the chief intelligence officer at the Department of Homeland Security and also to the director of New York State's Office of Homeland Security. He may be contacted at drjsteiner@gmail.com.

---

[1] U.S. Congress, House Committee on Homeland Security, Subcommittee on Intelligence, Information Sharing, and Terrorism Risk Assessment, *Homeland Security Intelligence: Its Relevance and Limitations*, Statement of Gregory T. Nojeim, Director on Freedom, Security, and Technology, Center for Democracy and Technology, 111th Cong., 1st sess., March 18, 2009, 1-2.

[2] Ibid., 14.

[3] Mark A. Randol, "Terrorism Information Sharing and the Nationwide Suspicious Activity Report Initiative: Background and Issues for Congress" CRS 7-5700 (Washington, DC: Congressional Research Service, November 5, 2009), 15-16, www.fas.org/sgp/crs/intel/R40901.pdf.

[4] Program Manager, Information Sharing Environment, "Findings and Recommendations of the SAR Support and Implementation Project" (Washington, DC: Bureau of Justice Assistance, US Department of Justice; the Major Cities Chiefs Association; DOJ's Global Justice Information, October 2008), 6.

[5] Ibid., 31.

[6] Program Manager, Information Sharing Environment, "Nationwide SAR Initiative Concept of Operations" (National SAR Initiative, December 2008), 8.

[7] "Final Report: Information Sharing Environment (ISE)—Suspicious Activity Reporting (SAR) Evaluation Environment" (Washington, DC: Bureau of Justice Assistance, U.S. Department of Justice, January 2010).

[8] Nojeim, testimony, *Homeland Security Intelligence*, 4-6.

[9] American Civil Liberties Union, "More About Suspicious Activity Reporting" (June 2010), http://www.aclu.org/spy-files/more-about-suspicious-activity-reporting

[10] Ibid.

[11] This is described at http://www.fbi.gov/page2/sept08/eguardian_091908.html.

[12] Joseph Straw, "Terror Threat Tracking System Shares Thousands of Tips from Locals, FBI Says" (March 2010), http://www.securitymanagement.com/print/6888.

[13] U.S. Department of Homeland Security, "Critical Infrastructure Protection" (August 2010), http://www.dhs.gov/files/programs/critical.shtm.

[14] U.S. Department of Homeland Security, *National Infrastructure Protection Plan: 2009*, http://www.dhs.gov/xlibrary/assets/NIPP_Plan.pdf

[15]U.S. Department of Homeland Security, "About the Homeland Infrastructure Threat and Risk Analysis Center (HITRAC)," http://www.dhs.gov/xabout/structure/gc_1257526699957.shtm

[16] The National Infrastructure Simulation and Analysis Center (NISAC), http://www.sandia.gov/nisac/

Building Resilient Communities: A Preliminary Framework for Assessment

Patricia H. Longstaff, Nicholas J. Armstrong, Keli Perrin, Whitney May Parker, Matthew A. Hidek

THE PROBLEM

Governments, non-governmental organizations, and community leaders in many countries face a daunting task: the design and implementation of policies, programs, and systems that help local communities cope with a panoply of threats ranging from terrorist attacks to natural disasters. In highly developed societies, this task is often compounded by associated problems such as aged, overburdened, and complex critical infrastructure systems;[1] the catastrophic potential of chemical, biological, radiological, nuclear, and explosive (CBRNE) threats; and the increasing interconnectivity of many global systems of transportation and communication.

The idea of building resilience to natural and man-made disasters is now a dominant strategic theme and operational goal in the current U.S. national security policy discourse.[2] Yet, even with unlimited resources, it is highly unlikely that a community can prevent or protect itself from all the possible dangers it may face. In the United States for example, complex distribution systems are now the primary mechanism for supplying populations with food and water. Gasoline-powered vehicles remain the dominant mode of transportation. Individuals and organizations build their everyday activities around complex systems over which they have little control, such as electricity, computerized systems, and communication networks supported by distant satellites. Each of these modern conveniences allows communities to function more efficiently. Yet few people maintain a stockpile of food and water or possess alternative modes of transportation, power generation, or communication in the event of an emergency.

Meanwhile, governments, communities, and individuals have never been so devastatingly unprepared to cope with disturbances to infrastructure, vital resources, or public goods and services. Part of the problem is that the efficiencies inherent within these complex systems of modern life reduce resilience through a loss in redundancy and diversity. Another aspect is that few systems are designed with resilience as a specification. The ability of these systems to bounce back after a disaster will have a direct impact on the ability of a community to respond and recover. It is thus important to consider all the resources that a community must count on when assessing resilience.

Researchers in varied and distinct disciplines have struggled with the concept of *resilience* in their respective fields for decades.[3] Scholars and practitioners continue to wrestle with this concept in hope of developing useful prescriptive homeland security policy guidance,[4] and community-level assessment tools.[5] While there is still much to debate about how to draft precise definitions of resilience and its attributes, and how to operationalize and apply resilience concepts within each discipline, overlap in the

research of each discipline is significant enough to be instructive as to what makes systems resilient.

The recent focus on resilience marks a shift from *resistance* strategies focused solely on the anticipation of risk and the mitigation of vulnerability to more inclusive strategies that integrate both *resistance* (prevent, protect) and *resilience* (respond, recover) in the face of disasters. In the past, some scholars have maintained that anticipation strategies should be used to focus on known problems, while those geared towards resilience are better suited for the unknown. It is important to point out that individually, both aspects have shortfalls. Just as planning based on anticipated threats can lead to resource investments to counter hazards that never materialize, planning from the broader resilience standpoint may call for the short-term diversion of resources in an effort to ensure long-term sustainability.[6]

Compounding the challenge is the difficulty in developing a flexible planning process that responds to changing conditions.[7] The greater the uncertainty, the greater the need for flexibility.[8] Yet, the pervasiveness of "worst-case," "probabilistic" planning lacks the "possibilistic thinking" needed to face both the dangers *and* the opportunities that no one can predict.[9] Finding the right balance between anticipation and adaptation, order and chaos, resistance and resilience is the challenge each community must face and calls for an approach based on continuous learning and transformation,[10] rather than anticipation and control.[11]

This article moves beyond *debating definitions of resilience*, towards the development of a preliminary conceptual framework for *assessing community resilience*. We recognize that not all frameworks are created equal, nor do they satisfy all constituent audiences.[12] The proposed framework presented herein is consistent with Nobel Laureate Elinor Ostrom's stated purpose of a framework: to "identify the elements (and the relationships among these elements)...to consider for analysis...organize diagnostic and prescriptive inquiry...[and] provide the most general set of variables that should be used to analyze all types of settings relevant for the framework."[13] It does not outline a cookie-cutter solution for all communities to apply, but rather an approach that allows community leaders and policymakers to begin to think about resilience as it pertains to their own community's unique circumstances. While sacrificing operational specifics in the interim, it summarizes the core attributes of resilient systems (resource performance, resource diversity, resource redundancy, institutional memory, innovative learning, and connectedness) in the context of five key community subsystems (ecological, economic, physical infrastructure, civil society, and governance). Through the examination of each community subsystem, a preliminary, community-based, resilience assessment framework is proposed for continued development and refinement.

In leading up to this conceptual framework, however, the article presents the definition of resilience used here, an argument for a community-based approach, and a description of what we believe the research shows are the core attributes of resilience within community systems.

WHAT IS RESILIENCE?

In current policy debates, the meaning of resilience varies by disciplinary perspective. For most, resilience (with its roots in the Latin word *resilio*) means to adapt and "bounce back" from a disruptive event.[14] Similarly, resilience also refers to the ability of a system to absorb, change, and still carry on.[15] As applied to social systems, resilience refers to the capacity of a community system, or part of that system, to absorb and recover from disruptive events.[16] We have adopted the definition used by scholars at the multi-disciplinary Resilience Alliance because it is applicable across the relevant systems examined here: *the capacity of a system to absorb disturbance, undergo change, and retain the same essential functions, structure, identity, and feedbacks*.[17] It can be a characteristic of individuals, small groups, networks, organizations, regions, nations, or ecosystems. This definition retains the core concepts of those definitions semi-officially adopted by federal agencies responsible for homeland security.[18]

Note that resilience does not necessarily mean that the system will look just as it did before a disturbance or "surprise." It will maintain its functions but individual parts of the system may have changed (adapted) to new conditions in the environment. For example, sometimes, when part of a system is not resilient and fails, other parts of the system must assume its functions and appropriate its resources. Thus, a resilience strategy does not guarantee short-term stability, but rather survivability of the system's essential functions in the long term. Resilience is often an emergent property of the system,[19] and therefore often difficult to measure and predict.

Resilience is sometimes confused with the concept of "resistance" – an attempt to prevent or stop disruptive events from happening. Resistance strategies include physical countermeasures such as trying to stop terrorists from boarding aircraft and building firewalls to protect computer systems from intruders. Resilience strategies, on the other hand, assume that resistance may not always be possible and thus include the provision of or access to alternative resources and services if the resistance strategy fails.

Resistance is not antithetical to resilience. Rather, resilience subsumes it. If a community can resist a disturbance, its resources are robust enough to prevent the disturbance from reducing community functioning without any need for adaptation. However, a strategy that only directs resources toward resisting threats would almost certainly be costly, and possibly conflict with societal norms and individual liberties. Moreover, when resistance strategies fail, they have a tendency to fail catastrophically.[20]

A COMMUNITY-BASED APPROACH

We do not assume that government is the primary guarantor of resilience, although it can be an important facilitator. Similarly, we do not assume that there is one optimal set of choices or resource allocations for all societies preparing and planning for potential "surprises" that may come their way. Nor do we assume that the choices that social groups make today will work in the future. Although resilience can be fostered on multiple scales, the community is an appropriate level for building basic resilience.

A central reason we focus on resilience at the community level is because most disasters are local and affect communities differently – a flood or earthquake would not affect residents of Singapore the same way that it would affect residents of San

Francisco, California. Communities are unique and have their own local needs, experiences, resources, and ideas about prevention of, protection against, response to, and recovery from different types of disasters. Each community has access to resources and the ability to manipulate and make decisions that single individuals do not. Since all disaster planning and response requires the immediate involvement of a wide range of local institutions (often in concert with state and national organizations), they are typically the appropriate level of focus for emergency planning and response activities. A community-level focus on resilience – as opposed to a "one-size-fits-all" or "top-down" approach – results in local participation, ownership, and flexibility in building resilience.[21] Moreover, because communities are parts of greater wholes (states, regions, and nations), a bottom-up community resilience approach builds state, regional, and national resilience concurrently.[22] Strengthening local coping capacity can help empower local communities rather than foster institutional dependency.[23]

A community is a group of people who share a common physical environment, resources, and services, as well as risks and threats. It is also a collective body that has boundaries (often geographic), internal and external feedbacks, and "a shared fate."[24] Because of this, a community is a complex physical and social system comprised of many sub-systems.[25] For example, a typical metropolitan area encompasses a diverse collection of districts and neighborhoods within the central city and its suburbs, with very different land-use norms, social interactions, income levels, and access to resources. Some experts refer to the "footprint" of a community as the region from which a city pulls its resources, that receives the city's waste, or that depends on the city's economy. This footprint usually reaches well beyond the city limits.[26] Disruption of community systems can come from external points and have broad effects within and without. For instance, the source that generates and provides power to an urban energy system is part of that system, but may be located well outside of the given urban area.[27]

In contrast, a rural community might be limited to a smaller collective of residents inhabiting a valley or mountainous region. Likewise, rural subsystems will vary in form and significance to overall community functioning. For instance, the family (as an institution) and religious organizations may play a more dominant role in rural settings than they do in urban settings.

Within both communities and regions, there is usually a high level of interaction among government, corporate, nonprofit, and individual participants when addressing common needs.[28] Indeed, many communities already engage in comprehensive community planning. Therefore, we presume that communities will define themselves in conducting any resilience self-assessment. Also, our analytical model seeks to close the practical gap between state-provided security, human safety challenges such as disasters and terrorism, and trans-boundary connections between public and private resources as well as multiple planning and response levels within communities.[29]

Attributes of Community Resilience

What makes one community bounce back from a disruption quickly while another will struggle for years? What is resilience in a community setting? Simply put, it is the ability of a community to absorb a disturbance while retaining its essential functions. This does not mean that its degree of functionality remains in a constant state but that functionality will return in one form or another in a relatively short period of time. To be

resilient, the community must have both the resources available and the ability to apply or reorganize them in such a way to ensure essential functionality *during* and/or *after* the disturbance. Furthermore, since the community governance process will differ based on each geographical setting, measures taken with the aim of improving a community's assessment of its own resilience must be highly context-specific.[30] After a comprehensive literature review of resilience in multiple disciplines,[31] such as organization theory, political science, economics and specific grounding in the tradition of ecological resilience and the work of the Resilience Alliance,[32] we propose a model that allows communities to evaluate and plan for their resilience based on an analysis of the robustness of their available resources and adaptive capacity to utilize their resources.

Before elaborating further on what resource robustness and adaptive capacity entail, we note the broader implications for communities. Communities with a highly robust pool of resources and a high degree of adaptive capacity will be the most resilient. However, few communities will have the luxury of possessing high levels of both. If a community is either high in resources or high in adaptive capacity, they can afford to have somewhat less of the other and remain relatively resilient if they take these assets into account in their planning. However, when communities possess low levels of resources *and* low levels of adaptive capacity, they will be less resilient. So, if a community is lacking in resources, it should concentrate on building its adaptive capacity. For example, if a community lacks funds (resources) for advanced communications equipment, it can utilize resources on hand and self-organize in such a way (adaptive capacity) to perform the desired function. Hypothetically, two communities could have an equal amount of resilience, but a different mix of resources and adaptive capacity.

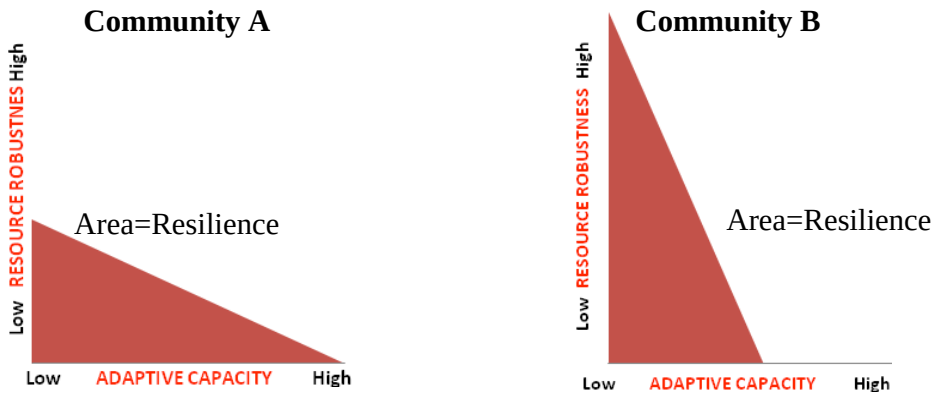


Figure 1. Resource Robustness and Adaptive Capacity

Resource Robustness

Resources are critical to a community's sustained functioning and provision of public services under a variety of conditions, in times of normalcy or crisis. Communities can evaluate the *robustness* of their resources by looking at the performance, diversity, and

redundancy of what is available to them. Resources are defined as "objects, conditions, characteristics, and energies that people value."[33] Importantly, this definition emphasizes the localized, value-laden quality of such an object or condition. Resources considered valuable to one community may not have the same inherent value to another, especially across different regions and cultures. Resources that are objects or conditions could range anywhere from snowplows to schools, from hospitals to food and water supplies, or from social cohesion to economic wealth. Likewise, characteristics and energies such as leadership, education level and ethical values could also be considered resources to a community.

Performance "describes the general level of capacity and quality at which an element or elements of a system performs an essential role."[34] Performance answers the question, "how well does this resource accomplish a particular function?" For example, a hammer performs better than a wrench for sinking a nail, because it is designed specifically to drive nails into solid objects. Performance of an object or condition also includes a quality relative to those of a similar nature. Thus, a stronger, more durable hammer performs better than those of inferior design, and thus has a higher relative quality. When looking at the function of water distribution within a community it would be important to know how well the water system works under average conditions and what might make it vulnerable to collapse.

Diversity is a measure of different types of available resources that perform a particular function.[35] A community that has high diversity in its available resources for critical functions will have a multitude of options for accomplishing those particular functions. Hammers, nail guns, and other hard objects all provide a diversity of options to sink nails. Yet, if the function is to attach one object to another, adhesives such as glue, screws and screwdrivers, staples and staplers, if available, provide a diversity of resources to draw upon, albeit with varying degrees of performance. Likewise, if there are several communication systems in a community (i.e., radio and reverse-911) there will be more chance to reach all citizens with important information and more likelihood of reaching people if one of those communication systems becomes inoperable.

Diversity can also come in the form of information and ideas for approaching a particular task. All else equal, a planning team comprised of individuals that come from a variety of backgrounds and experiences possesses a greater collective diversity of ideas and knowledge and, thus, a greater number of options to tackle a problem, compared to a team of individuals from similar backgrounds.

Redundancy is a quantifiable measure, or count, of a single resource type that performs a specific function.[36] Redundant resources provide a failsafe, or back-up, when any individual unit fails. Redundancy is also a form of operational slack, or buffering from external shocks. Having many hammers provides a high degree of redundancy for sinking nails. If one breaks, there are more to use. Likewise, emergency savings accounts are a form of redundancy in financial terms and allow for the continuance of an individual or family's lifestyle in the event of a job loss or unexpected event. A seventy-two-hour emergency preparedness kit allows a household to sustain itself in the event of a disaster, until a community response organization can respond and restore power and other basic services.

However, redundancy is often expensive. It means that there are resources sitting in reserve that may not be used – even while the community pays to maintain them. This becomes an important tradeoff that each community must make and depends in large part on how valuable a resource is to them and how likely it is that resource will be disrupted.

When combined, the performance, diversity, and redundancy of available resources determine a system's overall robustness.[37] That is, its ability to provide critical functions under a variety of conditions. For example, the robustness of a water system would be greatest when the system has high performance (i.e., sound delivery mechanisms, pipes, pumps, etc.), redundancy (i.e., multiple water lines), and diversity (i.e., multiple sources such as rivers, lakes, aquifers, and runoff). Every community, and each system within a community, must decide how to allocate time and money between performance, redundancy, and diversity, keeping in mind that it may be best to have a balance of the three attributes – not maximizing one to the detriment of the others.[38]

Adaptive Capacity

A community's *adaptive capacity* is a function of the ability of individuals and groups to: 1) store and *remember* experiences; 2) use that memory and experience to learn, *innovate*, and reorganize resources in order to adapt to changing environmental demands; and 3) *connect* with others inside and outside the community to communicate experiences and lessons learned, self-organize or reorganize in the absence of direction, or to obtain resources from outside sources.[39] Thus, institutional memory, innovative learning, and connectedness determine the foundation of adaptive capacity on a community level.

Institutional memory is the accumulated shared experience and local knowledge of a group of people. Over time, institutional memory is amassed through group-level observation and stored in a variety of ways such as documented records or repetitive rituals and ceremonies that are carried on as group membership evolves over time.[40] Rituals reinforce institutional memory by facilitating and reinforcing the recollection of rules and policies as well as the interpretation of changes or disturbances in the environment. Information and knowledge management systems that store, distribute, and aid in interpretation of large quantities of data are helpful in retaining institutional memory but only if they are accessible by people who need them, when they need them.

Innovative Learning is the ability of the group to use its information and experience to create novel adaptations to environmental changes or to avoid repeating old mistakes. Innovation is a form of dynamic learning that places emphasis on the capacity to identify and "create new responses or arrangements."[41] Innovative institutions sometimes encourage trial-and error type learning by allowing "errors and risk-taking behavior."[42] Other times innovations occur in a more deliberate way by putting new ideas or resources together with old ones when current strategies are not working. It is true that necessity is often the mother of invention. Innovative learning can be reduced by a failure to admit that something is not working to provide an important resource or function. This kind of learning can be especially difficult when it has to happen as an unanticipated disruption is unfolding. During a disruption, spreading information about the innovative learning going on in a community (both what is working and what is *not* working) requires a trusted source of information that may or may not be government

or the media. Identification of these trusted communication channels and maintaining that trust becomes critical.[43]

Innovation and learning are mutually increased through the practice of "adaptive co-management" which combines a management culture that places a premium on risk taking and experiential learning with the linkages and partnerships associated with cooperative management.[44] Leadership – a vital community resource – plays a pivotal role in establishing such a culture.

The creation of new ideas, resources, processes, and forms of organization are all results of innovative learning.[45] A community is in a position to learn and innovate when individuals and groups are able to experiment through trial and error. Repeated variations on experiments create knowledge – and hopefully institutional memory – of what new ideas, processes, and organizational designs work and those that do not. Ultimately, innovative learning allows the ability of a social group to anticipate both *future opportunities and future hazards*.

Finally, interpersonal and group *connectedness* is critical to the diffusion of institutional memory and innovative learning throughout the community. Community systems and subsystems typically have a variety of internal and external links between their various component parts of the system and the higher or lower levels of the system. These links are commonly characterized as social (informal) and organizational (formal) networks.[46] In the absence of formal direction, these connections – which often vary in strength[47] – contribute to a community system's ability to exchange, store, and recall knowledge, and take collective action in light of changing conditions.

However, the tightness or looseness of these connections can be both the community's strength and its vulnerability.[48] In *tightly coupled systems,* a change in one component (individual or subsystem) of the system engenders an immediate response from (or impact on) the other components. For example, an apartment complex is a tightly coupled shelter system because a fire in one living unit is likely to have an effect on the others. In a rural area, a fire at one farm will not have an immediate effect on the others as they are more loosely coupled. The efficiency of apartment complexes comes at the cost of less resilience to fires for individual units.

Yet, in *loosely coupled systems,* the components have weak enough links that they can ignore local disturbances. Since loosely connected units have more independence from the full system than tightly coupled ones, they can maintain their equilibrium or stability even when other parts of the system are affected by a change in the environment. Thus, if either innovation or localized responses to particular problems are specified goals, then loosely coupled systems seem most appropriate. For example, a more tightly coupled emergency management system would take longer to respond or have inappropriate responses for some unanticipated surprises if all the units in the system had to wait on centralized, bureaucratic decision making before they could act. Still, if the goal is standardization across the entire system, then a tight coupling is more likely to yield a desired outcome.

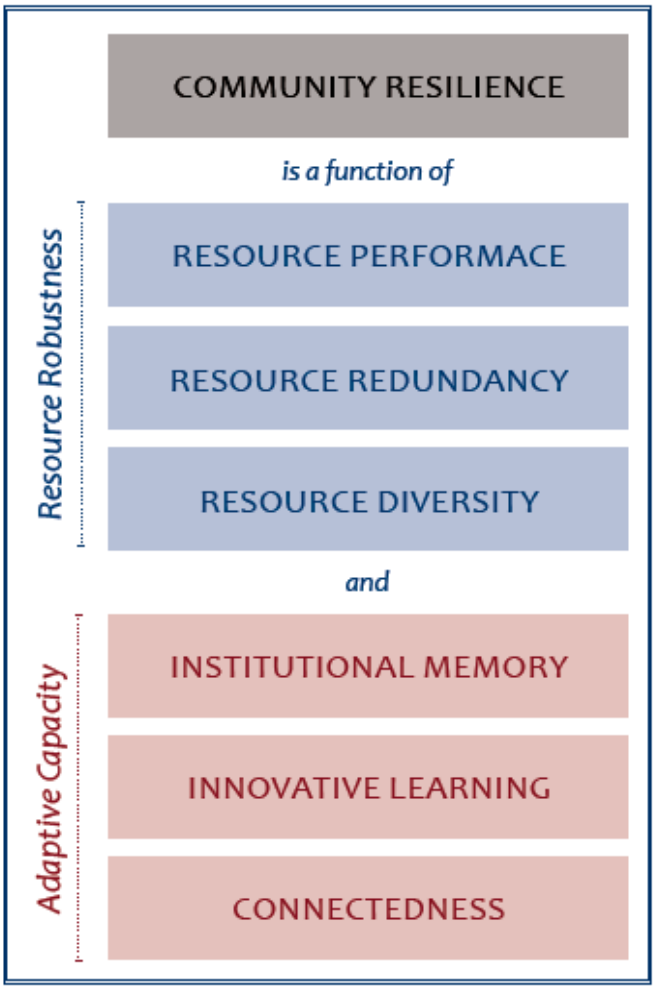


Figure 2. Aspects of Community Resilience

When a community possesses a high level of all three traits – institutional memory, innovative learning, and connectedness – it, in turn, possesses a high capacity to adapt to changes in the environment. If it has a relatively low level of one trait, it can often make up for this deficiency by addressing it directly or increasing the levels of the other two traits. For example, a large city with low levels of connectedness between ethnic groups could address this problem directly by creating bridges for dialogue and communication that will, in the event of a disruption, facilitate sharing and diffusion of institutional memory and innovative learning across groups. This requires that communities build connections and trust *before* a disruptive event. However, if such a strategy proves unfruitful, it may still be able to improve adaptability by increasing the access of these groups to a shared knowledge center, or by encouraging innovation and learning across all groups.

Living, or coping, with change and uncertainty requires the capability to integrate and apply learning, collective memory, innovation, and collaboration in ways that

sustain critical functions over time. A tall order – communities, governments, and organizations must continuously look forward, plan for multiple alternative futures, and test for or experiment with new ideas, while recalling and interpreting the past. In recognizing the directional nature of current hazards and changes, and by identifying external drivers of change, these social institutions have the opportunity to design the flexibility necessary to anticipate and adjust to change.

APPLYING A RESILIENCE APPROACH TO COMMUNITY SYSTEMS

With the ability to make sound self-assessments of their resilience to disasters and disruptions, communities can more appropriately prioritize preparedness efforts, allocate funding, and develop more innovative ways to organize their material and human resources. In order to help communities think about their resilience, our approach employs the concepts described above to assess each one of five key community subsystems: ecological, economic, civil society, governance, and physical infrastructure.[49]

These five were chosen based on an exhaustive review of academic and policy-oriented literature, and lengthy discussions on a set of sub-systems that, together, captured the core functions within a community. For example, earlier in our research, we included information and communication systems as a stand-alone system for analysis, but concluded it overlapped considerably with all other subsystems. We recognize that these subsystems are inherently interdependent, overlapping, and complex, even in small communities. Ultimately, the set of five key community subsystems represents a pragmatic choice between parsimony and exhaustiveness.[50] These five subsystems are a starting point for community analysis and individual communities may well identify other subsystems that are important to them.

Within each subsystem described below, we illustrate some of the attributes and characteristics of what we believe indicate resilience in each subsystem; that is, the robustness of the resources that make up the subsystem and its adaptive capacity. Attributes of resilience will vary depending on the type of system in question. For example, diversity in an ecosystem may be the number of different types of species, while diversity in an economic system may include the range of skill sets within a labor force. The discussion of each subsection is for explanatory purposes only. We do not attempt to "prove" the applications suggested or to offer a "how to" for each system. However, we hope that more specific guidance for communities will be developed as this research progresses.

Ecological Subsystems

Ecological systems are the combined biological and physical elements of the environment in which a community is located.

> [An] ecosystem is the complex of interconnected living organisms inhabiting a particular area or unit of space, together with their environment and all their interrelationships and relationships with the environment. An [e]cosystem is characterized by the description of populations; [the abundance] of individual species; interspecies relationships; activity of organisms; physical and chemical

> characteristics of environment; flows of matter, energy, and information; and description of changes of these parameters with time.[51]

Humans are an important part of a community's ecosystem but they are not the only important part. Without outside resources, humans cannot survive if the local environment does not support agriculture or provide enough clean water.

Some parts of an ecological subsystem will be beyond the control of a community, but are nonetheless helpful in describing a community's setting and the natural resources the community can use to provide for critical functions in times of disruption. The important natural resources might include items such as water supplies, wind patterns, climate, soil quality, and topography. The important task for each community is to look at the aspects of the ecological systems most valued in order to consider them when the community is forced to bounce back from a surprise. For example, it would be important to know wind patterns if you must respond to a cloud of volcanic ash or a biological attack. It may also be important to know the amount of available land for new uses such as temporary shelter construction. In addition, a diversity of habitats would allow some flora and fauna to survive if one habitat is rendered uninhabitable. Will these habitats support local food production? Does the environment support growing other crops if the current ones become economically unsustainable?

The adaptive capacity of ecological subsystems might be measured by how quickly key elements of the local environment can regenerate in the event of a disaster such as flooding or fire.[52] Grasses and insects will regenerate much faster than trees and mammals due to the length of their life cycles. Through evolution, many plants have developed adaptive capacity that allows them to be resilient because they "remember" how to bounce back from dangers such as fire by developing protective surfaces on their seeds. For agriculture, this adaptation period will be the time it takes to prepare the land and then plant either the existing crop or a new one that is more appropriate to new ecological (or economic) conditions. New crops may need new machinery and specialized knowledge to accomplish successful adaptation. Indicators of adaptive capacity include the ability of the environment to support a diversity of crops and wildlife.

Economic Subsytems

Economic systems are comprised of people, firms and institutions that interact to accomplish the production, distribution, and consumption of goods and services. A resilient economy can be essential for recovery efforts in a post-disaster setting.[53] The resources of an economic system are robust if they can deliver critical goods and services under a variety of conditions. The changes in conditions may happen quickly, like a flood. Or they may occur over a longer period of time, like climate change or the movement of firms to new markets.

A major disaster or catastrophic event could potentially put many economic activities at risk. Resilient local economic systems will have plans to get small businesses up and running to ensure that people feel safe going to markets, and to assure the public that the flow of currency is secure and individual bank accounts are protected. The first decision will be whether to try to return the economic system to its previous state or to adapt to new conditions.

Resource robustness in an economic subsystem would generally include performance, diversity, and redundancy within the labor markets and capital markets and 'land' or natural resources within a given community. According to some economists, the measure of these resources denotes the potential for "shock-absorption."[54] To assess the resources within an economic subsystem, economists might look at the conditions of the labor market, the make-up of the community's businesses, the preferences of consumers, measures of unemployment, and growth and/or inflation, among other signals.

Adaptive capacity in an economic subsystem might come in the form of policy options available to business or government leaders, such as whether to borrow, trade, finance, or substitute goods. Such tools increase the potential for "shock-counteraction,"[55] and amount to the ability of the economic subsystem to innovate and learn. To assess the adaptive capacity in an economic subsystem, experts could consider the fiscal position of the community – a healthy position would allow leaders to cut taxes or raise expenses to counteract the harmful shock. Economists might also look at the community's freedom to trade or make adjustments to trading relationships. In the labor market, economists might look at the ability of workers to change jobs or get new training in various industries.

Physical Infrastructure Subsystems

Physical infrastructure "refers to the substructure or underlying foundation or network used for providing goods and services; especially the basic installations and facilities on which the continuance and growth of a community, state, etc., depend...[and] include roads, water systems, communications facilities, sewers, sidewalks, cable, wiring, schools, power plants, and transportation and communication systems."[56] The practitioners, engineers, and policy makers that use, design, and manage these assets are included within the subsystem as well.

Assessing the resource robustness within a community's physical infrastructure subsystem would require an accounting for each of the infrastructure sectors listed above, especially considering that the robustness of each sector could vary dramatically within the same community. A community could have a superior transportation system, but a woefully inadequate water system. In addition, communities have varying control over the complex, networked infrastructure systems on which they rely. For example, many communities rely on power from the electric grid. Thus, they are unable to affect the performance or redundancy of their own energy infrastructure because it is managed and regulated on a broader scale. Realizing this, communities might work to require these higher levels of regulation to include appropriate redundancy to ensure that the system can bounce back after a disruption. Potentially costly, redundant telephone switches or electric generation and transmission capacity would almost certainly be paid for through increased rates for businesses and consumers. This illustrates tradeoffs that must be made between increasing resilience and reducing costs in the short term.

An adaptive capacity assessment in a given infrastructure sector depends, in part, on the nature of the component under consideration. Some components are structured or designed to adapt. The internet, for example, automatically reroutes information around damaged networks. Other components that consist of fixed resources, like a

transportation system that consists of bridges and roads, can only adapt in the short term through innovation by the system's users and managers that reroutes traffic around damaged areas.

Civil Society Subsystems

For our purposes, "civil society" refers to the formal and informal modes of social organization and collective action outside of governmental authority (i.e., non-governmental and philanthropic organizations, health and human service organizations, faith-based organizations, unions, associations, etc.). These institutions contribute to community values, provide forums for civic action and dialogue, and enhance quality of life and social welfare. They are often key players in recovery from a sudden disruption such as a natural disaster.

Assessing the resource robustness within a community's civil society subsystem would entail accounting for the diversity (number of different types) of civil society organizations, their redundancy (total number by category), and the performance of these diverse organizations in accomplishing their missions. A large number of volunteer organizations in a community may appear to offer high redundancy, but if these organizations experience difficulties maintaining membership, mobilizing support, or accomplishing meaningful projects for the community, they may not necessarily be considered *robust* resources.

An adaptive capacity assessment in a given community would require a careful examination of the mechanisms and procedures the civil society uses to retain and recall its collective experiences, the production of new and innovative techniques for achieving community goals, and the strength of ties between civil society organizations. Using the volunteer sector again as an example, indicators such as organizational longevity, employee turnover, and growth of new organizations would provide a general sense of institutional memory. However, this should also take into account how organizations retain and embed their experiences in processes and individuals.

Governance Subsystems

Systems of governance include the public organizations (political, administrative, legislative, and judicial institutions) that contribute to the administration of government functions of the community. There may be overlap into the social and private spheres through public-private partnerships. Governance also includes the processes through which government institutions, or any group of people with a mandate or with a common purpose, make decisions.[57] Governance also sets the parameters for ordered rule, cooperative action,[58] decision-making, and power sharing through institutions.[59]

Assessing the resource robustness of a community's governance subsystem is often limited to a performance assessment in terms of the governing entities themselves because competing governing entities sometimes undermine the functions of the system. This is apparent in post-conflict communities that suffer from diverse governing structures (tribal, national, and intervening structures) all operating at once. Performance may be measured in multiple ways – from the cost and quality of services delivered in relation to the resources collected from the citizens, to the strength of the government's mandate to act on the citizens' behalf.[60] In some communities there may

be great value in having redundancy and diversity in staffing, especially for critical functions and resources, even if this is not efficient and costs more in the short term.

An adaptive capacity assessment in a given community would entail a range of inquiries. Does the government have the capacity to institutionalize and adapt lessons-learned, such as modifying emergency response plans following an event? How extensive is the discretionary authority granted to government officials during a crisis (for example, the authority to commandeer resources or waive regulatory restrictions as needed)? How connected are the various units of government in times of disruption?

DEVELOPING AN ASSESSMENT FRAMEWORK

The critical elements of a local resilience assessment include an unflinching look at the five subsystems as they really are and a willingness to see possibilities for putting resources together in new ways in the event of a disruption. At a minimum, a comprehensive community resilience assessment would entail an examination across each of the five subsystems that make up the community, as briefly described above. Communities should assess each subsystem's resource robustness in terms of performance, diversity, and redundancy as well as its adaptive capacity in terms of institutional memory, capacity for innovation, and internal and external connectedness. Each system must be initially assessed separately because the attributes of resilience are manifested differently. Overlaps between these subsystems should then be dealt with to form a picture of the whole.

The following list of questions represents the most basic level of examination to assess the resilience of a community subsystem.

Basic Questions for Resilience Assessment

- Which functions are vital to our community within this subsystem?
- What resources are available to perform this function?
    - How well does this resource perform a particular function? How well would it perform in a disruption? *(Performance)*
    - How much of this resource do we have? *(Redundancy)*
    - Are there other resources available that could perform this function? *(Diversity)*
- To what extent do organizations and informal social groups within this subsystem instill and maintain a common memory? *(Institutional Memory)*
- To what extent do organizations and informal social groups within this subsystem foster a culture of continuous learning and innovation? *(Innovative Learning)*
- To what extent are organizations and informal social groups within this subsystem internally and externally connected? Are they loosely connected or tightly connected? How will a disturbance that affects one organization or social group impact others? *(Connectedness)*

While this list of questions appears rudimentary, it can easily lead to a lengthy set of functions and resources under each subsystem, accompanied by evaluative criteria and/or indicators for each resilience attribute (performance, redundancy, diversity, institutional memory, innovative learning, and connectedness). The boxes below provide a simple breakdown of how an analysis would be organized by subsystem with one or two example indicators. The potential depth and comprehensiveness of such an assessment is limitless and ultimately up to the prerogative of the community or analyst.

ECOLOGICAL

- RESOURCE ROBUSTNESS
  - Performance (quality of top soil)
  - Diversity (variety of habitats, flora, and fauna)
  - Redundancy (amount of available land)
- ADAPTIVE CAPACITY
  - Institutional Memory (evolutionary, genetic adaptations)
  - Innovative Learning (finding an alternative food source)
  - Connectedness (food webs, linkages in food chain)

ECONOMIC

- RESOURCE ROBUSTNESS
  - Performance (median household income)
  - Diversity (variety of labor force skill sets)
  - Redundancy (number of large-scale businesses)
- ADAPTIVE CAPACITY
  - Institutional Memory (historical modeling, forecasting)
  - Innovative Learning (testing new products in market)
  - Connectedness (import and export volume)

Figure 3. Resilience Analysis Breakdown (with example indicators)

CONCLUSION

As stated previously, this article outlines a *preliminary* conceptual framework for assessing resilience. It is a first step toward moving beyond academic debates and toward a useful policy tool. While discussion and debate will – and should – continue on the exact nature of resilient systems in the various disciplines, we believe there is a significant enough overlap in the research to propose this framework for more concrete analysis. Just as no one definition of resilience will fully satisfy participants in this diverse field of research and practice, no one tool will be equally satisfying or sufficient. What matters is that communities have an approach that is relatively easy to understand and use to guide decision-making.

Notably, this framework is community-based, holistic, and scalable. The design allows planners and policy-makers to conduct a resilience assessment that is adapted to fit their own particular circumstances, based on the assumption that communities themselves are best able to identify and make value judgments regarding which functions and resources matter most. Communities are also better equipped than outside evaluators to determine the scale and scope of the geographic and political boundaries that define them. In addition, because the proposed framework is scalable, it can potentially allow for application on multiple levels of state, regional, and international governance.

We acknowledge that this framework requires further development both in academic circles and communities. Options include assembling experts from each subsystem to evaluate how to best measure the resilience attributes (resource robustness and adaptive capacity) quantitatively, qualitatively, or in combination. Researchers might develop a catalog of evaluative questions to be assessed, scaled, and normalized according to subsystem, and then aggregate these questions to form a collective resilience index. Another option involves extensive case study analysis.

Lastly, the resilience approach described here is no panacea for addressing the wide range of natural and man-made threats to society. Nor should it completely supplant risk- and vulnerability-based approaches to homeland security. Rather, all of these efforts should be mutually supporting. But until researchers and practitioners move beyond the definitional debate and get on with developing something useful in the field, resilience will remain nothing more than just another good concept and meaningless buzz-word.

This article is based on research presented in P.H. Longstaff, N. Armstrong, and K. Perrin, "Building Resilient Communities: Tools for Assessment," Project on Resilience and Security white paper, Institute for National Security and Counterterrorism, Syracuse University (March, 2010), available at: http://insct.syr.edu/uploadedFiles/insct/topics_and_projects/resilience/INSCT%20White%20Paper_Building%20Resilient%20Communities.pdf.

Patricia H. Longstaff is the David Levidow Professor of Communication Law and Policy at Syracuse University's Newhouse School of Public Communications, and specializes in the business and public policy issues affecting the communications industry. Her most recent book, The Communications Toolkit: How to Build or Regulate Any Communications Business,

was published by MIT Press in 2002. She is a graduate of Harvard University (MPA) and Iowa University (JD, MA Communications). Ms. Longstaff may be contacted at phlongst@syr.edu.

Nicholas J. Armstrong is a research fellow at the Institute for National Security and Counterterrorism (INSCT) at Syracuse University. His research centers on post-conflict security sector reform and institutional resilience. Armstrong is a graduate of West Point and the Maxwell School of Syracuse University (MPA). He is currently pursuing a security-focused PhD in the Maxwell School's interdisciplinary Social Science doctoral program. Mr. Armstrong may be contacted at narmstro@maxwell.syr.edu.

Keli Perrin is the assistant director of INSCT. She also serves as an adjunct professor at the Maxwell School of Syracuse University. She is a graduate of SUNY Institute of Technology, Syracuse University College of Law (JD, magna cum laude) and the Maxwell School of Syracuse University (MPA). Ms. Perrin may be contacted at kaperrin@law.syr.edu.

Whitney May Parker is a research fellow at INSCT. She holds a MA in international relations from the Maxwell School of Syracuse University, specializing in intercultural communication and negotiation, and a bachelor's in political science with a specialization in international relations and certification as a professional mediator from Boise State University. Ms. Parker may be contacted at whitneyparker@gmail.com.

Matthew A. Hidek is assistant professor in the Division of Social and Behavioral Sciences at Cazenovia College. He holds a PhD in social science from Syracuse University's Maxwell School of Citizenship and Public Affairs and a master's in community and regional planning from Temple University. Dr. Hidek may be contacted at mahidek@cazenovia.edu.

ABOUT THE INSTITUTE FOR NATIONAL SECURITY AND COUNTERTERRORISM (INSCT) The Institute for National Security and Counterterrorism (INSCT) at Syracuse University is a research and academic center jointly sponsored by the College of Law and Maxwell School of Citizenship and Public Affairs. Directed by William C. Banks, INSCT leads a systematic, interdisciplinary approach to teaching, research, and public service focused on important national and global problems of security and terrorism. For more information, please see the INSCT homepage at www.insct.syr.edu.

---

[1] S. Flynn, *The Edge of Disaster: Rebuilding a Resilient Nation* (New York: Random House, 2007).

[2] See for example, The White House, *The National Security Strategy of the United States of America*. (Washington, DC: May 2010); U.S. Department of Homeland Security (DHS), *One Mission, Securing Our Homeland; U.S. Department of Homeland Security Strategic Plan 2008-2013* (Washington, DC: 2008); DHS, *National Infrastructure Protection Plan* (Washington, DC: 2009); DHS, *National Disaster Recovery Framework (Draft)* (Washington, DC: February 2010); and J. Cascio, "The Next Big Thing: Resilience," *Foreign Policy* 88, No. 3 (May/June, 2009).

[3] B. Walker, C. S. Holling, S. R. Carpenter, and A. Kinzig, "Resilience, adaptability and transformability in social–ecological systems," *Ecology and Society* 9 (2004): 5.

[4] J. H. Kahan, A. C. Allen, and J. K. George, "An Operational Framework for Resilience," *Journal of Homeland Security and Emergency Management* 6, No. 1 (2009): 1-47.

[5] K. Perrin participated in a Subject Matter Working Group meeting in June 2010 as part of the Community and Regional Resilience Institute's (CARRI) Community Resilience System Initiative. See http://www.resilientus.org/community_resilience_system_initiative.html. An earlier version of this paper was circulated at this meeting for feedback.

[6] A. Widalvsky, *Searching for Safety* (New Brunswick: Transaction Books, 1988); (cited in J. M. Normandin, M. C. Therrien, and G. A. Tanguay, "City Strength in Time of Turbulence: Strategic Resilience Indicators," (paper presented at the Joint Conference on City Futures, Madrid, 4-6 June, 2009). Available at http://www.cityfutures2009.com/PDF/43_Therrien_Marie_Christine.pdf).

[7] J. Rosenhead, "Planning Under Uncertainty I: The Inflexibility of Methodologies," *The Journal of the Operational Research Society* 31, No. 3 (1980): 209-216.

[8] A. Etzioni, *The Active Society: a Theory of Societal and Political Processes* (London: Collier-Macmillan, 1968); K. Boulding, "Reactions on Planning, the Value of Uncertainty," *Technology Review* 77, (Oct/Nov 1974); T. Marschak and R. Nelson, "Flexibility, Uncertainty and Economic Theory, *Metroeconomica* 14, (1962): 42-58; (cited in J.Rosenhead, "Planning Under Uncertainty I: The Inflexibility of Methodologies," *The Journal of the Operational Research Society* 31, No. 3 (1980): 209-216).

[9] L. Clarke, *Worst Cases: Terror and Catastrophe in the Popular Imagination* (Chicago: University of Chicago Press, 2006).

[10] L. Comfort, "Risk and Resilience: Inter-organizational Learning Following the Northridge Earthquake of 17 January 1994," *Journal of Contingencies and Crisis Management* 2, No. 3 (1994): 157-170.

[11] J. Gleick, *Chaos, Making a New Science* (London: Penguin Books, 1987).

[12] For example, "An Operational Framework for Resilience" (cited in note 18) is primarily a set of resilience planning and resource allocation guidelines for homeland security and emergency management policymakers. The framework provides an operationally relevant rubric for envisioning resilience across the four main homeland security mission areas (prevent, protect, respond, and recover). Yet, it neither explains what exactly makes complex systems resilient nor offers a method to evaluate resilience. How can resource allocation across the various mission areas be justified without a basic understanding of the underlying dynamics of resilience?

[13] E. Ostrom, *Understanding Institutional Diversity* (Princeton, NJ: Princeton University Press, 2005), 28.

[14] R. Klein, R. Nicholls, and F. Thomalla, "Resilience to Natural Hazards: How Useful is this Concept?" *Environmental Hazards* 4 (2003): 35–45; S. Manyena, "The Concept of Resilience Revisited," *Disasters* 30, No. 4 (2006): 434-450.

[15] C. S. Holling, "Resilience and Stability of Ecological Systems," *Annual Review of Ecological Systems* 4 (1973): 1-23.

[16] P. Timmerman, *Vulnerability, Resilience and the Collapse of Society: A Review of Models and Possible Climatic Applications* (Toronto: Institute for Environmental Studies, University of Toronto, 1981).

[17] The concept of "resilience thinking" was first developed in C.S. Holling, "Resilience and Stability of Ecological Systems," *Annual Review of Ecological Systems* 4 (1973): 1-23. See also the web site for the Resilience Alliance: http://www.resalliance.org, and L. Gunderson, C. Allen, and C.S. Holling (eds.), *Foundations of Ecological Resilience* (Washington D.C.: Island Press, 2010). These ideas were applied to homeland security issues by P. H. Longstaff in *Security, Resilience, and Communication in Unpredictable Environments Such As Terrorism, Natural Disasters, and Complex Technology*, Program for Information Resources Policy, Harvard University (November 2005), http://pirp.harvard.edu/pubs_pdf/longsta/longsta-p05-3.pdf.

[18] J. Kahan, A. Allen, and J. George, "An Operational Framework for Resilience," *Journal of Homeland Security and Emergency Management* 6 (2009): 1-48, http://www.bepress.com/jhsem/vol6/iss1/83. The Homeland Security Advisory Council Critical Infrastructure Taskforce (HSAC CITF) favors this definition: "Resiliency is defined as the capability of a system to maintain its functions and structure in the face of internal and external change and to degrade gracefully when it must." The Department of Homeland Security (DHS) uses this definition: "Resilience is the ability of systems, infrastructures, government, business, and citizenry to resist, absorb, and recover from or adapt to and adverse occurrence that may cause harm, destruction, or loss [that is] of national significance." Other definitions and an extensive review of the literature can be found at F. Norris et al., "Community Resilience as a Metaphor, Theory, Set of Capabilities, and Strategy for Disaster Readiness," *American Journal of Community Psychology* 41 (2008): 127-150.

[19] Phenomena are said to be emergent when they arise from the collective actions of many uncoordinated agents. See, e.g., Steven Johnson, *Emergence: The Connected Lives of Ants, Brains, Cities, and Software* (New York: Scribner, 2001).

[20] S.D. Sagan, *The Limits of Safety: Organizations, Accidents, and Nuclear Weapons* (Princeton, NJ: Princeton University Press, 1993).

[21] There is growing agreement among many organizational theorists that the best responses to challenges often come from the bottom up and not from the top down, or a combination thereof. See, e.g., John Seely Brown and Paul Duguid, *The Social Life of Information* (Cambridge, MA: Harvard University Press, 2000).

[22] For example see M. Bruneau, S. Chang, R. Eguchi, G. Lee, T. O'Rourke, and A. Reinhorn, "A Framework to Quantitatively Assess and Enhance the Seismic Resilience of Communities," *Earthquake Spectra* 19 (2003): 733-752; D. Godschalk, "Urban Hazard Mitigation: Creating Resilient Cities," *Natural Hazards Review* 4, No. 3 (2003): 136-143; and F. Norris et al., "Community Resilience as Metaphor."

[23] B. Wisner, P. Blaikie, T. Cannon, and I. Davis, *At Risk: Natural Hazards, People's Vulnerability and Disasters* (London: Routledge, 2004).

[24] F. Norris et al., "Community Resilience as Metaphor," 128.

[25] Communities must be thought of as *complex systems* as opposed to simple, linear systems (where 2+2 always equals 4). Researchers from many fields, including public administration, have discovered that complex systems often behave in similar ways; see, e.g., L. Dennard, K. Richardson, and G. Morcol, eds., *Complexity and Policy Analysis: Tools and Methods for Designing Robust Policies in a Complex World* (Goodyear, AZ: ISCE Publishing, 2008). Also, while there is no universally accepted and comprehensive definition of complex systems, there are some things that they seem to have in common: they are made up of many components; contain intricate webs of causal links and feedbacks that are tightly or loosely coupled; have interdependencies among components (or modules); are open to influences from the outside environment; as a whole, are more than a sum of their parts; exhibit nonlinear, dynamic behavior; have so many dimensions or variables that they are mathematically intractable. For an explanation of this list that is readable by a non-specialist, see, Melanie Mitchell, *Complexity: A Guided Tour* (Oxford and New York: Oxford University Press, 2009); and Thomas Homer-Dixon, *The Ingenuity Gap: Facing the Economic, Environmental, and Other Challenges of an Increasingly Complex and Unpredictable World* (New York: First Vintage Books, 2002), 110-115.

[26] V. Heiken, R. Brown, G. George, O. Jones, and C. Andersson, "Modeling Cities: The Los Alamos Urban Security Initiative," *Public Works Management and Policy* 4 (2000): 198-212.

[27] T. Lewis and R. Darken, "Potholes and Detours in the Road to Critical Infrastructure Protection Policy" *Homeland Security Affairs* 1, (2005): 1-11, http://www.hsaj.org/?article=1.2.1.

[28] R. Platt, *Disasters and Democracy* (Washington, D.C.: Island Press, 1999).

[29] B. Sundelius, "A Brief on Embedded Societal Security," *Information & Security* 17 (2005): 23-37.

[30] S. Cutter , L. Barnes, M. Berry, C. Burton, E. Evans, E. Tate, and J. Webb, "A Place-based Model for Understanding Community Resilience to Natural Disasters," *Global Environmental Chan*ge 18, No. 4 (October 2008): 598-606.

[31] For a more extensive review on resilience concepts and background literature, see both P.H. Longstaff at note 18 and also, P.H. Longstaff, N. Armstrong, and K. Perrin, "Building Resilient Communities: Tools for Assessment," Project on Resilience and Security white paper, Institute for National Security and Counterterrorism, Syracuse University (March, 2010), http://insct.syr.edu/uploadedFiles/insct/topics_and_projects/resilience/INSCT%20White%20Paper_Building%20Resilient%20Communities.pdf.

[32] More information about the Resilience Alliance is available at http://www.resalliance.org/1.php.

[33] F. Norris et al., "Community Resilience as Metaphor," 131.

[34] Homeland Security Studies and Analysis Institute, "Resilience Conceptual Development: An Operational Framework for Resilience" (August 27, 2009), 22, http://www.homelandsecurity.org/hsireports/Resilience_Task_09-01.pdf.

[35] Researchers in many disciplines have observed that having multiple different options, or diversification of resources, is an asset when developing resilience. See, e.g., W. Brian Arthur, "On the Evolution of Complexity," in *Complexity: Metaphors, Models and Reality* 19, ed. G. Cowan, D. Pines, D. Meltzer (Santa Fe Institute Studies in the Sciences of Complexity Proceedings, 1995), 65-78, 67. However, when a system gets more diverse, its complex interaction networks spread unevenly and the forces working on the system do not have the same effect on the diverse components. Thus, a successful strategy to increase the survivability of individuals or groups in such a system will almost never be "one size fits all" and will be most effective if choices and allocations are made at the lowest possible level.

[36] Redundancy is usually a resistance strategy and is employed where the danger to be avoided is relatively predictable or potentially catastrophic. Aircraft, for example, have multiple engines so that if one fails the redundant system will pick up that function. In human-engineered systems, sometimes-identical systems are added to back up critical systems that might fail. This type of redundancy is frequently designed into the system and generally makes it more costly. See, e.g., S.D. Sagan, *The Limits of Safety: Organizations, Accidents, and Nuclear Weapons* (Princeton, NJ: Princeton University Press, 1993).

[37] Fundamentally, robustness depends on the ability of individuals, groups, or technologies to tolerate a broad range of conditions. Robust systems have *broad tolerance* for changes in their environment. For example, a machine that can work under a wide variety of external conditions is said to be very robust. In other situations, broad tolerance depends on the ability to adapt to *changing* conditions. For example, some species are said to be robust because they can go into hibernation when water supplies are low. The ability of humans to find new ways to meet their needs in the face of surprise greatly increases their robustness or broad-tolerance resilience. We can often figure out alternative ways to procure water, food, and shelter. Sometimes robustness is accomplished with systems that are capable of performing multiple functions and can act as backup for another system. This is called *distributed robustness* in some systems and redundancy in others, see, e.g., A. Wagner, *Robustness and Evolvability in Living Systems* (Princeton NJ: Princeton University Press, 2005), 239-246.

Buffering is also a resilience strategy that results from building diversity and redundancy into a complex system. A buffering strategy may attempt to stop bad things from spreading to critical components of a system, or it might be a conscious allocation of resources that will be kept in reserve to use to shield the systems from the effects of a surprise. Levies are a buffer against rising water in a river. Computer systems often have buffers that will stop a virus from invading critical part of the system. Emergency savings accounts, surplus inventories, and slack time in manufacturing operations are also buffering strategies. All come with significant financial or opportunity cost, but they are good for dealing with frequently occurring or potentially catastrophic risks.

[38] There are tradeoffs between these three attributes. For technology with high customer expectations of reliability, betting the farm on redundancy can lead to disaster when the system is faced with a surprise that was not anticipated by the designers, and one that cannot be handled with redundant capabilities. In addition, redundancy and/or diversity could be counterproductive if the complexity of the system makes it more opaque and difficult to understand for the people who must operate it. Redundancy can also lead people to have too much confidence in the system and forget to watch for surprises. Heavy layers of redundancy or lots of diversity can furthermore make it possible to conceal errors and surprises (fearing the 'blame game"), with the result that there is less accurate information about how the system is operating.

[39] Complex systems are *adaptive* when individual agents operate independently and change their behavior in response to forces in their environments via feedback. Other agents will copy changes that result in the agents' obtaining more resources. There is some evidence that the most resilient organizations are those that have some experience with surprise and have adapted in order to survive. See Dennis S. Mileti and John H. Sorenson, "Determinants of Organizational Effectiveness in Responding to Low Probability Catastrophic Events," *Columbia Journal of World Business* (Spring 1987): 14. We would thus expect a culture that has not changed or adapted to be less resilient. In addition, the ability of an individual or group to adapt may be tied to the state of their development. Humans, organizations, social systems, and ecosystems all *develop*; that is, they change over time in form and function such that they grow, mature, die, and change in interesting ways characteristic of the species or type of organization or ecosystem, as shaped by cultural and biological evolution; see L. Gunderson and C.S. Holling, eds.,

Panarchy: Understanding Transformations in Human and Natural Systems (Washington, DC: Island Press, 2002).

[40] F. Berkes and C. Folke, "Back to the Future: Ecosystem Dynamics and Local Knowledge," in Gunderson and Holling, *Panarchy*, 141.

[41] F. Berkes, "Understanding Uncertainty and Reducing Vulnerability: Lessons from Resilience Thinking," *Natural Hazards* 41 (2007): 291.

[42] Ibid.

[43] See P.H. Longstaff at note 18.

[44] Ibid., citing C. Folke, S. Carpenter, T. Elmqvist, L. Gunderson, C.S. Holling and B. Walker, "Resilience and Sustainable Development: Building Adaptive Capacity in a World of Transformations," International Council for Science, ISCU Series on *Science for Sustainable Development*, No. 3 (April 2002), http://www.sou.gov.se/mvb/pdf/resiliens.pdf.

[45] K.G. Tidball and M.E. Krasny, "From Risk to Resilience: What Role for Community Greening and Civic Ecology in Cities?" in A. Wals, ed., *Social Learning Towards a more Sustainable World* (Wagengingen Academic Press, 2007), 149-164.

[46] There is almost universal agreement that the best starting point for trying to manage an unpredictable system is to identify the various temporal and organizational scales involved. See P. H. Longstaff at note 18. In systems that operate on more than one scale, resilience strategies can operate within each scale but also across scales. For example, in the human body, the immune system acts first on a local scale to confront an infection by sending a variety of forms of immune cells (within-scale resilience through diversity). If this strategy fails, the system responds by "scaling up" its response and inducing fever. When similar functions (not necessarily similar mechanisms) operate across scales, they make the system more resilient because they are redundant: if one function fails, the other goes into action. Each level of the system operates separately, and often each level has its own emergent properties and/or operates over different time scales and responds to different cycles. Surprises or risks that manifest themselves over a long period require different strategies than dangers that can pop up at any time. Risks to one part of the system are treated differently from those that might affect the entire system. The boundaries between scales should receive careful attention because that is where surprises are likely to occur.

[47] Network theory and science provide a substantial knowledge base on the significance of social and organizational links. See, e.g., A. Barabasi, *Linked: The New Science of Networks* (Cambridge, MA: Perseus Press, 2002), Chapter Six; D. J. Watts, *Small Worlds: The Dynamics of Networks Between Order and Randomness* (Princeton, NJ: Princeton University Press, 1999), 285; J.W. Meyer and W. R. Scott, *Organizational Environments: Ritual and Rationality* (Beverly Hills, CA: Sage, 1983); B. Uzzi, "Social Structure and Competition in Interfirm Networks: The Paradox of Embeddedness," *Administrative Science Quarterly* 42, No. 1 (1997): 35-67; M. J. Dollinger, "The Evolution of Collective Strategies in Fragmented Industries," *Academy of Management Review* 15, No. 2 (1990): 266–285; E. Patterson, D. Woods, R. Cook, and M. Render, "Collaborative Cross-Checking to Enhance Resilience," *Cognition, Technology and Work* 9, No. 3 (2007): 155-162; J. D. Orton and K. E. Weick, "Loosely Coupled Systems: A Reconceptualization," *Academy of Management Review* 15, No. 2 (1990): 203–223.

[48] See, e.g., M. Granovetter, "The Strength of Weak Ties," *The American Journal of Sociology* 48, No. 6 (1973): 1360-1380; S. Snook, *Friendly Fire: The Accidental Shootdown of U.S. Black Hawks Over Northern Iraq* (Princeton, N.J.: Princeton University Press, 2000).

[49] K. Perrin, "Operationalizing Resilience: Assessment Models for Community Resilience," resilience and security working paper (Institute for National Security and Counterterrorism, Syracuse University, August 2009), http://www.insct.syr.edu/Projects/Resilience/Home.htm.

[50] Additionally, these subsystems closely correspond to the six Recovery Support Functions outlined in the Department of Homeland Security's draft *National Disaster Recovery Framework* (Washington, DC: February 2010): Community Planning & Capacity Building; Economic Development; Health, Social & Community Services; Housing; Infrastructure Systems; and Natural and Cultural Resources. The major difference in our approach is that "housing" would be considered within the scope of physical infrastructure and "cultural resources" would be included in civil society. Fundamentally, both our chosen subsystems and DHS recovery support functions address the same core elements of a community – the

only real difference is the chosen boundaries between them. Yet, as the descriptions below illustrate, resilience attributes could just as easily be described within the narrower conception of disaster response functions.

[51] S.A. Ostroumov, "New Definitions of the Concepts and Terms Ecosystem and Biogeocenosis," *Doklady Biological Sciences* 383 (2002): 141–143. Translated from *Doklady Akademii Nauk* 383, No. 4 (2002): 571–573.

[52] B. Walker and D. Salt, *Resilience Thinking: Sustaining Ecosystems and People in a Changing World,* (Washington, DC: Island Press, 2006).

[53] See A. Rose, "Economic Resilience to Natural and Man-made Disasters: Multidisciplinary Origins and Contextual Dimensions," *Environmental Hazards* 7 (2007): 383–398.

[54] L. Brigulio, G. Cordina, S. Bugeja, and N. Farrugia, "Conceptualizing and Measuring Economic Resilience," working paper (Economics Department, University of Malta, 2006), https://secure.um.edu.mt/__data/assets/pdf_file/0013/44122/resilience_index.pdf.

[55] Ibid.

[56] See U.S. EPA, Office of Grants and Debarment, definition of "Infrastructure" for purposes of the American Recovery and Reinvestment Act of 2009, May 8, 2009, http://www.epa.gov/ogd/forms/Definition_of_Infrastructure_for_ARRA.pdf. Because of the critical nature of information sharing to community resilience, we exclude communication infrastructure from this section of our analysis and explore it as a stand alone category.

[57] U.S. Agency for International Development (USAID), "How Resilient is Your Coastal Community? A Guide for Evaluating Coastal Community Resilience to Tsunamis and Other Coastal Hazards," (U.S. Indian Ocean Tsunami Warning System Program, 2007), http://apps.develebridge.net/usiotws/13/CoastalCommunityResilience%20Guide.pdf.

[58] P. Healey, "Creativity and Urban Governance," *Policy Studies* 25, No. 2 (2004): 87-102.

[59] L. Lebel, J. Anderies, B. Campbell, C. Folke, S. Hatfield-Dodds, T. Hughes, and J. Wilson, "Governance and the Capacity to Manage Resilience in Regional Social-ecological Systems," *Ecology and Society* 1, No. 1 (2006): 19.

[60] For more background on performance management in public administration see G.A. Brewer, "Building Social Capital: Civic Attitudes and Behavior of Public Servants," *Journal of Public Administration Research and Theory* 13 (2003): 5-26; H. Hatry, *Performance Measurement: Getting Results* (Washington, DC: Urban Institute, 1999); E.T. Jennings and M. Patrick Haist, "Putting Performance Measurement in Context," in P.W. Ingraham and L.E. Lynn, eds., *The Art Of Governance* (Washington, DC: Georgetown University Press, 2006), 173-194; J. Melkers and K. Willoughby, "Models of Performance-Measurement Use in Local Governments: Understanding Budgeting, Communication, and Lasting Effects," *Public Administration Review* 65 (2005): 180-90; and T.H. Poister and G. Streib, "Performance Measurement in Municipal Government: Assessing the State of the Practice," *Public Administration Review* 59 (1999): 325-335.

Homeland Security and Support for Multiculturalism, Assimilation, and Omniculturalism Policies among Americans

Fathali M. Moghaddam and James N. Breckenridge

This article presents data suggesting that Americans' views of policies toward immigrants are pertinent to matters of homeland security. "Homeland" is a concept shaped partly by how people psychologically differentiate "citizen" from "immigrant." The differentiation of these categories is critical to individuals' political and social identity. Homeland security scholars are unlikely to be aware, however, of this country's substantial majority preference for an alternative to the traditional, yet deeply divided, incompatible policies of assimilation and accommodation. Moreover, the publics' appraisal of the threat of terrorism, the priority they assign to homeland security institutions, their trust and confidence in homeland security organizations, and their support for counter-terrorism measures are linked to their immigration policy preference even after accounting for their race/ethnicity and socioeconomic status. Homeland security professionals would do well to consider the potential implications of these preferences.

Practitioners and researchers in the domain of security have been engaged for several decades in an important debate concerning the relative merits of a "realist" versus a "human security" approach.[1] The realist approach focuses primarily on military security, and represents the dominant school in the domain of security studies. The human security approach is newer and involves an emphasis on health security, food security, shelter security, and other "humanitarian" concerns that are argued to be a priority for ordinary people in their everyday lives. Although the debate between the realist and human security camps has been constructive, there is a danger that both approaches are being left behind by new challenges created by accelerating globalization. Among the most important of these challenges is rapid and large-scale movement of people around the world bringing about "sudden" intergroup contact.[2]

Humans have always been migrating, starting from Africa to reach all the major landmasses by about 10,000 years ago.[3] But until fairly recently, migrations were relatively slow. The human groups in interaction had more time to adapt to one another. In the modern era, using jet planes and rapid trains, large numbers of people can move long distances in a relatively short time. The availability of rapid transportation systems has been coupled with the globalization of the economy, so that a demand for cheaper labor in one part of the world can be met with a speedy supply of cheaper labor from other parts of the world. Consequently, in the last few decades there has been a rapid increase of South Asians in the United Kingdom, North Africans in France, and Turks in Germany, with the result that there are now about twenty million Muslims in the European Union.

Rising intergroup contact in recent decades has created new tensions in the European Union, and these tensions have been further intensified by a series of terrorist attacks. The most well-publicized of these attacks are the March 11, 2004, bomb explosions on trains in Madrid which resulted in close to 200 deaths and over 1,000 serious injuries, and the July 7, 2005, bomb explosions on the London public transportation system, which also resulted in multiple fatalities and serious injuries. An outcome of terrorist

attacks has been a re-examination of policies for managing diversity; Europeans have been forced to ask, are we integrating minorities the best way? For example, Andrew Jakubowicz assessed reactions to the London terrorist bombings in this way: "The updraft from the bombings carried a message about the critical importance of working out what 'multiculturalism' could continue to mean."[4] This question was brought into sharp focus when the Dutch filmmaker Theo Van Gogh was brutally murdered in Amsterdam by an Islamic fanatic on November 2, 2004. Van Gogh's "crime" was that he had, in collaboration with the Dutch Muslim feminist Ayaan Hirsi Ali, made a short film, *Submission*, critical of the treatment of women in Islamic societies. Van Gogh's murder put the spotlight on the Muslim fanatics in Europe, and forced Europeans to critically re-think their policies for managing diversity. Similarly, the threat of home-grown terrorism in the United States, highlighted by the case of about twenty young Somali-Americans apparently recruited by violent Islamic fanatics, has fueled a debate about the best policies for managing diversity in the United States, as well as the threat of terrorism, trust in government, and related security issues.

Two main policies have been used to manage cultural and linguistic diversity: *assimilation*, the washing away of intergroup differences, and *multiculturalism*, the highlighting, strengthening, and celebration of intergroup differences.[5] Both these policies are founded on psychological assumptions, some of which are questionable.[6] An assumption underlying assimilation policy, for example, is that intergroup differences can be washed away through contact, to eliminate any important basis for group-based divisions. But social identity research using the minimal group paradigm demonstrates that group members can use even trivial criteria as a basis for intergroup differentiation and ingroup favoritism.[7] By implication, no matter how similar the members of a society become through assimilation, it will be possible to manufacture dissimilarity, even on seemingly trivial criteria. Some of the key psychological assumptions underlying multiculturalism are also questionable, including the *multiculturalism hypothesis*, the idea that confidence in one's own ethnic heritage will lead one to be open and accepting toward the outgroup members. Empirical evidence does not provide solid support for this hypothesis,[8] nor do historical examples, such as the Nazis, who arguably showed high confidence in their ingroup heritage, but were not open and accepting toward outgroups (although there is support for some interpretations of multiculturalism, particularly among minorities).[9]

There is continued debate between supporters of multiculturalism and assimilation,[10] and some efforts to compare the two policies using empirical evidence.[11] However, given that the psychological assumptions underlying both policies are in important ways flawed, we should also explore alternative policies that are already an implicit part of psychological discussions of intergroup relations.[12] Muzafer Sherif's concept of superordinate goals,[13] and Gaertner and Dovidio's Common Group Identity Model both suggest a third alternative policy, whereby groups emphasize commonalities such as identities and goals.[14] This third alternative is reflected in the policy of omniculturalism, which proposes a two-stage process in the socialization of individuals: during stage one, the focus is on human commonalities; during stage two, intergroup differences and distinctiveness are introduced.[15] The objective of omniculturalism is to establish a solid basis of commonality between people within the framework of a primary identity, before

adding an emphasis on how people also belong to groups that in some respects differ from one another.

The present study examines three research questions. The first concerns the extent to which Americans would support omniculturalism, as compared with multiculturalism and assimilation. The second concerns the support of majority and minority group members for the different policies. Some previous research has demonstrated that African Americans and other minorities show stronger support for multiculturalism, whereas white Americans show stronger support for assimilation policy.[16] A third set of research questions – the central focus of this article – concern possible differences in the attitudes of supporters of assimilation, multiculturalism, and omniculturalism, toward homeland security threats, how America should react to such threats, and the extent to which individuals trust authorities to do the right thing.

In summary, terrorist attacks in Western democracies, such as the United States, the United Kingdom, and Spain, have resulted in a re-assessment of multiculturalism and other policies for managing diversity.[17] Because assimilation has been endorsed to a greater degree by majority groups (primarily of western European descent), and because terrorist attacks are perceived as arising from minority (primarily Middle Eastern) communities, we expected support for assimilation to be associated with greater concern about future terrorist attacks, as well as stronger American reactions to terrorist attacks. Growing concerns about the possibility of "home grown" terrorism may increase the salience of these issues for American security practitioners and researchers, especially in light of current population projections, which suggest that by 2050 whites will represent a minority and one out of five Americans will be an immigrant.[18]

Methods

Participants in this research were a nationally representative probability sample of 4,000 adults age eighteen and older selected randomly from an internet-enabled panel maintained by Knowledge Networks (KN) in November 2008. KN panel members are recruited through a random digit telephone dialing system based on a sample frame covering the entire United States. In contrast to "opt-in" Web surveys, which recruit participants of unknown characteristics via "blind" Internet solicitations, KN panel members are selected on the basis of known, non-zero probabilities. Individuals are not permitted to volunteer or self-select for participation in the KN panel. In addition, individuals who lack either computers or Internet access are provided equipment or access without charge. KN panel-based surveys have demonstrated acceptable concordance with a variety of "benchmark" large-scale surveys.[19]

In the present study, the response rate to invitations to participate was 71 percent. To reduce the effects of potential non-response and non-coverage bias, post-stratification sample weights,[20] incorporating the probability of participant selection based on age, gender, race, and ethnicity benchmarks from the most recent available Census Bureau *Current Population Survey* and supplements were employed in all statistical analyses using algorithms modified for complex survey designs in the statistical software packages STATA.[21]

MEASURES

Cultural policy preferences. Participants were grouped into one of three perspectives on cultural differences policies according to participants' response to the following question:

"Which statement below best fits your view about immigration to the United States: When people come to America,

1. People should set aside their cultural differences and "melt into" the American mainstream;
2. People should maintain and celebrate their distinct group culture
3. People should first recognize and give priority to what they have in common with all other Americans, and then at a second stage celebrate their distinct group culture."

We label responses 1 thru 3 Assimilation, Multiculturalism, and Omniculturalism, respectively. Participants could also choose not to declare any preference.

Political ideology. Participants identified their favored political ideology as "extremely liberal," "liberal," "somewhat liberal," "moderate or middle of the road," "slightly conservative," "conservative," or "extremely conservative." In the following analyses, participants were grouped into three categories: *liberal* (extremely liberal or liberal), *conservative* (extremely conservative or conservative), or *other* (all other responses).

Terrorism risk perceptions. Participants rated the probability over the next five years of terrorist attacks using an anchored scale from zero ("totally unlikely to occur") to 100 ("absolutely certain to occur") and assessed the probability of acts of terror within the country (*risk to nation* – "How likely do you feel a terrorist attack is somewhere within the United States?"), as well as attacks directly involving the participant (*risk to self* – "How likely do you feel that you personally will directly experience an act of terrorism?"). An additional dichotomous indicator variable was included representing participants who reported that they were "very concerned" or "extremely concerned" about terrorism ("How concerned or worried are you about a terrorist attack happening in the area of the country where you live sometime during the next 12 months?").

Emotional response to the threat of terrorism. Following the instructions, "Please help us to understand how you feel when you think about threats of terrorism using the following scale," participants completed the *Positive and Negative Affect Schedule – Expanded Form*,[22] which requires participants to rate sixty emotional adjectives on a five-point scale from one ("slightly or not true of your feelings") to five ("extremely true of your feelings"). Composite subscales assessing the degree of fear and anger were employed in the present study. These subscales have demonstrated good psychometric properties in other samples and have been significantly correlated with public perceptions about terrorism and support for various counterterrorism policies.[23]

Confidence in government, preparedness, counterterrorism measures, and security priorities. Participants were also asked whether they "agreed," "strongly agreed," "disagreed," or "strongly disagreed" with a series of statements related to

terrorism and terrorism policies. To simplify the presentation of results, responses were collapsed into categories indicating either agreement or disagreement. Statements assessed *confidence* in certain government organizations (i.e., the federal and state governments, the Immigration and Customs Enforcement agency, the Border Patrol, in response to the statement "This organization will do a good job carrying out its role in fighting terrorism"), community terrorism *preparedness* ("I believe my community is sufficiently prepared for a terrorist attack if it happened here"), and the *importance of revenge* ("It is important for United States to take revenge on the people and countries responsible for terrorist acts against this country"). In addition, participants were asked whether they agreed that in order to "protect against terrorism" the government should adopt certain *measures*, including "Engage in racial or ethnic profiling," "Restrict the rights of non-citizens and foreign visitors," or "Require all Americans to have a national identification card." Finally, participants were asked to rank terrorism-versus disaster-related activities as the top "homeland security priority for the United States."

RESULTS

More than three out of five American adults preferred omniculturalism.[24] Among those who preferred another policy, more favored assimilation over multiculturalism (Table 1). Gender, age, race and ethnicity, education, income, political ideology, and urban residential status distributions within policy preference groups are listed in Table 2.

Cultural View	Percent	95% C.I.
Assimilation "People should set aside their cultural differences and 'melt into' the American mainstream."	19.67%	(18.19 – 21.24)
Multiculturalism "People should maintain and celebrate their distinct group culture."	13.81	(12.43 – 15.30)
Omniculturalism "People should first recognize and give priority to what they have in common with all other Americans, and then at a second stage celebrate their distinct group culture."	62.71	(60.77 – 64.61)
Elected not to respond	3.81	(3.04 – 4.77)

Table 1: Distribution of Endorsements

Though most members of each sociodemographic category preferred omniculturalism, distinct sociodemographic profiles differentiated proponents of assimilation or multiculturalism. Significantly greater proportions of women, adults under age forty-five, members of non-white races or ethnicities, urban residents, or political liberals, characterized multicultralists. Conversely, white non-Hispanics, older adults over age fifty-nine, individuals with annual household incomes from $10,000 to $20,000, and

political conservatives were more prevalent among assimilationists. Assimilationists were also more apt to have partial or full high school educations, but were less likely to have pursued or completed college educations.

Variable	Cultural Policy Preference			Total Sample (100%)
	Assimilation (19.7%)	Multiculturalism (13.8%)	Omniculturalism (62.7%)	
Gender				
Female	47.5%	***60.8%*** [a]	49.5%	51.3%
Age				
18-29	15.4	***32.0*** [a]	21.4	21.7
30-44	24.3	***31.4*** [a]	26.7	26.9
45-59	30.1	25.5	28.3	28.3
60+	30.2	***11.1*** [a]	23.6	23.2
Race/Ethnicity				
White, Non-Hispanic (NH)	77.7	***56.9*** [a]	75.9	73.5
Black (NH)	8.6	***12.9*** [a]	8.8	9.4
Other (NH)	3.6	***8.6*** [a]	4.1	4.6
Hispanic	9.2	***20.6*** [a]	10.1	11.4
Multiple Race/Ethnicities	1.0	1.0	1.1	1.1
Education				
< High School	***16.6*** [b]	14.1	9.9	11.9
High School	***38.6*** [b]	25.6	29.6	30.9
Some College	***24.1*** [b]	31.4	29.4	28.6
B.A. or higher	***20.7*** [b]	28.9	31.1	28.7
Income				
< $10,000 ($10k)	6.3	5.3	4.9	5.3
$10k - $19k	***12.9*** [b]	6.3	8.7	9.2
$20k - 39k$	25.9	25.1	22.5	23.6
$40k - $59k	20.1	23.6	20.0	20.6
$60k - $99k	23.4	25.8	26.8	26.0
$100k -$174k	9.0	11.6	14.0	12.6
$175k +	2.4	2.4	3.0	2.8
Urban-Rural Classification				
Urban	81.3	***86.9*** [a]	82.3	82.8
Political Ideology				
Conservative	***26.1*** [b]	13.6	22.5	21.9
Liberal	11.6	***24.8*** [a]	16.0	16.2

Table 2: Distribution of Sociodemographic Variables by Policy Preference

[a] Differs significantly from Assimilation and Omnicultural groups $p < .005$ (two-tailed)
[b] Differs significantly from Multicultural and Omnicultural groups $p < .003$ (two-tailed)

Average predicted probabilities of a terrorist attack on the nation or against the self, as well as average levels of fear and anger experienced in response to terrorism within each group are shown in Figure 1. Responses for the omnicultural group closely tracked the average national response. Assimilationists reported the most elevated appraisals of the probability of attacks against the nation or self, as well as the greatest degree of anger in response to terrorism. Omniculturalists, however, reported significantly less fear than either assimilationists or multiculturalists, but averaged significantly higher appraisals than multiculturalists of the likelihood of a terrorist attack on the nation.

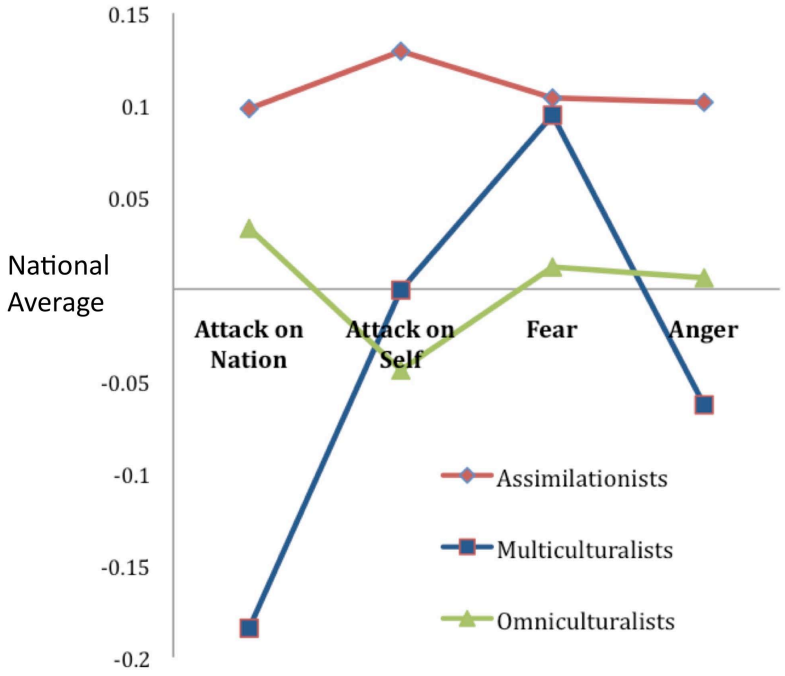


Figure 1: Average Perceived Threat and Emotional Response by Cultural Policy Preference

(Vertical axis indicates deviation from national averages as a percentage of one standard deviation. Differences are significant at $p < .01$)

Participants' priorities and support for particular responses to the threat of terrorism reflected these divergent views of threat and emotional response (Table 3). Intense worries about terrorism were least common among multiculturalists and most prevalent among assimilationists. Significantly more assimilationists – in contrast to significantly fewer multiculturalists – viewed terrorism as the top homeland security priority, and also asserted the importance of seeking revenge against terrorist actions. Moreover, support for modifying civil liberties to prevent terrorism – racial profiling, restricting the rights of non-citizens, and requiring a national identity card – was most prevalent among assimilationists and once again, least prevalent among multiculturalists. While more assimilationists had confidence in the federal government's capacity to counter terrorism, more multiculturalists had confidence in the Immigration and Customs Enforcement. Omniculturalists were more likely to view disaster preparedness as the top homeland security priority and to judge their communities as better prepared for crises.

Variable	Cultural Policy Preference		
	Assimilation	Multiculturalism	Omniculturalism
"Very" or "extremely" worried about terrorism	***26.7%*** [b]	***12.8%*** [a]	22.6%
Top priority for Homeland Security:			
Terrorism	***77.7*** [b]	***64.4*** [a]	68.5
Disasters	11.6	12.7	***18.8*** [c]
Confidence in:			
Federal Government	***71.1*** [b]	65.9	65.9
Immigration & Customs Control	53.3	***61.2*** [a]	53.2
Border Patrol	66.4	65.6	***59.9*** [c]
State Government	66.1	65.6	66.8
Views community as unprepared for terrorist attack	60.5	61.2	***66.7*** [c]
Believes it is important for U.S. to seek revenge	***75.1*** [b]	***54.1*** [a]	64.7
In order to prevent terrorism, supports:			
Racial profiling	***46.9*** [b]	***21.8*** [a]	35.2
Restrict rights of non-citizens and foreign visitors	***78.2*** [b]	***54.7*** [a]	70.5
Require national ID card	***68.6*** [b]	***49.6*** [a]	56.4

Table 3: Terrorism Concerns, Priorities, Confidence & Support for Aggressive Measures by Cultural Policy Preference

[a] Differs significantly from Assimilation and Omnicultural groups $p < .001$ (two-tailed)
[b] Differs significantly from Multicultural and Omnicultural groups $p < .001$ (two-tailed)
[c] Differs significantly from Multicultural and Assimilation groups $p < .001$ (two-tailed)

With respect to security priorities and responses, omniculturalism was situated between the extremes of the alternative cultural policy preferences. Moreover, when multivariate procedures were employed to adjust statistically for sociodemographic differences among cultural preference groups, the differences among omniculturalists, multiculturalists, and assimilationists in perceived threat, emotional response, security priority, confidence in government, perceived community preparedness, and support for aggressive responses to terrorism were sustained.

DISCUSSION

The objective of this study was to explore attitudinal support among Americans for the traditional policies of assimilation and multiculturalism, as well as the new policy of omniculturalism. A second research question focused on the support of majority and minority groups for the different policies. Third, we explored the relationship between support for different policies for managing cultural diversity and security issues, specifically related to the threat of terrorist attacks, how America should react to attacks, feelings about the possibility of terrorist attacks, and trust in authorities to do the right thing in response to terrorist attacks.

With respect to support for different cultural diversity policies, omniculturalism represented a clear majority preference across all sociodemographic groups, although there were some sub-group differences: whites, men, and older adults were more prevalent among assimilationists; non-whites, women, and younger adults were more prevalent among multiculturalists. Consequently, any future exploration of the omnicultural perspective must also attend to the generational and diversity differences that underlie dissenting perspectives among a significant portion of the population. That such differences predicted the roughly 4 percent of participants who declined to state a cultural preferences, as well as the 29 percent of those who declined to participate in this survey further,[25] underscores the need for careful scrutiny of the pattern of minority preferences identified in the present study.

Preferences for cultural policies were correlated significantly with terrorism threat perceptions and emotional responses, as well as attitudes towards homeland security priorities, confidence in certain governmental organizations' capacities to carry out their counterterrorism missions, and willingness to modify civil liberties to prevent terrorism. Although assimilationists did not differ from multiculturalists in reported fear, assimilationists expressed the highest levels of anger, an affective response associated strongly with support for aggressive counterterrorism policies in other studies.[26] Indeed, support for aggressive measures was most common among assimilationists, a group which also judged the likelihood of future attacks as more probable than those who endorsed alternative cultural policies, and least prevalent among multiculturalists, a group which appraised national threats of terrorism as less likely than other groups. In several respects, the attitudes towards homeland security among omniculturalists represented a middle ground between the divergent views of assimilationists and multiculturalists.

Omniculturalism arises in part out of well-researched ideas in the social psychology of intergroup relations. Both the earlier field research of Sherif and the more recent

experimental research of Gaertner and Dovidio have demonstrated that the re-categorization of the members of different groups as a single group can reduce the original intergroup biases.[27] The applied benefits of superordinate goals have been demonstrated in culturally and ethnically diverse classrooms.[28] The Common Ingroup Identity Model has taken the further step of carefully exploring potential antecedents, consequences, and mediating processes of re-categorization that results in a superordinate category.[29] However, missing from this picture has been empirical evidence to suggest that a "third alternative" along these lines would be supported among the general population.

This study presented participants a third alternative, omniculturalism, with two steps: First, recognizing what is common to all Americans, second, celebrating distinct group cultures. Endorsement of this alternative policy represents positive feedback for research exploring the path of re-categorization, but it also highlights a need for additional research on developmental questions. In particular, at what age should the education of children emphasize what is common to everyone, and at what age should the focus be on distinct group cultures? Input from developmental science should guide schools and other socialization agents on this question. In future research, more attention also needs to be given to the difference in support shown by majority and minority group members for the three policies for managing diversity. An important limitation to the present study is that perspectives on cultural policy were measured by a single item. Future studies should include multiple measures, as well as, perhaps, comparisons among each pair of alternatives. Our statistical analyses utilized post-stratification weights to adjust for sampling biases. Nevertheless, the sociodemographic factors we found associated with a preference for assimilation or multiculturalism in this study also tended to characterize individuals in the KN panel who declined to participant. Thus, the magnitude of support for omniculturalism – albeit, considerable (i.e., 60 percent) – could well have been attenuated if all invited participants had been recruited successfully for the survey.

We believe that the alternative policy of omniculturalism also has potential to both gain support from diverse populations internationally and serve as an effective policy at the international level. This is because omniculturalism presents opportunities for groups to both find common ground in shared human characteristics and establish their own special (and perhaps unique) characteristics at a secondary level. A challenge in future research is to further explore these possibilities internationally.

Support for different policies for managing diversity was systematically associated with different patterns of attitudes toward security issues. Support for assimilation was associated with greater concern and anger about the possibility of a terrorist attack, as well as support for stronger reactions in the case of an attack. This included greater willingness to seek revenge, to carry out racial and ethnic profiling, and to restrict the civil liberties of foreigners in case of a terrorist attack. In contrast, supporters of multiculturalism policy downplayed the possibility of a terrorist attack and were least likely to seek revenge and agree to racial and ethnic profiling, as well as to impose restrictions on the civil liberties of foreigners as a protection against terrorism. We believe this pattern of results is explained in part by the fact that support for multiculturalism was most prevalent among minority groups, whereas support for assimilation was most prevalent among majority groups. At the same time, terrorist

attacks have been seen as emanating from Islamic communities (within and outside Western societies), and the target of such attacks have often been major urban centers in the West, such as New York, London, and Madrid. Thus, majority groups support assimilation of minorities into mainstream society, and perceive terrorism (emanating from minority communities) as a greater threat and something to be angry about and avenged.

The pattern of distrust toward authorities shown by supporters of assimilation and multiculturalism was also different. Whereas supporters of assimilation expressed greater confidence in the counterterrorism capacity of the federal government, supporters of multiculturalism expressed greater trust and confidence in the present capabilities of Immigration and Customs Enforcement. These differences might be attributed to controversy regarding illegal immigration. Multiculturalists' confidence in the status quo perhaps reflects a reluctance to support strengthening immigration controls; conversely, assimilationists' lack of confidence might reflect greater willingness to strengthen immigration controls.

The finding that support for different policies for managing cultural diversity was systematically related to attitudinal differences toward security issues reflects back in important ways on the traditional debate between the two main sides in debates about security, suggesting an interactive link between factors identified by realists and human security advocates. On the one hand, the large-scale movement of people and sudden contact between human groups can result in "host" majority groups feeling threatened, desiring the minority to assimilate, and wanting revenge for terrorist attacks.[30] Furthermore, in this context the majority seems to have less confidence in federal and immigration authorities to do the right thing. These trends are no doubt to some extent associated with the majority groups perceiving the influx of "aggressive" minorities as increased competition for scarce resources. However, more than material resources are involved: minority groups support multiculturalism and seem to want to maintain their distinct identities. They are less fearful about terrorist attacks and do not support America "avenging" such attacks. Clearly, both material factors, identified by realists, and "soft" factors such as identity, identified by advocates of human security, are involved in these intergroup processes.

Since the 1990s there has been increased focus on the approximately 12-15 million illegal immigrants believed to be in the United States. For many, illegal immigrants represent a "threat" that requires an immediate solution. However, even if the "problem" of illegal immigration is solved, the far greater challenge of managing an increasingly diverse population of United States citizens looms ahead of us. In the long term, even if all 12-15 million illegal immigrants either become legal or leave the country (an unlikely event), effective policies are still urgently required for managing inter-group relations among the enormously diverse population of over 300 million Americans, which today includes 37 million legal first-generation immigrants. Such policies must receive greater attention from authorities, researchers, and others concerned with homeland security. The findings of this study highlight the value of exploring alternative policies for managing diversity, as well as critically re-thinking links between both alternative and traditional policies and homeland security.

Fathali M. Moghaddam is professor, Department of Psychology, and director of the Conflict Resolution Program, Department of Government, Georgetown University. His most recent book is The New Global Insecurity *(2010); more details about his research and publications can be found at his website: www.fathalimoghaddam.com.*

James N. Breckenridge, PhD, is professor of psychology and co-director of the PGSP–Stanford Consortium at the Palo Alto University. He is also associate director of the Center for Interdisciplinary Policy, Education and Research on Terrorism (CIPERT) and a senior fellow at the Center for Homeland Security and Defense (CHDS).

Correspondence regarding this paper should be directed to the first author.

This research was supported in part by funding from the Department of Homeland Security through the Center for Homeland Defense and Security at the Naval Postgraduate School, Monterey, CA.

---

[1] A. Collins, ed., *Contemporary Security Studies* (Oxford University Press, 2007); M.I. Midlarsky, *Handbook of War Studies* (Boston: Unwin Hyman, 1989); R. Paris, "Human Security: Paradigm Shift or Hot Air?" *International Security* 26 (2001):87-102; M. Weissberg, "Conceptualizing Human Security," *Swords and Ploughshares: A Journal of International Affairs* XIII (2003): 3-11.

[2] F.M. Moghaddam, *Multiculturalism and Intergroup Relations: Psychological Implications for Democracy in Global Context* (Washington, DC: American Psychological Association Press, 2008).

[3] S. Wells, *The Journey of Man: A Genetic Odyssey* (Princeton, NJ: Princeton University Press, 2002).

[4] A. Jakubowicz, "Anglo-multiculturalism: Contradictions in the Politics of Cultural Diversity at risk," *International Journal of Media and Cultural Politics* 2 (2006): 255.

[5] W.E. Lambert and D.M. Taylor, *Coping with Cultural and Racial Identity in Urban America* (New York: Praeger, 1990).

[6] Moghaddam, *Multiculturalism and Intergroup Relations.*

[7] H. Tajfel, C. Flament, M.G. Billig, and R.F. Bundy, "Social Categorization and Intergroup Relations," *European Journal of Social Psychology* 1 (1971): 149-177.

[8] Lambert and Taylor, *Coping with Cultural and Racial Identity*.

[9] M. Verkuyten, "Ethnic Group Identification and Group Evaluation among Minority and Majority Groups: Testing the Multiculturalism Hypothesis," *Journal of Personality and Social Psychology* 88 (2005): 121-138.

[10] B.J. Fowers and B.J. Davidov, "The Virtue of Multiculturalism: Personal Transformation, Character, and Openness to the Other," *American Psychologist* 61 (2006): 581- 594.

[11] J.A. Richeson and R.J. Nussbaum, "The Impact of Multiculturalism versus Color-blindness on Racial Bias," *Journal of Experimental Social Psychology* 40 (2004):417-423; C. Wolsko, B. Park, C.M. Judd, and B. Wittenbrink, "Framing Interethnic Ideology: Effects of Multicultural and Color-blind Perspectives on Judgments of Groups and Individuals," *Journal of Personality and Social Psychology* 78 (2000): 635-654.

[12] B. Park and C. M. Judd "Rethinking the Link between Categorization and Prejudice within the Social Cognition Perspective, *Personality and Social Psychology Review* 9 (2005): 108-130.

[13] M. Sherif, *Groups in Harmony and Tension: An Integration of Studies on Intergroup Relations* (New York: Octagon Books, 1973).

[14] S.L. Gaertner and J.F. Dovidio, *Reducing Intergroup Bias: The Common Ingroup Identity Model* (Philadelphia, PA: Psychology Press, 2000).

[15] F.M. Moghaddam, "Omniculturalism: Policy solutions to Fundamentalism in the Era of Fractured Globalization," *Culture & Psychology* 15 (2009): 337-347.

[16] J.D. Vorauer, A. Gagnon, and S.J. Sasaki, "Salient Intergroup Ideology and Intergroup Interaction," *Psychological Science* 20, No. 1, (2009): 444-446; Wolsko et al., "Framing Interethnic Ideology."

[17] Jakubowicz, "Anglo-multiculturalism."

[18] J.S. Passel and D.V. Cohn, *Pew Social and Demographic Trends: U.S. Populations Projections: 2005-2050*, http://pewsocialtrends.org/pubs/703/population-projection-united-states.

[19] L.C. Baker, M.K. Bundorf, S. Singer, and T.H. Wagner, *Validity of the Survey of Health and the Internet and Knowledge Network's Panel and Sampling* (Palo Alto, CA: Stanford University, 2003), http://www.knowledgenetworks.com/ganp/reviewer-info.html; J.M. Dennis and R. Li, "More Honest Answers to Web Surveys? A study of Data Collection Mode Effects," *Journal of Online Research* (October 2007):1-15; T. Heeren, E.M. Edwards, J.M. Dennis, S. Rodkin, and R.W. Hinson, "A Comparison of Results from an Alcohol Survey of a Prerecruited Internet Panel and the National Epidemiologic Survey on Alcohol and Related Conditions," *Alcoholism: Clinical and Experimental Research* 32 (2008): 222-229.

[20] In contrast to "opt in" Internet-based surveys, in which only the reported demographics of participants who choose to volunteer for the survey are available, complete population demographics for the KN Panel are known prior to survey recruitment. Consequently, a unique advantage of sampling from a pre-recruited web-enabled panel is that the sociodemographic characteristics of panel members who declined the invitation to participate can be unambiguously described. In this study, people who declined to participate were more likely to be female, under age thirty, black or Hispanic, and have a high school or less education. Statistical analyses that fail to account for response rate differences among such subgroups of participants can bias estimates of effects and yield imprecise and misleading standard errors and confidence intervals. Sampling weights are typically employed to reduce bias of this kind. Details regarding the Knowledge Networks panel design and post-stratification sample weighting are available on-line at http://www.knowledgenetworks.com/ganp/docs. Briefly, an iterative process is used to create weights that are inversely proportional to the probability of selecting each subject, i.e., the proportion of people in the population belonging to each "cell" or cross-classification by age, gender, race/ethnicity, education, income, and geographic region groups. Participants in over-represented cells are weighted less; participants in under-represented cells are weighted more. Iteration is continued until the distribution of weighted data converges on the most recently available U.S. Census distributions for each cell. Sampling weights are employed in subsequent statistical analyses to adjust for response rate and coverage biases and to strengthen the representativeness of results.

[21] Bureau of Labor Statistics and U.S. Census Bureau, *Current Population Survey,* (Washington, DC: U.S. Census Bureau, 2008), http://www.census.gov/cps/; StataCorp, *Stata Statistical Software: Release 10* (College Station, TX: StataCorporation, 2007).

[22] D. Watson and L.A. Clark, *The PANAS-X. Manual for the Positive and Negative Affect Schedule – Expanded Form* (Iowa City, IA: University of Iowa, 1994).

[23] J.N. Breckenridge and P.G. Zimbardo, "The Political Psychology of Terrorism Five Years after September 11," paper presented at the International Society of Political Psychology (2007); Breckenridge and Zimbardo, "The Psychology of Political Violence: Implications for Constructive Public Policy?" paper presented at the American Psychological Association (2007).

[24] Some participants (3.8 percent) declined to state a cultural policy preference. A logistic regression of response status (no stated preference versus any stated preference) on the sociodemographic variables listed in Table 2 was statistically significant ($F(17, 4000) = 2.57$, $p < .001$), indicating that non-response could not be construed as randomly missing data. Participants who had received some college education were twice as likely as those with less than a high school education to endorse one of the three cultural policy perspectives (AOR (adjusted odds ratio) = .484, $p < .01$). Participants with annual incomes between $60,000 and $174,000 were from three to five times more likely to respond than participants in the lowest income category (AOR= .319, $p < .001$ and AOR = .179, $p < .001$, for incomes $60,000-99,000 and $100,000-174,000, respectively). The remaining analyses in this paper are confined to participants who chose one of the three perspectives on cultural differences, but include all demographic indicators as covariates throughout. A multinomial logistic regression of declared cultural policy alternatives

(assimilation, multiculturalism, omniculturalism) on all predictors (gender, age, race and ethnicity, education, income, political ideology, and urban/rural status) was also statistically significant ($F(40,3840) = 4.62$, $p < .0001$).

[25] See previous note.

[26] See note 23, Breckenridge and Zimbardo.

[27] Sherif, *Groups in Harmony and Tension;* S.L. Gaertner and J.F. Dovidio, "Understanding and Addressing Contemporary Racism: From Aversive Racism to the Common Ingroup Identity Model," *Journal of Social Issues* 61 (2005): 615-639.

[28] E. Aronson, C. Stephan, J. Sikes, N. Blaney, and M. Snapp, *The Jigsaw Classroom* (Beverly Hills, CA.: Sage, 1978).

[29] Gaertner and Dovidio, "Understanding and Addressing Contemporary Racism."

[30] F.M. Moghaddam, "Catastrophic Evolution, Culture, and Diversity Management," *Culture & Psychology* 12 (2006):7415-434.