

2011

# Homeland Security Affairs Journal, Volume VII - 2011, 10 Years After: The 9/11 Essays

Monterey, California. Naval Postgraduate School

HOMELAND SECURITY AFFAIRS

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

SEPTEMBER 2011

# 10 YEARS AFTER: THE 9/11 ESSAYS

# Notes from the Editor

*Homeland Security Affairs (HSA)* is pleased to present this special collection of essays in remembrance of the ten-year anniversary of September 11, 2001. We chose to honor those who lost their lives that tragic day, as well as those whose lives were forever impacted, by reflecting on the homeland security lessons and achievements since 9/11 and the challenges that lie ahead.

The emergence of homeland security forced the United States to revisit, over the past ten years, some of its founding principles and social values in order to address tough security questions. What are the federal government's constitutional responsibilities (and limits) to prevent, prepare for, respond to, and recover from events, versus those of state and local governments? What is the appropriate tradeoff between privacy, civil liberties, and security? In a free market economy, how do we engage businesses as active homeland security partners without heavily regulating industry? What are the definitions of war, a prisoner of war, enemy combatant, terrorist, and criminal and how do we bring these people to justice? What responsibilities do individual citizens have for their own safety and the security of their community? In the age of social networking, what is a community and what holds it together?

In assembling these essays, *HSA* invited the U.S. Department of Homeland Security's three Secretaries – current Secretary Janet Napolitano and former Secretaries Tom Ridge and Michael Chertoff – to reflect on homeland security's past and future. *HSA* also asked Department of Defense Assistant Secretary Paul Stockton (the founding Director of the Naval Postgraduate School's Center for Homeland Defense and Security) to pen an essay from the homeland defense point of view. We are grateful that all four accepted our offer.

In "Progress Toward a More Secure and Resilient Nation," Secretary Napolitano states, "Our experience these past ten years also has made us smarter about the kind of threats we face, and how best to deal with them." Her essay focuses on the strategy of local hometown security as a key to making our communities and the nation safer in the future. Napolitano argues that, " … more and more often, state, local, and tribal law enforcement officers – and their community partners – are best positioned to uncover the first signs of terrorist activity."

Secretary Ridge reminds us, in his essay "Never Any Doubt: A Resilient America," of the dangers of complacency and that "ten years is enough time to know that in the next ten years, the fight will still be with us." He also reminds us that as new threats surface, our tools, policies, and security strategies must continue to evolve. "Because after taking fifty years to win the Cold War, while we emerged as the lone superpower, we were also left with a stockpile of weapons, tactics, and diplomatic relationships that were of little utility in the new security environment."

In "9/11: Before & After," Secretary Chertoff provides an overview of the "new legal architecture for counterterrorism" which required a refashioning of US laws and processes "focused on three elements of the counterterrorism process: intelligence collection, information integration, and terrorist incapacitation." His analysis includes observations on the legal challenges that homeland security presents in preventing attacks, sharing information and bringing terrorists to justice.

Assistant Secretary Stockton's essay, "Ten Years After 9/11: Challenges for the Decade to Come," is an invitation to practitioners and academics to work in partnership with the Department of Defense to build on the far-reaching progress that has already occurred since 9/11. Stockton identifies two areas that require specific attention: defense support to civil authorities and "a little-known but vital realm of preparedness: civil support to defense."

*HSA* also invited faculty from the Naval Postgraduate School's Center for Homeland Defense and Security (publisher of *HSA*) to reflect on areas related to their research and teaching. The ten essays presented here provide insight to a broad array of domestic, international, technological, economic, academic, and social topics that influence how we live and govern. More importantly, the faculty essays help us better understand opportunities for increased security over the next decade.

In "Does Homeland Security Exist Outside The United States?" Nadav Morag contends "Homeland security is a uniquely American concept. It is a product of American geographic isolation and the strong tendency throughout American history to believe that there was a clear divide between events, issues and problems outside US borders and those inside US borders." In answering the question, he examines how other countries have organized their security policies, strategies, and plans.

John Rollins provides a transnational perspective on how the US approaches homeland security. As US economic, political, social, and environmental interests become more global, so have security threats. Rollins believes "the US no longer has the geographic or economic luxury of approaching security issues from a domestic or international perspective. Regardless of where a threat emanates from, today's security professionals need to recognize, respond, and appreciate the near- and long-term transnational implications of risks facing the nation."

One security component that was the focus of much scrutiny following 9/11 is the US intelligence and information sharing system. In "Domestic Intelligence Today: More Security but Less Liberty?" Erik Dahl discusses the reshaping of the US intelligence system over the past ten years and argues, "that even though we as a nation decided not to establish a domestic intelligence organization, we have in recent years done just that…." His overview concludes that while progress has been made, "… the development of a vast domestic intelligence structure since 9/11 has moved the balance [between security and liberty] quite firmly in the direction of more security, but less liberty."

Adaptable, creative, risk-taking, and innovative are words that are used to describe entrepreneurs, especially in the technology sector. They are also words that could be used to describe al-Qaeda during the past ten years. Rodrigo Nieto-Gómez looks at the innovation process that drives the technology sector and how the convergence of technology made 9/11 possible. He also explores the difficulties that technology convergence poses for homeland security professionals. "This retrospective distortion creates a security ecosystem where homeland security practitioners feel pressured to try to 'connect the dots' every time, instead of adapting to an environment of emerging patterns and mutating dots that cannot be connected."

"If there is any advantage to being at war, it is that it creates conditions for exploring new knowledge and gathering disparate players around the flagpole for support." Stan Supinski's essay, "Security Studies: The Homeland Adapts," examines the development of homeland security education since 9/11 and the influences that have helped to shape its evolution. Supinski highlights some key challenges that remain to be addressed in order for homeland security to achieve academic maturity.

The essay by Susan Page Hocevar, Erik Jansen, and Gail Fann Thomas is an example of the maturing of homeland security as an academic area of study. "Inter-Organizational Collaboration: Addressing the Challenge," demonstrates how scholars have become engaged in theoretical work that can provide the basis for new homeland security policies, plans and organizational arrangements. The authors' work focuses on identifying factors that contribute to effective inter-organizational collaboration and the

factors that inhibit collaboration. This is an area that has proven to be one of the most critical challenges for the homeland security community.

Sam Clovis brings education into the homeland security discussion using a different argument. "My intent is to call the attention of my homeland security colleagues to the idea that public education reform must be part of any serious discussion about national or homeland security." Clovis argues, "A better-educated citizenry will be less dependent on government and more independent in times of crisis … will be more attentive to issues and challenges at the state and local level and more engaged at the national level … will cost less in public funding and will contribute more to the public coffers."

In "How Proverbs Damage Homeland Security," Chris Bellavita discusses twelve proverbs – or accepted truths – that have characterized the homeland security narrative. He contends that in the haste to establish a homeland security enterprise and create new policies and strategies, many homeland security proverbs may be inaccurate and "distort the homeland security narrative in a way that inhibits the search for more effective ideas to protect the nation." Bellavita sees an opportunity over the next ten years for academics and strategists "to take another look at the basic assumptions underpinning our homeland security narrative, and identify evidence that supports or refutes the proverbs used to guide strategic direction."

In, "The Post-Tragedy 'Opportunity-bubble' and the Prospect of Citizen Engagement," Fathali Moghaddam and James Breckenridge examine the opportunities that exist for leaders to mobilize the public immediately following a tragic event. "Although great crisis will inevitably invite consideration of many alternatives, leadership must pay special attention to opportunities to engage the public as capable *partners* in their country's response to the crisis – calling upon them as citizens with civic duties, as well as rights."

Future generations of Americans will inevitably view 9/11 as a historical event and time period much like the bombing of Pearl Harbor and the Vietnam War era. However, 9/11 brought about significant changes to the country and American's daily lives. These changes are the subject of James Wirtz's essay, "The Last Days of Summer." "Instead of remaining an 'extraordinary' activity," Wirtz suggests, "homeland security in the United States is becoming part of everyday life because it is slowly but surely improving the ability of federal, state, local and tribal agencies to prevent and respond more quickly and effectively to all sorts of threats and incidents."

Homeland security is still a work in progress and we as a nation are still working through many important issues that touch on who we are as a nation. One of the true benefits of homeland security is that America gains strength through the process of debating answers, solutions, and options. The essays in this special issue provide perspective on the ongoing national homeland security dialogue.

# Progress Toward a More Secure and Resilient Nation

Janet Napolitano

A decade has now passed since the tragic attacks of 9/11, when terrorists exploited our nation's aviation system to kill nearly 3,000 innocent men, women, and children, including citizens of more than 90 countries.

Today, as we approach the tenth anniversary of 9/11, there is no question that America is stronger and more secure than we were a decade ago. We have bounced back from the worst attacks ever on our soil, and have made progress on every front to protect ourselves.

In late July, I released a report outlining the significant progress the Department of Homeland Security (DHS) and our many partners have made in fulfilling specific recommendations by the 9/11 Commission to make our nation stronger, safer, and more resilient.[1]

The report details the great strides we have made over the last decade to secure our nation against a terrorist attack or other disaster, to protect our critical infrastructure and cyber networks, and to engage a broader range of Americans in the shared responsibility for our security.

Our experience these past ten years also has made us smarter about the kind of threats we face, and how best to deal with them. We have used this knowledge to make our nation and communities more resilient, not only to terrorist attacks, but also to threats and disasters of all kinds, while safeguarding the fundamental rights of all Americans.

But there should be no doubt: serious threats from terrorism remain. Terrorism did not begin on 9/11, nor did it end with the death of Osama bin Laden. Today's terrorist threats are real and rapidly evolving. They demand our constant vigilance. And they demand our willingness to learn and adapt.

While defending against this evolving threat is the founding mission of DHS, no federal agency – or any part of government – can, by itself, deliver security. Perhaps more than at any point in our nation's history, we share in this responsibility. And this has broad implications for how we will continue to work with our partners to keep our country safe and secure.

## EVOLVING THREATS

The terrorist threats facing the United States have evolved significantly over the last decade, and continue to evolve. In addition to the direct threats from al Qaeda, we also face growing threats from other foreign-based terrorist groups that are inspired by al Qaeda's ideology, but that have few operational connections to the core al Qaeda group.

We face a threat environment where violent extremism is neither constrained by international borders nor limited to any single ideology. Indeed, one of the most striking elements of today's threat picture is that plots to attack America increasingly involve American residents and citizens, including individuals who may be in the United States and are prepared to carry out terrorist attacks with little or no warning.

Over the past two years, we have seen al Qaeda-inspired terrorist groups seek to recruit individuals who are either Westerners, or have connections to the West, and who are unknown to authorities. The increasingly savvy use of the Internet, mainstream and social media, and information technology by these groups adds an additional layer of complexity.

The fact that these new kinds of threats can come from any direction, and with little or no warning, changes much of our thinking about terrorism prevention. Of course, we need a strong military and top-notch intelligence to fight terrorism abroad; the operation that led to Osama bin Laden's death clearly demonstrates this.

This essential international dimension to "homeland" security ranges from aviation and supply chain security, to information sharing about the latest terrorist travel routes, tactics, and technologies. Indeed, the importance of international partnerships is

why DHS has a significant international presence – in seventy-five different countries, the third largest international footprint of any US government agency.

We also, however, face threats from within our own borders. As a result, our state, local, and tribal law enforcement officers, our first responders, and individual citizens are often the first to notice signs of potential terrorist activity in their communities. And that means we need every part of our society to be cognizant of the kinds of threats that exist, and knowledgeable about common sense steps to counter them.

## BUILDING THE TWENTY-FIRST CENTURY HOMELAND SECURITY ENTERPRISE

For the past several years, DHS and our partners have worked to develop and strengthen the homeland security enterprise to better mitigate and defend against dynamic threats, minimize risks, and maximize the ability to respond to and recover from attacks and disasters of all kinds.

This approach is based on the simple but powerful premise that homeland security begins with *hometown* security.[2] We are all now stakeholders in the effort to keep our families and communities, our businesses, our social networks, and our places of meeting and worship secure and resilient.

These insights have driven our effort to build critical features that did not exist on 9/11, and which address key recommendations of the 9/11 Commission. For example, we understand the critical importance of analyzing threat information at the local level, and then sharing that information wherever it may be relevant. That is why today we have seventy-two recognized state and major-urban-area fusion centers throughout the country.

These fusion centers serve as focal points where information about threats can be gathered, analyzed, and shared among federal, state, local, tribal, territorial, and private sector partners. Fusion centers also support and interact regularly with FBI-led Joint Terrorism Task Forces (JTTF), which coordinate resources and expertise from across the federal government to investigate terrorism cases.

We also have greatly expanded and enhanced the Nationwide Suspicious Activity Reporting Initiative, which trains state and local law enforcement to recognize behaviors and indicators related to terrorism, crime, and other threats, and standardizes how those observations are documented, analyzed, and shared with the FBI, other law enforcement, and communities throughout the country.

We launched the new National Terrorism Advisory System in April 2011, replacing the outdated color-coded system of alerts. This new system delivers timely, detailed information about terrorist threats to the public, government agencies, first responders, transportation hubs, and the private sector.

We are expanding the "If You See Something, Say Something™" campaign. It is a simple and effective program, first implemented by New York City's Metropolitan Transportation Authority, to raise public awareness of indicators of terrorism, crime, and other threats, and to emphasize the importance of reporting suspicious activity to the proper law enforcement authorities – from federal buildings to transit systems to major sports and entertainment venues.

In addition to these measures, we have taken very significant steps to facilitate the exchange of information about terrorists and criminals with international partners; strengthen airline passenger pre-screening; enhance screening for explosives; protect cyber networks and critical infrastructure; bolster security of our air, land, and sea borders and identification documents; and ensure robust privacy and civil liberties safeguards.

Additionally, to help counter the threat of violent extremism in our communities, DHS has trained more than 46,000 front-line law enforcement professionals, and has worked with hundreds of communities and local organizations over the last eighteen months to implement community-oriented policing strategies that have been successful in other crime-reduction efforts, such as combating gang violence in places like Los Angeles.[3]

## HOMETOWN SECURITY: A ROLE FOR ALL OF US

The elements of this new homeland security enterprise are designed to support and complement one another, and to protect privacy, civil rights, and civil liberties. They reflect the emerging reality that more and more often, state, local, and tribal law enforcement officers – and their community partners – are best positioned to uncover the first signs of terrorist activity. Therefore, DHS has made a priority of getting information, tools, and resources *out* of Washington, DC, and *into* the hands of those on the front lines of keeping their communities safe.

And growing evidence shows the tremendous role the public can play in homeland security. According to one recent outside analysis, from 1999 through 2009 a total of eighty-six terrorist plots against Americans were foiled. These were motivated by a range of ideologies, with those linked to al Qaeda or their affiliates only representing about half.

What is most critical to note, and which often does not get the attention it deserves, is that information that originated with the public is credited with stopping almost one third of these plots. When you add federal, state, local, and tribal law enforcement, more than 80 percent of foiled plots came from a combination of old fashioned vigilance and cooperation, information sharing, community-oriented policing, and citizen awareness.[4]

In many ways, this is not really a new story. America has a long history of communities playing an active role in their own security, and of responding to new threats by adopting new precautions. For decades, we looked to civil defense and neighborhood watch programs as elements of our own protection. And in the early years of the Cold War, Americans all knew where the closest fallout shelter was, and we kept children indoors when polio outbreaks were the biggest threat to public health.

The threats we have seen emerging over the last few years require us to be nimble and forward leaning. We ought to be alert, not alarmed, and that requires us to engage in regular discussion about preparedness and response to the threats a particular community may face. Building secure hometowns across the country requires each of us as individuals – and also as parents, business owners, or community leaders – to play a role.

Indeed, all of us can learn more about the signs or indicators of potential criminal or terrorist planning, and say something to the proper authorities if we see something out of place. It was a street vendor who tipped off police to the Times Square bombing attempt in 2010. In January 2011, alert city workers in Spokane, Washington reported a suspicious backpack and, in doing so, thwarted what almost certainly would have been a deadly bombing along the Martin Luther King Day parade route.

We can practice safe cyber habits whenever we are online, and also share and teach them to our children. This is especially relevant in the wake of several major breaches and phishing attacks that have targeted consumers and the public.

And we can all take the basic steps to be ready for an emergency, including making a plan for reuniting with family in a crisis. We need only look at the deadly tornadoes, and the flooding and wildfires many communities have endured this year to understand the value of preparedness.

Today, hometowns across the country are working together, building a strong foundation for a secure and resilient homeland. Because of these efforts, and those of our men and women on the front lines and our dedicated counterterrorism and emergency management professionals, we are stronger than we were on 9/11.

We will never be able to seal our country under a glass dome to prevent future terrorist attacks or disasters. But we can continue to do everything possible to minimize the possibility that such an attack will succeed, and maximize our ability to respond effectively. Protecting the nation is a shared responsibility and we all have an important role to play.

## ABOUT THE AUTHOR

***Secretary Janet Napolitano*** *has led the US Department of Homeland Security since*

*2009. Prior to this appointment, Secretary Napolitano was serving her second term as governor of Arizona and was recognized as a national leader in homeland security, border security, and immigration.*

[1] Department of Homeland Security, *Implementing 9/11 Commission Recommendations, Progress Report 2011* (Washington, D.C., 2011), http://www.dhs.gov/files/publications/implementing-9-11-commission-recommendations.shtm.

[2] See description of "Hometown Security" concept at http://www.dhs.gov/files/programs/hometown.shtm.

[3] See DHS factsheet, "How DHS is Countering Violent Extremism," http://blog.dhs.gov/2011/08/how-dhs-is-countering-violent-extremism.html.

[4] Kevin Strom, et al., *Building on Clues: Examining Successes and Failures in Detecting U.S. Terrorist Plots, 1999-2009* (Institute for Homeland Security Solutions, 2010), www.ihssnc.org/portals/0/Building_on_Clues_Strom.pdf.

# 9/11: Before and After

Michael Chertoff

## WHERE WERE WE?

Until September 11, 2001, the United States had limited experience with terrorist attacks on our own soil, and only intermittent experience with attacks overseas. During the 1970s and 80s, airline hijackings and overseas bombings were the focus of most terrorist activity. In 1993, violent Islamist extremists bombed the World Trade Center, causing six deaths and more than a thousand injuries, but failing to significantly damage the structures themselves. During the next decade, several domestic focused Islamist terrorist plots were foiled at the planning stage; however, additional attacks were conducted overseas, by operatives of Hezbollah killing US service personnel in 1996 at the Khobar Towers complex in Saudi Arabia, by al Qaeda bombing of US embassies in East Africa in 1998, and the attack on the USS Cole near Yemen in 2000. The most deadly attack domestically during the 1990s was the Oklahoma City bombing, carried out by Timothy McVeigh, an anti-government extremist.

All of these attacks and attempts were addressed through the existing criminal justice system. Under that legal architecture, the Foreign Intelligence Surveillance Act and Title III of the Omnibus Crime Control and Safe Streets Act, as well as a host of other statutes and regulations, governed domestic intelligence collection. Exchange of information collected by foreign and domestic agencies was determined by a strict set of rules that was (perhaps somewhat incorrectly) interpreted as forbidding pure "intelligence" information from being collected for law enforcement purposes, and – conversely – made it difficult to share criminal justice-derived information with other agencies. When terrorists were apprehended either in the United States or abroad, they were accorded the treatment of any other criminal defendant, including receiving warnings about the right to silence, and a full-blown criminal jury trial.

The attacks of September 11, 2001 and the consequent retrospective investigations – such as the *9/11 Commission Report* – exposed the inadequacy of this architecture in addressing and thwarting further attacks. The inability to coordinate information collection and integration among various agencies led to the failure to identify patterns of behavior that might have provided warning of attack. Rules designed to govern electronic surveillance in the days of fixed land-line communications were difficult to apply to communications media such as mobile, disposable telephones or voice over internet communications. And even when terrorists were identified and apprehended, difficulties in providing evidence admissible in traditional courtroom proceedings left authorities with few avenues to detain or incapacitate them.

For the fundamental lesson was this: a counterterrorism architecture that is founded on criminal justice principles is fundamentally oriented to punishing those who have plotted or carried out attacks. But with the danger to innocent life posed by modern terrorism, prevention and not punishment becomes the critical driver for counterterrorism. And that required refashioning our legal tool set.

This refashioning focused on three elements of the counterterrorism process: intelligence collection, information integration, and terrorist incapacitation. The first refers to how we can better collect information in real time within the context of modern global communication, travel, and finance. The second focuses on how we can better combine and integrate that information once collected. And the third addresses how we can act on that information to incapacitate terrorists at the earliest stage before they can advance their operations.

## WHERE ARE WE?

### Intelligence Collection

In the wake of the attacks of September 11, the Bush Administration worked with Congress to update some of the rules governing interception of electronic communications and to streamline information requests. The USA PATRIOT Act, passed overwhelmingly, updated electronic surveillance rules to allow warrants to intercept individuals even when they frequently changed phones, and to grant access to Internet communications on the same basic terms as applicable to traditional telephone communications.

Somewhat more controversial was the implementation of regulations designed to collect routine traveler and financial information. During the past decade, the United States government implemented US VISIT, a program that captures fingerprints from all foreign travelers entering the United States. The government also exerted its right under the Chicago Aviation Convention to collect from the airlines commercial travel data relating to inbound travelers. This kind of data proved crucial in identifying high-risk travelers who are connected with known or suspected terrorists. Based on these "red flags," aviation and border security officials can now take a closer look at these travelers from among the millions who cross our borders each day.

The legality of these efforts has never been seriously challenged under US constitutional or statutory law. European data protection officials, however, resisted the use of commercial data on the grounds that it invaded the privacy of European travelers under European laws. The clash between international law giving the US the right to vet all incoming air travelers and European law seeking to cloak the privacy of those travelers threatened to cause disruption in the air industry. Fortunately this was averted for the time being through a US-European Union agreement that set an acceptable framework to accommodate security and privacy concerns.

A similar legal impasse arose from US government efforts to collect information from the so-called SWIFT system, an interbank network that exchanges global financial transactions every day. Government collection of this data under legal process allowed quick identification of suspicious movement of funds that might be used to support terrorist operations. This was precisely the type of smart intelligence collection advocated by the 9/11 Commission. In 2006, however, the *New York Times* chose to reveal the existence of the SWIFT collection program, thereby not only giving warning to terrorist financiers but provoking another privacy dispute with European authorities. Ironically, as even the *Times* acknowledged, the legal underpinnings of the SWIFT program were not open to serious question.

Perhaps the most controversial change in collection architecture arose from a dispute over the legality of an electronic surveillance program directed at intercepting certain international communications. The conflict was resolved by the passage of the FISA Act Amendments, which provided the US government with additional procedures and specific limitations to collecting information and intelligence from foreign terrorists and their affiliates located outside of the United States.

### Information Integration

Perhaps the most well known finding of the 9/11 Commission was the missed warning signs that arose from a "failure to connect the dots" of individual intelligence items. This failure arose from institutional and cultural obstacles within the intelligence agencies, but also from a legal approach to the relationship between law enforcement and intelligence collection that built a substantial barrier to information sharing. The PATRIOT Act amended the law to dramatically lower the legal barrier to sharing, and to create a presumption of sharing rather than an inhibition against sharing. Ironically, a later court decision by the FISA Court of Review established that the previous interpretation of the FISA restriction on information sharing was unduly stringent, and reflected an overly cautious approach to the legal requirement.

Little legal controversy has arisen in the United States over information sharing,

although cultural barriers within the agencies remain, most recently demonstrated by the failure to integrate warning information of the would-be 2009 Christmas bomber, Umar Farouk Abdulmutallab. European views on information sharing remain dramatically different, however, with a strong bias against allowing integration of information from individual databases. For this reason, American and European officials have engaged in lengthy negotiations over the years about how willing the latter are to share biographic and biometric data even about individuals who are known criminals or terrorists. This information is not simply beneficial to the United States. Using known information about individuals, such as travel information, is an essential tool for detecting potentially dangerous individuals associated with terrorism and transnational criminal activity. Despite the differences between the US and European officials, information sharing agreements involving travel information and methods of payment exist today and incorporate appropriate privacy protections for individual personal information. As a result, the US has been able to enforce our border and immigration laws by disrupting, denying and dismantling terrorist travel as well as human trafficking and drug smuggling networks seeking to enter our nation.

## Incapacitation

The most controversial elements of the new legal architecture for counterterrorism arise from the question of how to incapacitate someone apprehended here or overseas as a terrorist.

For the first several years after the September 11 attacks, Congress took no action to address the issue of incapacitation, as it had done with the issues of intelligence collection and sharing through the PATRIOT Act. The question of detention and punishment evolved within the Executive Branch. Alongside the customary criminal justice architecture, the Bush Administration established a military commission structure, drawing upon the historical model of military commissions that were impaneled during the Civil War and the Second World War and its aftermath. Military commissions – applicable only to non-US citizens – were designed to mete our punishment for the laws of war in the same way that the civilian justice system had punished terrorists for violating civilian laws.

Neither the courts nor the commissions, however, had a clear mechanism for detaining operatives who were terrorist threats before they were charged with a crime and punished. Such detention was available for those in the civilian system after charges were leveled, but that process required willingness to proceed to a trial in relatively short order. Especially for those caught on the battlefield overseas, where admissible evidence might be difficult to assemble, beginning the criminal justice process was impractical. Moreover, civilian arrest and charging triggered the right to silence, which frustrates the process of questioning for intelligence gathering, which was a primary objective when capturing terrorists.

Under these circumstances, the Bush Administration asserted the right to detain and hold enemy belligerents without trial or even military commission in line with the traditional authority of the military to hold prisoners in wartime. What was unclear in the initial stages of the conflict in Afghanistan was exactly what procedural mechanisms would be made available to assure those held were, in fact, affiliated with terrorists, and how this would mesh with various procedures mandated under the Geneva Convention.

Over the subsequent ten years, the evolution of the detention and incapacitation process has been ad hoc, if not at times chaotic. Contrary to conventional wisdom – indeed, conventional myth – the Bush Administration did not simply push all suspected terrorists into the military system. Generally, the Administration charged Americans and those captured on American soil in the civilian criminal justice system. Only two individuals apprehended in the United States were detained as military belligerents; each of these was eventually charged and convicted in US civilian courts. On the other hand, non-Americans apprehended overseas were generally detained in military facilities (including Guantanamo), and some began to be charged or processed through the military commission system. Thus, the Bush

Administration in practical terms deployed both civilian and military legal systems to handle issues of detention, with a rough presumption that those apprehended in the US and American citizens would be addressed through the former, and those non-citizens captured overseas would be addressed through the latter.

What was far less settled was the review to be afforded to those non-citizens held in military custody. Congress' failure to establish a process, and the Defense Department's restrictive approach to detainee rights, provoked ever more vigorous judicial review and eventually a significant overturning of parts of that system. While the Supreme Court affirmed the fundamental right of the president to detain and hold enemy belligerents during hostilities, the Court eventually granted at least detainees in Guantanamo some legal latitude to challenge the bases for their confinement by filing habeas corpus petitions in federal court. When Congress finally engaged in 2007 through the Military Commissions Act, the Congressional effort to limit this review was struck down by the Court. As a result, the exact scope of review for detainees in Guantanamo – let alone elsewhere – remains murky. A recent survey of individual cases suggests that the government prevails in the vast majority of challenges to date.

The advent of the Obama Administration was widely expected to herald a sea change in the approach to detention. After the president on his first day declared his intent to close Guantanamo, advocacy groups eagerly anticipated a return to the pre-9/11 legal architecture for detention, operating exclusively through the criminal justice system. Early returns suggested this change would occur, and the announced decision by Attorney General Eric Holder to try Khalid Sheikh Mohammed and other 9/11 coconspirators in federal court in New York was the apogee of this movement. But strong resistance – and perhaps a strong dose of reality triggered by the near success of the 2009 Christmas Day bomber – began to reverse direction. Over the last year, the Obama Administration has indicated that the 9/11 conspirators will be tried in military commissions, and while other terrorists have been tried in civilian courts, that mixed approach is largely consistent with the pragmatic approach of the Bush Administration. Perhaps most notable as a symbolic reversal, however, is the continued vitality of terrorist detention at Guantanamo, a practice that is likely to continue in the future given strong Congressional prohibitions against bringing Guantanamo terrorist detainees into the United States.

However inelegantly evolved, the current legal structure for incapacitating terrorists seems a rough compromise between security and civil liberties concerns, and is distinguished by a remarkable degree of continuity between the Bush and Obama Administrations. The executive branch's authority to detain enemy belligerents has been affirmed by both presidents, and by the Supreme Court. Some court review is afforded those held in the United States and in Guantanamo, but the rules of that review remain indistinct and uncertain. Military commissions are functioning under somewhat more generous rules for defendants, but no case has yet worked itself through the process. And legal adviser Harold Koh – who as dean of Yale Law School was an outspoken critic of the Bush Administration counterterrorism policy on civil liberties grounds – has recently issued a full throated defense of the president's right to order the killing of terrorists overseas.

## WHERE SHOULD WE BE?

Although the legal architecture governing intelligence collection has adapted to new technologies in the last ten years, new challenges emerge. As cyber crime and "hacktivism" increase in frequency and consequence, the government's ability to monitor in real time for malicious code and similar cyber hacking tools is constrained by real uncertainty about the legal effects of the rules for electronic communications surveillance. If the malicious code is buried in the flow of Internet packets that delivers the stream of communication, does that mean those packets can only be scanned under the relatively stringent rules governing interception of communications? Or does the fact that the scanning is undertaken at the packet level mean surveillance rules should

not apply, since malicious computer instructions rather than intelligible communications are being sought? Sorting this legal conundrum, with far-reaching implications for both security and freedom of the Internet, is one of the overpowering legal challenges confronting us today.

By contrast, information sharing is on firmer legal footing in the United States. Here the continuing effort will be to resolve ongoing disputes with the European Union, which has reopened the controversy over American use of inbound airline passenger commercial data.

Finally, and most unsettled, are the legal rules that will govern detention of terrorist suspects. The current structure, fashioned case by case though the courts, leaves many questions unresolved. Issues of burdens of proof, what kind of evidence is admissible and what proof is sufficient, await definitive answers. Only Congress has the institutional capability and authority to fashion a comprehensive procedure for reviewing these cases that balance practical security concerns and fundamental fairness. Unless the administration and the legislators find the time and will to address these issues, uncertainties in our legal framework for detention will result in a system that is less than optimal from both security and liberty standpoints.

## ABOUT THE AUTHOR

***Michael Chertoff*** *was secretary of the US Department of Homeland Security from 2004 to 2009 and is presently co-founder and managing principal of The Chertoff Group and a senior of counsel at the law firm of Covington & Burling, LLP.*

# Never Any Doubt: A Resilient America

Tom Ridge

On September 10, 2001, most Americans were feeling good about their place in the world as a strong, unchallenged nation with a strong, expanding economy.

The ugliness and brutality of terrorism was viewed as an unseemly part of the modern world. With the exception of Oklahoma City and the 1993 World Trade Center bombing, such incidents occurred "over there" – beyond our borders. We were a superpower, enjoying a standard of living unequalled in the world, with friends to the north and south and oceans to the east and west. We were safe, secure, and many concluded, immune from such horrific acts.

It was absolutely unimaginable then that a small group of individuals, with limited funding, regardless of the intensity of their hatred, could conceive and execute an attack that could result in a catastrophic loss of life and economic devastation of hundreds of billions of dollars.

The attacks of 9/11 left the country stunned and in grief, but as I look back over the last ten years, it is abundantly clear that America was, is, and always will be an undeniably resilient nation.

We went from the bent knee of prayer to a battle plan, and have become a better, stronger nation for everything we have achieved.

In a decade's time, we strengthened our intelligence assets and partnered with allies and friends. We captured and killed terrorists and destroyed safe havens in Afghanistan and around the globe.

We undertook one of the biggest change management challenges of our time with the reorganization of the federal government. We stood up a new department, Homeland Security, combining twenty-plus agencies and 180,000-plus people. Federal, state and local authorities re-positioned as the country embraced an emotionally charged and strategically driven national mission. We did so with an eye toward the safekeeping of our civil liberties, our Constitution and the integrity of the American brand.

We improved preparedness and response capabilities and established layers of security throughout our aviation system. We embedded new technologies at our borders and deployed fingerprint-based screening and radiation portal monitors at our ports of entry. In light of the new security threat, we were compelled to think and act anew, and we did.

With public and private sector leadership and investment, we are more secure. But we remain a target nonetheless.

What we know now more than ever is that over the course of ten years, the threat remains strong and continues to change. We have thwarted some attacks, but we have also been fortunate that a few others have simply failed.

As we close one vulnerability, we should anticipate that terrorists will adapt and seek out another. They are patient, strategic actors and before them lays a map of the world and a centuries-old ideology of hate and intolerance that we resoundingly reject in the Western world.

This is a multi-generational threat, and war. And for that reason, we must always view security as an ongoing process, not an endpoint. A deliberative process, not a breathless reaction to all conceivable threats, is required at all times.

In that regard, it is helpful to view the threat of terrorism in the context of another threat we faced in the latter half of the 20th century – when two super powers armed with thousands of nuclear weapons had a very serious staring contest.

It was a time during which we built the strongest economy in the world, advanced the cause of civil and human rights at home and abroad, and demonstrated that our political and economic system could deal with that very real threat to our way of life while our citizens continued to enjoy and to promote the freedoms that are at America's very foundation.

We should have equal confidence in our ability to do the same in the twenty-first century.

But also, we must be committed to making sure that we have all of the tools and resources we need at our disposal. Because after taking fifty years to win the Cold War, while we emerged as the lone superpower, we were also left with a stockpile of weapons, tactics, and diplomatic relationships that were of little utility in the new security environment.

Adapting to this threat environment takes commitment. It takes collaboration. It takes a willingness to recognize and overcome what might be the single greatest threat in the fight again terrorism – one that affects all of our actions by not affecting action at all. Complacency.

When reporters ask me what worries me most, they expect me to say a nuclear event or a bio-agent. Those potential scenarios worry me, yes. But the important thing in my mind is that we continue to see the world through a 9/11 lens. More so, a 9/12 lens.

On September 12, 2001 we were grieving, but we had a sense of unity and an aggressive state of determination – that the perpetrators of the attack would come to justice and that we would take every step, every measure, every opportunity to make this country and its people more secure.

Every day, we have learned a little more. Every day, more people are working together to find security solutions and identify vulnerabilities. But every day, we get a little farther away from the tragedy.

So we have to be willing to look over our shoulders, and let the images and feelings of an unspeakable and intolerable tragedy motivate us. We also must be mindful that terrorists do not rest, so neither can we. We cannot underestimate the appeal of their belief system and their willingness to be patient in bringing the broader world to accept that belief system. We have wristwatches, but they have time. That means that in spite of the significant progress we have made, much work remains to be done.

We have strengthened information sharing in country and among allies and friends, but we still saw an attempted Christmas Day bomber come very close to his goals due to overt and repeated information not being shared. This began with the bomber's own father expressing concern to authorities that his son had been radicalized. We need to create a culture of intelligence sharing where everyone feels empowered to hit the send button, to share more, not less.

We have bolstered communication technologies, but after hearing of the heartbreaking difficulty first responders on 9/11 had in speaking to each other with outdated equipment and disparate channel frequencies, an interoperable broadband communications system remains undelivered. If the tragedy of 9/11, the specific recommendations of the 9/11 Commission and the sustained pleas of police, firemen, and emergency service professionals cannot generate federal support for such a network, then what will it take?

We have instituted an entry system to validate who comes into the country, but have not created an exit system that ensures these same visitors leave and do not exploit an as-yet unfinished system. The technology exists but Congress has not kept pace. It is likely therefore that we have people among us who have overstayed their visas. Where are they now and what are they doing? Where is the sense of urgency needed to address this?

It would be easy to cite all the vulnerabilities we have yet to address and the 9/11 recommendations we have yet to meet. But as I know, Secretary Chertoff knows, and Secretary Napolitano knows, achieving these and other goals requires the navigation of a federal system where urgency does not come easily when politics, budgets, and bureaucracy are involved.

As citizens, we are entitled to have expectations of our government relative to our security. What we cannot expect is that the government can create a fail-safe, risk-free environment. That perhaps has been a notion that makes many people uncomfortable. But ten years on from 9/11, we simply must be prepared to accept the fact that no matter how hard we try, another attack is likely.

Trying to determine what scenarios pose a threat to the United States is like trying to find a needle in a haystack. The solution, as we have found out, is to remove much of the haystack from the needle. But that does not mean that we must treat every person as a

potential terrorist or that every possible scenario must be explored.

Risks are ever present and cannot be eliminated. They must be managed. Priorities have to be set and trade offs must be made. That means we have to balance how much security is enough with our fiscal realities.

Do we spend billions defending commercial airlines against shoulder-fired missiles, or do we invest in nuclear detection technology to inspect the 20 million cargo containers shipped to our ports? Do we appropriate the money to complete the US-VISIT system or do we give states more money for equipment and training? Do we choose among adding more layers of security at chemical sites, addressing a different security risk in mass transit, or channeling that investment to a national health or energy security priority?

The needs and wants are limitless. Resources are not. So we must manage the risk carefully and judiciously. That responsibility is great and complex. And ten years later, it doesn't get any easier.

One of the biggest news stories of the year, one that capped a decade of emotion, was the killing of Osama Bin Laden. What we immediately understood, even long before it happened, was that despite the fact he was brought to justice, his death didn't mean much to the threat we continue to face. As Benazir Bhutto once advised: "You can imprison a man but not an idea. You can exile a man, but not an idea. You can kill a man, but not an idea." Bin Laden is gone, but the ideology lives on in others.

The images of home videos of bin Laden demonstrated that he was just one guy. Just one man – sitting in his easy chair, flipping the remote control, worrying about the gray hairs in his beard, frustrated when he'd flub the lines of his own scripts – those videos of warning we used to see. He was just a guy. Not much of a warrior. No super-human mystique about him.

But it only took that one guy and a few believers. Likewise, it only took one time, one difficult September morning, for America to understand that the world has changed and we must change with it.

Ten years is not a lot of time, but it was enough time to begin. It was enough time to commit ourselves to a new fight and underscore an America we have long since known. Ten years is enough time to know that in the next ten years, the fight will still be with us. It will go on. But we will go on with it, as a stronger and more secure country, as the resilient and freedom-loving people we have always been, and as a nation that will always remember those we lost one September day.

## ABOUT THE AUTHOR

***Tom Ridge*** *served as the 43rd governor of Pennsylvania before becoming the nation's first assistant to the president for homeland security in 2001 and, in January 2003, the first secretary of the newly created US Department of Homeland Security. Ridge is the founder and CEO of Ridge Global, an international security and risk management firm, headquartered in Washington, DC.*

# Ten Years After 9/11: Challenges for the Decade to Come

Paul Stockton

One of the best ways to honor those who perished on 9/11 is to rededicate ourselves to finding, and fixing, the gaps in preparedness that still confront our nation. Over the past decade, the Department of Defense (DoD) has greatly improved its ability to support the federal departments and agencies that lead US preparedness against terrorism and natural hazards. Yet, significant challenges remain in our ability to provide such defense support to civil authorities. Still greater shortfalls are emerging in a little-known but vital realm of preparedness: civil support to defense.

This essay begins by examining two gaps in DoD support to civil authorities. The first is DoD support to the Federal Emergency Management Agency (FEMA) for catastrophes more severe than Hurricane Katrina. The second gap is that of defense support to the civilian law enforcement departments and agencies that lead the prevention of terrorism in the United States.

I will then flip the familiar construct of defense support to civil authorities upside down, and explore the crucial roles that civilian agencies – and the private sector – can play to support the Department of Defense. I will argue that DoD is increasingly dependent on domestic infrastructure beyond the department's control, and that this infrastructure may be at growing risk of attack. I will also argue that only through new forms of civil-military cooperation can DoD ensure its ability to execute its core missions, at home and abroad. I hope that the shortfalls highlighted below will become part of the research agenda for graduate students and faculty, and a focus for the community of practice in homeland defense and security that is one of the greatest achievements of the past decade.

## DEFENSE SUPPORT TO CIVIL AUTHORITIES

### Complex Catastrophes

The Department of Defense is well prepared to support the Department of Homeland Security (DHS), FEMA and other federal departments and agencies in responding to "normal disasters" – that is, hurricanes, wildfires, and other events of typical magnitude, that most often spur governors to request federal assistance or prompt the federal government to position resources in anticipation of need. Of course, there are opportunities to improve our preparedness for normal disasters. Thanks to the leadership of the state governors, we are making progress across a broad range of issues in defense support for disaster response, especially in strengthening unity of effort between state and federal military response forces.[1]

The National Level Exercise 2011 (NLE 11) highlighted the need to strengthen our preparedness for events worse than normal disasters – disasters even more severe than Hurricane Katrina. NLE 11 was based on a scenario that began with a magnitude 7.7 earthquake along the New Madrid fault. An earthquake of that magnitude occurred in 1812; a similar one could strike at any time. The destructive effects could be far greater than two centuries ago, however. The Mid-America Earthquake Center notes that if such an event were to take place today, "the consequences would be much more significant and damage would be much more severe in terms of injuries and fatalities, structural damage, and economic and social impacts."[2] Indeed, the resulting devastation could so exceed the damage in normal disasters that these extraordinary events should be classified separately as "complex catastrophes."

Complex catastrophes differ from normal disasters in two ways. First, the scale of destruction is vastly greater. Katrina resulted

in 8,800 casualties, primarily (though not exclusively) in Louisiana and Mississippi. An earthquake like the one described in NLE 11 could inflict up to ten times as many casualties across eight states and four multi-state FEMA regions.[3] Localities and states near the New Madrid fault have made remarkable progress in improving preparedness for such an event. Nevertheless, the magnitude of the destruction and need for life-saving capabilities would almost certainly prompt governors to ask FEMA for large-scale federal assistance – with FEMA, in turn, asking DoD for unprecedented levels of defense support. Responding to those requests in a timely manner could create complex challenges for the department in sourcing the requested capabilities, transporting them, and then providing for their reception, staging, onward movement, and integration in a severely disrupted environment.

Second, as NLE 11 demonstrated, complex catastrophes may create cascading, region-wide failures of critical infrastructure, starting with the disruption of the commercial electric power grid. A 7.7 New Madrid earthquake would produce vastly greater damage to the grid than occurred in Hurricane Katrina or any other disaster in US history.[4] The net effect of physical damage to high-voltage transformers and other hard-to-replace components could be lengthy power outages across numerous states, with the potential for post-quake rolling blackouts also occurring in Chicago, the Eastern United States, and elsewhere.[5]

This loss of power could create cascading effects on communications and other critical infrastructure. From a public safety perspective, the most immediate concern might be the impact on municipal water systems, which in Memphis and most other cities depend on commercial electric power to operate. The loss of power could jeopardize the availability of drinking water from those systems. Transportation infrastructure could be degraded as well; gas and diesel fuel pumps, for example, depend on electric power to function. While many hospitals and other facilities critical to disaster response efforts have backup diesel-powered generators, we anticipate few will have sufficient fuel on hand to offset power outage lasting weeks to months, and that companies responsible for resupplying them could face a radical mismatch between supply and demand.

DoD is working today with FEMA and the DHS National Protection and Programs Directorate (NPPD), as well as other federal departments and agencies, to assess the lessons learned from NLE 11 and better prepare for complex catastrophes. Doing so will require innovative thinking on how to strengthen our preparedness. Consensus will be easy to reach on key foundations of our drive for greater preparedness. For example, in both complex catastrophes and normal disasters, the Post-Katrina Emergency Reform Act of 2006 (and the leadership role it assigns to the administrator of FEMA) will continue to govern response authorities and supported/supporting relationships. Other challenges of preparing for complex catastrophes could prove more difficult, however, starting with the need for better analysis of how cascading infrastructure failure could both increase requests for federal assistance, and make that assistance much more difficult to provide.

## Defense Support to Law Enforcement

The most critical shortfalls revealed by 9/11 were not in disaster response, but rather in terrorism prevention. Over the past decade, the Department of Justice (DOJ), the Federal Bureau of Investigation (FBI), the Department of Homeland Security (DHS), and other federal, state, local, and tribal law enforcement agencies have made great strides in strengthening US prevention capabilities.[6] The efforts of DoD and its partners abroad have also weakened al-Qaeda. As President Obama notes, "we have put al-Qaeda on the path to defeat."[7] The president also notes, however, that "we continue to face a significant terrorist threat from al-Qaeda, its affiliates, and its adherents."[8] This threat includes efforts by al-Qaeda to inspire individuals within the United States to conduct their own attacks, and to disseminate plans on how to construct improvised explosive devices (IED).[9]

Of course, the primary DoD contribution to preventing terrorism against the United

States has been (and will remain) our operations abroad to disrupt, dismantle, and ultimately defeat al-Qaeda and its affiliates. The department also takes very seriously its responsibilities for homeland defense. In addition, within the United States, DoD supports – within the constraints set by the Constitution and other US law – its lead federal partners in their law enforcement efforts when they request prevention-related assistance. Those requests may grow in the future. For example, if terrorists were to launch a campaign using IED in the United States, DoD has technical expertise from dealing with such threats abroad that – consistent with US law – could be used to help meet requests for assistance by the FBI, DHS and other law enforcement agencies that would lead domestic counter-IED efforts.

President Obama has taken decisive steps to integrate US government prevention efforts more effectively. The June 2011 *National Strategy for Counterterrorism* lays out the overarching goals, and the steps to achieve them, that the US government will follow.[10] Presidential Policy Directive 8 (PPD-8), National Preparedness, further specifies how the United States will organize to meet the challenges of terrorism and other key hazards at home. Among other features, PPD-8 provides for the creation of a national preparedness system that will include a series of integrated national planning frameworks, covering prevention, protection, mitigation, response, and recovery. The frameworks – including prevention – will be supported by an interagency operational plan that provides a detailed concept of operations; a description of critical tasks and responsibilities; detailed resource, personnel, and sourcing requirements; and specific provisions for the rapid integration of resources and personnel. PPD-8 also requires the DoD and other federal departments and agencies to develop department-level operational plans, as needed, to support the interagency operations plans.[11]

The nation has long needed a national prevention framework. Now, thanks to PPD-8, we will soon have one. PPD-8 sets out stringent deadlines for the development of a national preparedness goal and the supporting preparedness system. Building out the prevention framework and the follow-on detailed operational plan will also require innovative thinking and new approaches to strengthen collaboration, across the federal government and among federal, state, local, tribal, and private sector entities.[12]

## CIVIL SUPPORT TO DEFENSE

The concept of defense support to civil authorities is widely understood. Less familiar but increasingly important are opportunities for civilian agencies and private sector support to defense. Civilian agency support to DoD was very much in evidence on September 11, 2001. Firefighters, emergency managers, and law enforcement personnel from Arlington, Virginia, and other surrounding communities saved many lives at the Pentagon. We will always be grateful for their heroism. Their support that day also foreshadowed a growing challenge in the post-9/11 era. DoD is becoming ever more dependent on capabilities provided by civilian agencies and the private sector. Yet, those same capabilities are at increasing risk to cyber attack and other threats. New forms of civil-military cooperation are essential to meet the novel challenges of this era.

### The Defense Industrial Base

DoD has long depended on the private sector to help arm and equip the armed services. But in the post-9/11 era, something important has changed: the Defense Industrial Base (DIB) is under cyber attack every day. The July 2011 *Department of Defense Strategy for Operating in Cyberspace* notes

> Foreign cyberspace operations against US public and private sector systems are increasing in number and sophistication. DoD networks are probed millions of times every day, and successful penetrations have led to the loss of thousands of files from US networks and those of US allies and industry partners.[13]

It is the responsibility of the Department of Homeland Security to protect the nation's critical infrastructure, and DIB is one of the eighteen critical infrastructure sectors under the National Infrastructure Protection Plan. Given the DoD's particular dependence on

the DIB, the need for DoD and DHS to partner with this sector against the threats they face is especially crucial.

Accordingly, the two agencies are now working closely with the DIB to increase the protection of sensitive information. The DIB comprises the public and private organizations and corporations that support DoD through the provision of defense technologies, weapons systems, policy and strategy development, and personnel. To increase protection of DIB networks, DoD launched the Defense Industrial Base Cyber Security and Information Assurance (CS/IA) program in 2007. Building upon this program, DOD is working with DHS to pilot a public-private sector relationship intended to demonstrate the feasibility and benefits of voluntarily increasing the sharing of information about malicious or unauthorized cyber activity and protective cyber security measures.[14]

Still to be determined is whether and how the models of the DoD-DHS relationship with the DIB might be extended to other parts of the private sector on which DoD depends. The DoD *Cyber Strategy* lays out some key considerations in this regard. The *Strategy* notes that public-private "partnerships will necessarily require a balance between regulation and volunteerism, and they will be built on innovation, openness, and trust." In some cases, incentives or other measures may be necessary to promote private sector participation. Efforts must also extend beyond large corporations to small and medium-sized businesses to ensure participation and leverage innovation."[15] These efforts are only just underway, and will require intense dialogue and new thinking on the part of all of those in this growing realm of collaboration.

Fortunately, DHS and DoD have shared interests and a strong partnership in this area. Last year, Secretaries Gates and Napolitano signed a memorandum of agreement laying out areas of joint cooperation in cyber security, to ensure that scarce resources are applied to the highest priority areas and to avoid unnecessary duplication of effort.

## Fort Hood and the "Insider Threat"

DoD has traditionally focused on threats outside the perimeter of our military bases. Our adversary now seeks to exploit that familiar emphasis, and inspire attacks from within. Anwar al Aulaqi of al-Qaeda in the Arabian Peninsula is actively recruiting US military personnel and other radicalized US citizens to conduct "lone actor" attacks on US military targets. The author of *Inspire*, an English language magazine, intends to encourage and facilitate terrorist attacks on the United States. Al Aulaqi has been exhorting US sympathizers to conduct attacks similar to that which occurred at Fort Hood in November 2009: "This is because killing 10 soldiers in America for example, is much more effective than killing 100 apostates in the Yemeni military."[16]

DoD is already taking a range of internal measures to counter this new strategy. For example, military facilities in the United States now benefit from "active shooter" training programs that will enable their force protection personnel to counter insider threats more effectively. The DoD *Final Recommendations of the Ft. Hood Follow-on Review* identify a score of additional measures being implemented at military facilities nationwide to prevent a recurrence of the tragedy that struck Ft. Hood.[17] Other initiatives recommended in the report, however, will require longer-term academic and policy research.[18]

The need for innovation is even greater in those areas where DoD must depend on civilian departments and agencies to help DoD counter insider threats. Because DoD is generally restricted from collecting and storing law enforcement information on US citizens, DoD must rely on civilian agencies that play an increasingly important role in the overall system that protects US military facilities. As part of the Ft. Hood review, then-Secretary Gates directed several actions to improve DoD collaboration with the FBI at the Joint Terrorism Task Forces.[19] These ongoing efforts will be particularly effective in the context of a new, consolidated DoD-FBI Memorandum of Understanding being developed, aimed at promoting systemic, standardized information-sharing mechanisms and clarifying coordination

procedures as well as investigative responsibilities between DoD and FBI. DoD will also rely on FBI, DHS and the other civilian law enforcement agencies with which the FBI and DHS are networked to provide data on other domestic threats to U.S military installations, including "lone actor" attackers. Further, DoD, as part of its force protection efforts, is working closely with state and local law enforcement to recognize the indicators of a "lone actor" threat and share suspicious activity reports to prevent another Fort Hood type of attack from occurring. As this novel threat evolves, so too must the mechanisms by which the FBI and other civilian law enforcement agencies will support DoD.

**Mission Assurance**

The cyber threat to the DIB is only part of a much larger challenge to DoD. Potential adversaries are seeking asymmetric means to cripple our force projection, warfighting, and sustainment capabilities, by targeting the critical civilian and defense supporting assets (within the United States and abroad) on which our forces depend. This challenge is not limited to man-made threats; DoD must also execute its mission-essential functions in the face of disruptions caused by naturally occurring hazards.[20]

Threats and hazards to DoD mission execution include incidents such as earthquakes, naturally occurring pandemics, solar weather events, and industrial accidents, as well as kinetic or virtual attacks by state or non-state actors. Threats can also emanate from insiders with ties to foreign counterintelligence organizations, homegrown terrorists, or individuals with a malicious agenda.

From a DoD perspective, this global convergence of unprecedented threats and hazards, and vulnerabilities and consequences, is a particularly problematic reality of the post-Cold War world. Successfully deploying and sustaining our military forces are increasingly a function of interdependent supply chains and privately owned infrastructure within the United States and abroad, including transportation networks, cyber systems, commercial corridors, communications pathways, and energy grids. This infrastructure largely falls outside DoD direct control. Adversary actions to destroy, disrupt, or manipulate this highly vulnerable homeland- and foreign-based infrastructure may be relatively easy to achieve and extremely tough to counter. Attacking such "soft," diffuse infrastructure systems could significantly affect our military forces globally – potentially blinding them, neutering their command and control, degrading their mobility, and isolating them from their principal sources of logistics support.

The Defense Critical Infrastructure Program (DCIP) under Mission Assurance seeks to improve execution of DoD assigned missions to make them more resilient. This is accomplished through the assessment of the supporting commercial infrastructure relied upon by key nodes during execution. By building resilience into the system and ensuring this support is well maintained, DoD aims to ensure it can "take a punch as well as deliver one."[21] It also provides the department the means to prioritize investments across all DoD components and assigned missions to the most critical issues faced by the department through the use of risk decision packages (RDP).[22]

The commercial power supply on which DoD depends exemplifies both the novel challenges we face and the great progress we are making with other federal agencies and the private sector. Today's commercial electric power grid has a great deal of resilience against the sort of disruptive events that have traditionally been factored into the grid's design. Yet, the grid will increasingly confront threats beyond that traditional design basis. This complex risk environment includes: disruptive or deliberate attacks, either physical or cyber in nature; severe natural hazards such as geomagnetic storms and natural disasters with cascading regional and national impacts (as in NLE 11); long supply chain lead times for key replacement electric power equipment; transition to automated control systems and other smart grid technologies without robust security; and more frequent interruptions in fuel supplies to electricity-generating plants. These risks are magnified by globalization, urbanization, and the highly interconnected nature of people, economies, information, and infrastructure systems.

The department is highly dependent on commercial power grids and energy sources. As the largest consumer of energy in the United States, DoD is dependent on commercial electricity sources outside its ownership and control for secure, uninterrupted power to support critical missions. In fact, approximately 99 percent of the electricity consumed by DoD facilities originates offsite, while approximately 85 percent of critical electricity infrastructure itself is commercially owned.

This situation only underscores the importance of our partnership with DHS and its work to protect the nation's critical infrastructure – a mission that serves not only the national defense but also the larger national purpose of sustaining our economic health and competitiveness.

DoD has traditionally assumed that the commercial grid will be subject only to infrequent, weather-related, and short-term disruptions, and that available backup power is sufficient to meet critical mission needs. As noted in the February 2008 *Report of the Defense Science Board Task Force on DoD Energy Strategy*, "In most cases, neither the grid nor on-base backup power provides sufficient reliability to ensure continuity of critical national priority functions and oversight of strategic missions in the face of a long term (several months) outage."[23] Similarly, a 2009 GAO Report on *Actions Needed to Improve the Identification and Management of Electrical Power Risks and Vulnerabilities to DoD Critical Assets* stated that DoD mission-critical assets rely primarily on commercial electric power and are vulnerable to disruptions in electric power supplies.[24] Moreover, these vulnerabilities may cascade into other critical infrastructure that uses the grid – communications, water, transportation, and pipelines – that, in turn, is needed for the normal operation of the grid, as well as its quick recovery in emergency situations.

To remedy this situation, the Defense Science Board (DSB) Task Force recommended that DoD take a broad-based approach, including a focused analysis of critical functions and supporting assets, a more realistic assessment of electricity outage cause and duration, and an integrated approach to risk management that includes greater efficiency, renewable resources, distributed generation, and increased reliability. DoD Mission Assurance is designed to carry forward the DSB recommendations.

Yet, for a variety of reasons – technical, financial, regulatory, and legal – DoD has limited ability to manage electrical power demand and supply on its installations. As noted above, DHS is the lead agency for critical infrastructure protection by law and pursuant to Homeland Security Presidential Directive 7. The Department of Energy (DOE) is the lead agency on energy matters. And within DoD, energy and energy security roles and responsibilities are distributed and shared, with different entities managing security against physical, nuclear, and cyber threats; cost and regulatory compliance; and the response to natural disasters. And of course, production and delivery of electric power to most DoD installations are controlled by commercial entities that are regulated by state and local utility commissions. The resulting paradox: DoD is dependent on a commercial power system over which it does not – and never will – exercise control.

Although there are steps DoD can and should take on its own to improve resilience and continuity of operations, achieving more comprehensive electric grid security to ensure critical DoD missions is not something DoD can do alone. Meeting and securing the critical electric power needs of DoD in an interdependent and increasingly complex risk environment requires a broad scope of collaborative engagement between government and industry stakeholders whose roles and responsibilities in power grid security and resiliency are distributed and shared.

DoD is collaborating with DOE, DHS, the Federal Energy Regulatory Commission, and industry representatives, namely the North American Electric Reliability Corporation (NERC), in these matters. For example, DoD is planning to develop a combined kinetic and cyber threat-based scenario for the US electric power grid. This scenario could be tested by DOE and others on a regional scale throughout the country and could produce data to support the development of a new system "design basis" for building additional

resilience in the US electric power grid. The department is also working with the NERC on a case study of a military installation for analysis, paired up with the local utility provider, to determine what can be done in the short term to mitigate electric power vulnerabilities and risks. DoD will make the results of this analysis more broadly available to DHS, DOE, and the industry. These efforts will help DoD achieve greater energy grid security and resiliency and help mitigate the risks to critical DoD missions from commercial power outages.

DoD is making organizational changes and capability improvements that address electric power reliability and security issues and that enable better risk-informed decision-making and investments. In January 2011, DoD submitted a report to Congress describing on-going efforts to mitigate the risks posed to critical DoD missions by extended power outages resulting from failure of the commercial electricity supply or grid and related infrastructure.[25]

In the report, DoD identified risks to the infrastructure supporting its key missions and is working with affected mission owners to "buy down" risk to an acceptable level. When fully implemented, risk reduction courses of action are aimed at reducing these risks to an acceptable level for DoD. DoD is conducting a series of case studies to identify the policy and technical issues associated with mitigating long-term electric power outages on installations. DoD is also planning and conducting demonstrations on installations to create cyber-secure power systems with microgrids and other smart grid technologies to improve electric grid security. The Marine Corps Air Ground Combat Center at Twentynine Palms, California, is implementing energy efficiency and alternative energy initiatives to demonstrate how microgrids will serve as an important component of the smart grid.

DoD established the Energy Grid Security Executive Council (EGSEC) to oversee many of these initiatives. The EGSEC brings together experts and senior executives from across DoD and from DOE and DHS to focus on ensuring the security of the electric grid that serves DoD. The EGSEC focuses on DoD energy grid vulnerability issues, the risk to critical missions created by commercial power outages, and developing comprehensive mitigating solutions.

We must identify and acknowledge our vulnerabilities and make the right choices – in collaboration with our strategic "partners" – to buy down our collective risk to an acceptable and affordable level in an informed way across the department. Determining how best to do that will require a sustained analytic effort and a willingness to collaborate in new ways. Driving that process forward, in the realm of mission assurance and so many others, would be a wonderful way to honor those who perished on 9/11.

## ABOUT THE AUTHOR

***Paul N. Stockton*** *is the assistant secretary of defense for Homeland Defense and Americas' Security Affairs. In this position, he is responsible for the supervision of homeland defense activities, defense support of civil authorities, and Western Hemisphere security affairs for the Department of Defense. From 2002 – 2006, Assistant Secretary Stockton served as director for the Naval Postgraduate School's Center for Homeland Defense and Security.*

[1] "DOD, Governors Bridge Gaps in Disaster Response," *American Forces Press Service*, March 11, 2011, http://www.defense.gov/news/newsarticle.aspx?id=63128.

[2] Amr S. Elnashai, Lisa J. Cleveland, Theresa Jefferson, and John Harrald, *Impact of New Madrid Seismic Zone Earthquakes on the Central USA* (Urbana, IL: Mid-America Earthquake Center, October 2009), http://mae.cee.uiuc.edu/publications/2009/09-03.htm.

[3] Ibid.

[4] The North America Energy Reliability Corporation estimated that the quake would instantly de-energize approximately 750 transmission lines and 300 substations in the region, and cause "extensive damage" to approximately half of the 500kV substations and other critical elements of the grid in Tennessee and Arkansas. North American Electricity Reliability Corporation, *Electricity Sector Damage Assessment for National Level Exercise 2011* (March 2011).

[5] Ibid.

[6] The White House, Executive Office of the President, *National Strategy for Counterterrorism* (Washington, DC, June 2011), 1, 11-12.

[7] *National Strategy for Counterterrorism*, i.

[8] Ibid.

[9] "How to Make a Bomb in the Kitchen of Your Mom," *Inspire,* Summer 2010, 33.

[10] *National Strategy for Counterterrorism*, 11.

[11] The White House, Executive Office of the President, Presidential Policy Directive-8 (Washington, DC, March 2011), 1-2.

[12] A prime example of the need for innovation: what concept of operations should these partners utilize in an IED campaign, or in a series of Mumbai-style attacks in US cities? How can we ensure that prevention, protection, and response efforts will be conducted in an integrated, mutually supportive fashion during such campaigns, amidst the crushing media and political pressures that will emerge? In light of the roles in defense support to civil authorities that DoD may assume under the prevention framework and implementation plan, how should DoD be postured to respond to requests for prevention assistance quickly and effectively, consistent with the Constitution and other US law, and recognizing the competing priorities DoD will face in a difficult fiscal environment? Answering these questions will require a strong analytic effort that leverages the expertise and perspectives of all the participants in the preparedness system that PPD-8 requires.

[13] US Department of Defense, *Strategy for Operating in Cyberspace* (Washington, DC, July 2011), 3.

[14] Ibid., 8.

[15] Ibid., 9.

[16] "Inspire Responses," *Inspire,* Spring 2011, 11.

[17] U. Department of Defense, Office of the Secretary of Defense, *Final Recommendations of the Ft. Hood Follow-on Review* (Washington, DC, August 2010), 10.

[18] For example, the Secretary of Defense issued interim guidance on indicators of violent behavior that will be modified with the completion of three studies. First is a Defense Science Board study projected for completion in early 2012. This study will be followed by two medical studies (a retrospective study and a prospective study) on DoD personnel. DoD will, as appropriate, incorporate the lessons of the studies into policies and programs upon study completion.

[19] *Ft. Hood Follow-on Review*, 10.

[20] US Department of Defense, *Mission Assurance Strategy*, draft, 1.

[21] Joseph Straw, "How to Take a Punch," *Security Management* (May 2011).

[22] RDP are risk management tools developed by the various asset owners and coordinated with the Combatant Commanders who rely upon these critical nodes to define the risk in terms of the existing threats and hazards, vulnerabilities of the existing system, and the consequence of loss if this node's support was interrupted. Asset owners then provide various courses of action (COA) to reduce this generated risk score to an acceptable level for the combatant commander. Once completed, these COA are prioritized so that the department knows exactly where to spend its limited resources most effectively.

[23] Defense Science Board, *Report of the Defense Science Board Task Force on DoD Energy Strategy: "More Fight, Less Fuel"* (Washington, DC: Office of the Under Secretary of Defense for Acquisition, Technology, and Logistics, February 2008),

[24] GAO Report 10-147, *"Defense Critical Infrastructure: Actions Needed to Improve the Identification and Management of Electrical Power Risks and Vulnerabilities to DoD Critical Assets"* (Washington, DC: October 2009).

[25] National Defense Authorization Act for Fiscal Year 2009, "Mitigation of Power Outage Risks for the Department of Defense Facilities and Activities" (Washington, DC: January 2011).

# Does Homeland Security Exist Outside the United States?

Nadav Morag

Homeland security is a uniquely American concept. It is a product of American geographic isolation and the strong tendency throughout American history to believe that there was a clear divide between events, issues, and problems outside US borders and those inside US borders. Among other things, the legal and institutional tools with which the United States is able to deal with threats outside its borders (in the context of what is referred to as "national security") differ markedly from those it is able to employ inside its borders. In the aftermath of the terrorist attacks on September 11, 2001, American leaders realized that they would need new tools to deal with large-scale terrorist threats and yet they were constrained by the Constitution, legislation, and federalism. Consequently, they largely could not apply tried and tested national security tools and methodologies to the domestic arena. Homeland security policies, institutions, and methodologies thus developed to fill this void between what the US could do overseas and what it was unable to do domestically. The subsequent inability to deal with large-scale disasters, such as that produced by Hurricane Katrina in late August of 2005, led to a broadening of the definition of homeland security to include large significant disasters, major public health emergencies, and other large-scale events that had the potential to endanger the citizenry, economy, rule of law, and the general functioning of government and society.[1]

America's sister democracies around the world did not undergo the dual shocks of 9/11 and Katrina; thus, these countries did not face situations of significant social or economic chaos resulting from such a wide range of threats. Some of them, like Israel and the United Kingdom, had to cope with significant terrorist threats while others, such as Japan, had to cope with significant natural disasters, but none had to cope with massive and unprecedented terrorist events and natural disasters in the space of only a few years. Moreover, countries such as Australia, Canada, Germany, France, the UK, Israel, Japan, Italy, the Netherlands, and others had never really viewed domestic threats as qualitatively different from overseas threats and were able to use tools – such as the military – both externally and internally (though, of course, not in precisely the same way). Given the above, it is not surprising that the concept of homeland security, as an integrative idea that brings together domestic preparedness, response, and recovery efforts with respect to threats ranging from large-scale terrorism to natural disasters to pandemics (to name a few) was largely alien to these countries. It is not that other democracies did not prepare for, attempt to mitigate, respond to, and recover from terrorism, natural disasters, public health emergencies, threats to critical infrastructure, and the like; it is just that they did not view all of these activities as interlinked and part of a common effort designed to head off and, failing that, cope with and recover from events that could produce massive social and economic disruption.

With the creation, in the United States, of homeland security as a policy framework and practitioner and academic discipline during the course of the first decade of the twenty-first century, other democracies took notice and some began to use the terminology of homeland security without, necessarily, understanding its scope or *raison d'être*. Most countries have still not truly come around to the idea that counter-terrorism, emergency management, critical infrastructure protection, public health, combating large-scale crime, etc. are part and parcel of the same overall problem: that of maintaining social and economic stability and governmental functioning in the face of events that threaten to overwhelm the capacity of government and society to cope.

A case in point is the United Kingdom. The UK is one of the most, if not the most, prolific producer of national and local governmental strategies. It has an elaborate

and well-thought-out counterterrorism strategy known as CONTEST with four elements: Prevent, Pursue, Protect and Prepare.[2] Counterterrorism, as used in the UK, is a broad policy area that also includes maritime, aviation and border security, critical infrastructure protection, and resilience but it is not entirely equivalent to homeland security both because it does not address as broad a range of functions and because it is focused on preventing, preparing for, responding to, and coping with, terrorism. London and other local jurisdictions have also developed emergency management plans based on a three-tier incident management system (the tiers are referred to as gold, silver, and bronze) that separate the strategic functions from the tactical and operational ones.[3] These response systems will kick in during major terrorist incidents as well as disasters (the UK suffers from flooding on occasion), but they are not necessarily seen as integrally related to the counterterrorism effort.

From an organizational standpoint, a significant segment of the homeland security enterprise is housed in the Home Office, which is the national-level department that overseas aspects of the law enforcement mission. Although the UK's regional and national police forces are administratively independent, the Home Office does have oversight and funding influence over them. Moreover, the country's premier investigatory agency, the Serious and Organized Crime Agency (SOCA) is under the direct purview of the Home Office. The domestic intelligence mission, carried out by the British Security Service (MI5), is also under the authority of the Home Secretary. Finally, border security (the UK Border Agency operates under the auspices of the Home Office) and immigration are also within the Home Office's remit.[4] Nevertheless, functions such as those carried out by the Federal Emergency Management Agency (FEMA) and housed within the US Department of Homeland Security are not within the scope of Home Office operations. Moreover, at the state level, most homeland security agencies in the United States have a large emergency management component and many also include a public health component (though public health is primarily a local governmental function in the United States) and all of these do not exist in any one institution in the UK. In short, in terms of doctrine, policy, and organization, the UK does not view counterterrorism and emergency management (not to mention other elements of the homeland security enterprise) as part of a common operational sphere.

At the other end of the spectrum lies Canada, influenced as it is by its proximity and historic relationship to the United States. Canada has moved closer to the US model of a homeland security enterprise. Canada's national security policy (the reader will note this is national security more broadly, as opposed to just homeland security) incorporates the disciplines of law enforcement, intelligence, emergency management, public health, and transportation and border security, but it also includes aspects of international security that take it outside the sphere of the homeland security enterprise.[5] Organizationally Canada takes somewhat of a middle ground approach between the UK and the US in that, while it does not incorporates security and emergency management under the same organizational framework, it does view these disciplines as part of the overall public safety mission. The premier federal security department in the country is Public Safety Canada, which is responsible for federal law enforcement (via the Royal Canadian Mounted Police, RCMP, which also contracts to provincial and municipal governments to provide policing services) and intelligence (via the Canadian Security Intelligence Service, CSIS). While Public Safety Canada does not have direct organizational responsibility for emergency management in the way that DHS does via FEMA, it will play a coordinating role with federal ministries responsible for health and critical infrastructures, as well as with provincial and municipal authorities and the private sector.[6]

Israel arguably lies at the center of the spectrum. Though it does not possess an articulated national security strategy, let alone a homeland security one (Israeli prime ministers do not like to be penned in by formal strategies), it has, in practice, adopted elements of a homeland security doctrine that tie together the police, fire, EMS, the health

system, and the military. Despite fighting major wars at least once a decade since independence, the country's civilian sector was largely exempted from military attack (though not terrorism). However, the current presence of long range/high payload surface-to-surface missiles, as well as short-range/ low payload rockets, has made Israel's civilian population highly vulnerable. In the wake of the SCUD attacks on Israel in the 1991 Gulf War, the Israel Defense Force (IDF) recognized that the civilian sector had come to be part of the battle space (if not, indeed, the primary battle space) and created a fourth regional command (in addition to the Northern, Central and Southern Commands): the Homefront Command (HFC). The HFC was created to improve interagency cooperation between the military, first responders, and government ministries, to free the three IDF regional commands to focus exclusively on the front lines, to provide military resources to the civilian sector (capabilities such as search and rescue, WMD detection and response, etc.), and to enable the centralization of response efforts.[7] In normal times, the HFC is responsible for establishing emergency procedures, supervising preparedness exercises, and monitoring the preparedness of the health system, municipalities, the transportation system, and critical infrastructures. During periods in which Israel is facing an active wartime scenario (or potentially, a WMD terrorist attack or other mass casualty event), the Cabinet can declare a "limited state of emergency" whereupon the HFC is given command and control over the other response agencies. The integrative Israeli approach however, is focused primarily on the response piece of the homeland security mission. In terms of prevention and organizational structures, the police (Israel has a single national police force) coordinate with the domestic intelligence service, the Israel Security Agency (ISA, also known as the *Shin Bet* or *Shabak*) and the military (which has law enforcement powers in the West Bank), but each entity largely functions in its own operational sphere and according to its own operational doctrine.

Overall then, as the above examples have shown, homeland security is not really conceived of abroad as an "enterprise" and overarching discipline in the manner in which it is viewed in the United States. Whether or not it is entirely viewed in this manner in the United States is arguable since, at least from the organizational perspective, the homeland security mission is not even strictly confined to DHS at the federal level or to state or local homeland security offices at their respective levels of government. However, the homeland security enterprise is being actively developed as a discipline in the US and this is likely to continue to impact policies, strategies and institutions. Whether or not other countries will eventually adopt the same logic and view their disparate homeland security efforts as part of the same set of objectives requiring a joint policy, doctrinal, and organizational framework remains to be seen.

Notwithstanding the present absence overseas of homeland security as a coherent policy sphere, other countries are still engaging in homeland security-related policymaking and strategizing. Learning from other countries' experiences and approaches in this context is important not only because it makes sense for American decision makers to learn from the experiences of foreign governments (of which there are many) and thus avoid trying to "reinvent the wheel," but also because, in many cases, the threats are transnational and consequently safeguarding homeland security requires cooperation with other countries. Whether the threat emanates from radicalized Europeans accessing the United States under the visa waiver program in order to execute terrorist attacks, or aircraft passengers flying in to the US from an Asian city carrying the latest viral mutation with them, many homeland security threats emanate from abroad. Examples of such threats abound. In the terrorism sphere, in addition to the 9/11 attackers, Ahmed Resam (the "Millennium Bomber"), arrested in 1999, used Canada as a staging area for his plot to bomb the Los Angeles International Airport. Richard Reid (the "Shoe Bomber") boarded a Miami-bound flight in Paris in December 2001. The 2006 transatlantic liquid explosives plot (the "Overt Plot") was hatched and prepared in the UK and Umar Farouk Abdulmutallab (the "Underwear Bomber" or "Christmas Bomber") boarded his Detroit-bound flight in Amsterdam in

December 2009. The potential and actual spillover of Mexican criminal violence into the US has also been an issue of concern for some time. In the pandemic sphere, the SARS outbreak in China led to the US public health system being put on alert in December 2003 and the outbreaks of avian influenza and swine flu in Southeast Asia and Mexico respectively led to pandemic concerns in the US. In short, there is no lack of examples of homeland security threats emanating from overseas. It therefore follows that addressing these threats will not only require international cooperation, but also an understanding of how other countries, particularly allied democratic nations, address these issues within their own borders before those issues reach US shores, and what their respective laws, institutions, and modes of operation allow those countries to do.

Ultimately then, as homeland security becomes more of a global enterprise, other countries may realize the logic of having objectives supersede tools and methodologies. In other words, they may come to adopt American logic that the ultimate objectives of ensuring social and economic stability and the continued rule of law in severe crisis situations means that operational spheres as seemingly disparate as counterterrorism, law enforcement in the face of massive criminal activity, securing transport systems, borders, and critical infrastructure, and coping with public health emergencies and the management of crisis situations are all essentially part of the same effort. If and when this does occur, it will make it considerably easier for the United States to improve its ability to safeguard homeland security because it, and its global partners, will be viewing the problem in the same way and integrating their respective resources and strategies accordingly.

## ABOUT THE AUTHOR

***Nadav Morag*** *is a faculty member and deputy director for policy research at the Center for Homeland Defense and Security, Naval Postgraduate School. He is the author of* Comparative Homeland Security: Global Lessons *(Wiley & Sons, 2011) and is a former senior director at Israel's National Security Council.*

[1] See the differences in emphasis in the 2002 and 2005 versions of the *National Strategy for Homeland Security* as well as changing White House definitions of what falls within the Homeland Security mission space.

[2] UK Government, *Countering International Terrorism: The United Kingdom's Strategy* (London: Stationery Office, 2006).

[3] London Emergency Services Liaison Panel, *Major Incident Procedure Manual*, 7th ed. (London: LESLP, 2007).

[4] See the Home Office website: www.homeoffice.gov.uk

[5] Canadian Privy Council Office, *Securing an Open Society: Canada's National Security Policy* (Ottawa: Canadian Government, 2004).

[6] See http://www.publicsafety.gc.ca/prg/em/ci/index-eng.aspx.

[7] See http://www.oref.org.il/82-en/PAKAR.aspx.

# Ten Years After the Terrorist Attacks of 9/11: The Need for a Transnational Approach to Address Risks to US Global Security Interests

John Rollins

## INTRODUCTION

Increasing risks associated with man-made and naturally occurring incidents, coupled with the inter-relationship of seemingly disparate activities, suggest that the world is more dangerous and vulnerable than at anytime in recent history. The United States, as the most technologically advanced and globally connected nation on earth, is especially at risk to systematic or single-incident disruptions. Lessons learned from incidents occurring prior to and since the terrorist attacks of 9/11 have demonstrated that the current US approach to addressing risk is not always effective and may be ill suited to assess emerging challenges. The US no longer has the geographic or economic luxury of approaching security issues from a domestic or international perspective. Regardless of where a threat emanates from, today's security professionals need to recognize, respond to, and appreciate the totality of the near- and long-term implications of risks facing the nation. During this period of remembrance of the terrorist attacks of September 11, 2001, now is the time to consider transitioning away from a geographic-centric focus of safeguarding the nation's interests to a transnational approach to security that reflects a better understanding of the complexities of global risks.

### UNITED STATES APPROACH TO SECURITY PRIOR TO SEPTEMBER 11, 2001

Many changes to the US approach to addressing global security issues have occurred since World War I and have usually been in response to an incident that has demonstrated a shortcoming in the government's ability to effectively detect and respond to a threat. Based in part on the Japanese attack on Pearl Harbor in 1941 and the deficiencies observed in effectively addressing international security matters during World War II in 1947, the National Security Act was passed to better align the missions and goals of the military, foreign policy, and intelligence communities. The surprises associated with the start of the Korean War in 1950, the Iraq invasion of Kuwait in 1990, and the bombing of the Oklahoma City Murrah Federal building in 1995, led to agency reorganizations and redistribution of resources between the international and domestic security activities. Similarly, the Federal Emergency Management Agency has been reorganized numerous times after perceived failures in responding to natural disasters.

After each of these incidents, and others like them, successive administrations and policymakers pursued organizational changes to the nation's security apparatus, including a reprioritizing of focus and resources previously dedicated to overseas and domestic security activities. Often the philosophical and organizational changes approved by policymakers assumed that the next significant event would likely take the form of the most recent incident. In fact, some might suggest that many of America's security leaders continue to suffer from the same myopic approach to assessing current and emerging threats. The World Economic Forum's annual global risk report for 2011 found that "in an increasingly turbulent global environment there is the temptation to always focus on the most recent risk event, it is important to take a long-term perspective to risk assessment and response. Many global risks could emerge over decades rather than months or years."[1] Such a propensity to philosophically approach and organize to fight the last war may have contributed to the US government's under appreciation of risks facing the nation prior to 9/11. Al-Qaeda first

targeted US interests when attempting to attack service members in Yemen in 1992. In the intervening period, between 1992 and September 10, 2001, the terrorist group successfully carried out numerous other attacks against US global interests. Distracted by more recent events and lacking appreciation of global threats, the nation's security attention was focused elsewhere.

## POST-9/11 SECURITY: A SOMETIMES EFFECTIVE BUT NOT REFLECTIVE APPROACH TO THREATS

After the 9/11 terrorist attacks, the US reorganized its security apparatus, creating a host of new organizations and authorities to better address threats directed at the homeland. This reaction, and the subsequent Global War on Terror, came at high cost both in terms of blood and treasure and were undertaken during a very emotional and highly politicized environment. One might describe the post-9/11 approach to security as the taking of offensive actions overseas to defeat terrorists planning efforts directed at global interests while undertaking defensive measures in the homeland making it difficult for bad actors to enter or freely operate in the United States. The US military, foreign service, and the overseas-focused aspects of the intelligence community have been focused on the away game while the post-9/11 creation, the Department of Homeland Security, the Federal Bureau of Investigation, state, local, tribal, and private sector entities have been guarding the homeland. To some, such a concept could be viewed as a rational response to the terrorist attacks of 9/11. In hindsight, it could also be argued that while the attacks were significant and catastrophic, they were not indicative of a persistent threat challenging the American way of life. Furthermore, some might suggest that the US response to this tragedy has contributed to a misunderstanding of the diversity of threats found in the global environment and the creation of a sometimes-ineffective approach to assessing risk.

The post-9/11 government adoption of a bifurcated organizational and philosophical approach to national and homeland security has achieved a number of well-publicized and unreported counterterrorism, intelligence, natural disaster, and public health successes. However, there have also been examples where the unclear responsibilities of applicable organizations and the need to address prospective threats from a domestic or international perspective have led to inefficiencies, actual and near tragedy, and continuing challenges in detecting, responding, or recovering from a security-related issue. Examples include:

- Response and recovery efforts and offers of international assistance associated with Hurricane Katrina of 2005 and the 2010 B.P. oil spill,
- Intelligence community and diplomatic policy failures that nearly led to a successful detonation of an explosive device onboard a US bound aircraft in December 2009,
- Late recognition of radicalization efforts by global actors enticing US citizens to take-up arms against countrymen,
- Slow recognition and response to the 2009 global H1N1 pandemic, and
- Numerous counterterrorism-related legal and policy decisions void of appreciation of long-term implications and consequences.

For most of these incidences failures were assessed, additional resources were authorized, reorganizations implemented, and new policies were developed to ensure that the next time a similar incident occurs a more robust system would be in place to detect prospective anomalies. However, the conceptual approach to detecting and responding to threats remains the same: maintaining separate, and at times uncoordinated processes, based on the current understanding of the origination of the threat and the prospective targets. Future threats directed at US interests are increasingly less likely to observe and be constrained by national borders or the veil of geographic protection enjoyed since World War II. DHS Secretary Janet Napolitano offered a similar sentiment in June 2011 at a Center for Strategic and International Studies forum focused on building strong international partnerships, when she stated

that "the evolving threats we face are not limited by international borders."[2] Natural disasters have never recognized a nation's borders when causing damage and America's introduction to asymmetric warfare against US interests should serve as an indicator that some of America's greatest attributes; open society, multitude of connections to global activities, and observance of the rule of law, also serve to make us more vulnerable.

Due to the complexity of current and emerging threats and US interconnectedness with global financial, infrastructure, and security ecosystems, the nation is increasingly at risk of falling prey to man-made or naturally occurring incidences. Failed and failing states and ungoverned areas; sophisticated criminal syndicates; changes to the climate; the ease of manufacturing and surreptitious delivery of harmful explosive, biological, and technological devices with increasingly lethal results; and dwindling life-sustaining resources are but a few of the near- and long-term transnational security challenges the nation will be required to confront. Accompanying these threats will be a degraded international order whereby many nations' capacity to address challenges and organizations focused on global sustainability may be on the decline. Traditionally stable state powers the United States relies upon to identify risks and assist with addressing global security issues of mutual interest are encountering challenges in maintaining viability. An assessment accompanying the annually published Failed State Index, published in June 2011 by the Fund for Peace, notes "the upper echelons of the Failed States Index are occupied almost exclusively by Western European nations. Some of the worst slides this year were recorded in Western Europe as the economic crisis began to impact on countries such as Ireland and Greece."[3] Should other long-standing international partners of the US encounter economic difficulties, one must start questioning their capacity to be an effective member of the global security apparatus.

What might have been understood, but not adequately acted upon until after the terrorist attacks of September 11, 2011, was that a threat to US interests can be manifested from anywhere in the world and have both domestic and international implications. Such threats can have very real safety, economic, and societal consequences if security leaders are unable to appreciate the transnational implications accompanying risks found throughout the world. In a speech given to the South Carolina Corps of Cadets in October, 2010 DHS Secretary Napolitano addressed the need for today's security professionals to take a more global perspective of risks facing the nation when she stated that none of today's threats "stop at the border to morph from a national to a homeland security threat. Our thinking – and our responses – can't stop at the borders either." She further stated:

> The attacks of September 11, 2001 challenge the conventional notion that foreign threats were truly foreign and that we could maintain a divide between domestic and foreign affairs. Profound shifts are still underway and are even faster and more transformational that ever. The lines between the foreign and domestic are even murkier than before, if often not there at all.[4]

The nation can no longer afford to categorize or approach threats from a national or homeland security perspective. Strategies, policies, organizations, and resources devoted to addressing one aspect of risk to US global security interests will prove insufficient to the challenges facing the nation and may miss significant connections to the larger global threat environment. In order to best prepare the nation's security professionals to address emerging risks, a transnational approach should be adopted.

## A TRANSNATIONAL APPROACH TO PROTECTING US GLOBAL SECURITY INTERESTS

Whether a threat emanates from overseas or in the homeland, implications can be found, and should be explored, to gain a true appreciation of specific activity and possible consequences. A transnational security approach, which entails understanding and addressing the interrelationship of global risks to a nation's short- and long-term strategic interests, should be adopted to assist in recognizing and responding to

threats we know exist, threats we can envision, and unforeseen threats. The adoption of a transnational approach to protecting US global security interests would have a number of benefits, including:

- Giving current and future security professionals an opportunity to better appreciate the diversity and complexity of threats facing the nation,
- Providing policymakers a better understanding of the implications and consequences of actions pursued in response to an emerging threat,
- Utilizing funds and other resources in a more efficient and targeted manner, and
- Reducing the likelihood of unforeseen events and a more thoughtful approach to policy and resource considerations when a significant incident does occur.

The 2008 *National Intelligence Council's Global Trends 2025: A Transformed World* report affirmed the need for security professionals to have a transnational appreciation of risk by assessing that the future will entail a "rapidly changing international order of growing geopolitical challenges with an increased likelihood of discontinuities, shocks, and surprises."[5] The Global Trends report further noted that today's enemies have already adopted a global approach to terrorism, crime, and financial pursuits with the goal of "leveraging transnational outcomes across national and organizational boundaries."

The US *National Strategy for Counterterrorism*, released in June 2011, states "the preeminent security threat to the United States continues to be from al-Qaeda and its affiliates and adherents."[6] According to data compiled by the Centre for Research on the Epidemiology of Disasters, for the majority of the period between 1975 to 2010 there has been a steady trend upward of the number of people affected, and estimated damages caused, by natural disasters.[7] The 2011 Global Peace Index has found that the world is less peaceful for a third straight year based on assessing international, regional and national conflicts, safety and security in societies, and militarization efforts.[8]

As witnessed during the past decade, policy, organizational, and resource decisions made in a post-incident crisis environment often lack foresight and are dismissive of long-term consequences of actions pursued. Whether al-Qaeda will still be in existence when America observes the twenty-year remembrance of the attacks of September 11, 2001, the consequences of disasters continue to increase, or the world becomes a less peaceful place, a reasonable assessment of tomorrow's challenges suggests a new approach is needed to understand and address global risk. Elected officials and policymakers should use ongoing budgetary discussions related to reducing or eliminating funding for activities and programs that are seen as ineffective or duplicative to initiate changes to the nation's current approach to security. Through the use of future budget allocations, policy-makers should require systemic changes be made to the federal security apparatus that transitions security organizations away from focusing on threats from a geographically linear perspective to an appreciation of the global complexities associated with risks facing the nation. Future legislative, strategy, policy, and resource decisions should be based on a more mature understanding of the global risk environment with a desire for the federal government to be organized and resourced in a manner that corresponds to current and emerging transnational security concerns. Adoption of such an approach will better prepare the nation to address known threats and unforeseen risks.

As we enter a relatively peaceful period of remembrance with the tenth anniversary of the attacks of September 11, 2001, America now possesses a refined understanding of risks to the nation's global interests. Might this period of reflection serve as an opportune time to discuss adopting a transnational approach to meeting tomorrow's security challenges?

## ABOUT THE AUTHOR

***John Rollins*** *is an adjunct faculty member of the Center for Homeland Defense and Security (CHDS). The thoughts expressed in this article do not represent the views of CHDS or any other*

*organization with which Rollins may be affiliated.*

---

[1] World Economic Forum, *Global Risks 2011* (Geneva, Switzerland: World Economic Forum, 2011), 41.

[2] DHS Secretary Janet Napolitano, remarks before Center for Strategic and International Studies Statesmen's Forum, *Building Strong International Security Partnerships: The U.S.-India Homeland Security Dialogue*, Washington, DC, June 2, 2011, http://www.dhs.gov/ynews/releases/pr_1307485712555.shtm.

[3] J.J. Messner, senior associate at the Fund for Peace, "Remarks on Index Highlights of The Failed State Index 2011," Washington, DC, June 29, 2011, http://www.fundforpeace.org/global/?q=node/143.

[4] DHS Secretary Janet Napolitano, remarks before the Citadel's Corps of Cadets, *Greater Issues: Homeland Security Secretary Janet Napolitano*, Charleston, SC, October 21, 2010, http://externalaffairs.citadel.edu/napolitano_speech.

[5] National Intelligence Council, *Global Trends 2025: A Transformed World* (Washington DC: National Intelligence Council, November 2008), 3.

[6] President Barak Obama, *National Strategy for Counterterrorism*, June 28, 2011, 3, http://www.whitehouse.gov/sites/default/files/counterterrorism_strategy.pdf.

[7] United Nations International Strategy for Disaster Reduction, *Disaster Through a Different Lens: Behind Every Effect, There is a Cause*, (Geneva, Switzerland: United Nations International Strategy for Disaster Reduction, n.d.) 28.

[8] Institute for Economics and Peace, *Global Peace Index* (Sydney, Australia: Institute for Economics and Peace, 2011), 3.

# Domestic Intelligence Today: More Security but Less Liberty?

Erik J. Dahl

One of the most important questions about intelligence reform after the 9/11 attacks was whether the United States should establish a new domestic intelligence agency – an American equivalent of the British MI-5, some suggested. Supporters of the idea argued that only a completely new organization would be able to provide the fresh thinking and strength of focus that was needed, and they pointed out that the US was the only Western country without such an organization. Critics said the Federal Bureau of Investigation (FBI) was already well on its way to reinventing itself as just the sort of intelligence-driven agency the country needed and that establishing a new domestic intelligence agency would require the creation of a costly new bureaucracy to duplicate capabilities that already existed.

That debate was eventually settled in the negative. Although a number of major reforms were made to American intelligence – including, most notably, the establishment of the position of the Director of National Intelligence (DNI) – no central domestic intelligence agency has been created. Instead, the intelligence functions of the FBI have been beefed up and several new organizations have been created, including the National Counterterrorism Center (NCTC). Although occasionally the argument is still heard that the US needs a domestic intelligence service,[1] in general most intelligence professionals and outside observers appear to agree that no new domestic intelligence organization is necessary.

But this essay argues that even though we as a nation decided not to establish a domestic intelligence organization, we have in recent years done just that: we have created a vast domestic intelligence establishment, one which few Americans understand and which does not receive the oversight and scrutiny it deserves. There is good news here: this domestic intelligence system appears to have been successful in increasing security within the US, as demonstrated by numerous foiled terrorist plots and the lack of another major successful attack on American soil since 9/11. But there is also bad news: these gains are coming at the cost of increasing domestic surveillance and at the risk of civil liberties.

This essay begins by reviewing the debate over whether a domestic intelligence agency was needed after 9/11. It then describes the current system of homeland security intelligence within the US, including the growth of new intelligence organizations at the state and local level, and argues that this constitutes a de facto domestic intelligence organization. Next it demonstrates that the development of this domestic intelligence structure has moved the balance between security and liberty quite firmly in the direction of more security, but less liberty. The essay concludes by arguing that even though these developments might very well be acceptable to the American people, we cannot know whether they are acceptable or not without a better-informed national discussion about domestic intelligence.[2]

## The Debate over a Domestic Intelligence Agency

One aspect of the debate over intelligence reform following the 9/11 attacks was the question of whether the United States should establish a new domestic intelligence agency. Although the question was often framed in terms of whether the US should create an organization modeled on the British MI-5, several options were widely discussed.

The change supported by many experts was to form an independent intelligence service within the FBI. The FBI already had the lead on most domestic intelligence issues and since 9/11 had been increasing its focus on intelligence, so forming such an organization within the FBI appeared to be the simplest option, involving few changes to the rest of the intelligence community. A group of six experienced intelligence and national security experts, writing in *The*

*Economist*, argued for this approach.[3] The *WMD Commission Report* also supported such a change, proposing that the counter-terrorism, counter-intelligence, and intelligence services of the FBI be combined to create a new National Security Service.[4]

Critics, however, argued either that such a change was unnecessary because the FBI was already transforming itself into an intelligence-driven agency, or that it would be a dangerous move because the FBI was likely to remain primarily a law enforcement organization, unsuited to the intelligence mission and inclined to use its increasing intelligence and surveillance powers at the risk of civil liberties.

Another idea was to create a new intelligence agency under the newly created Department of Homeland Security (DHS). Federal Judge Richard Posner, for example, argued for such an organization, to be called the Security Intelligence Service, with the head of this agency to be dual-hatted as the DNI's deputy for domestic intelligence.[5]

The idea that was most often talked about was to create a wholly new, independent organization, possibly modeled on the British MI-5 (which is officially known as the Security Service). Supporters of the idea noted that most Western countries have some sort of domestic intelligence agency. In Britain MI-5 collects and analyzes domestic intelligence, but it has no police power or arrest authority; foreign intelligence in the British system is handled by MI-6, the Secret Intelligence Service.[6] Critics argued that the MI-5 model was unlikely to be applicable to the US because Britain is a much smaller, more centralized country with fewer local police forces and a powerful Home Office, while the US is much larger and decentralized, with thousands of independent local police and sheriff's departments.

Experts also examined domestic intelligence models from other countries, including Australia, India, France, and Germany.[7] Other than MI-5, the model most often pointed to as appropriate for the US was the Canadian Security Intelligence Service (CSIS). The CSIS was established relatively recently (1984), after the Canadian national police force (the Royal Canadian Mounted Police) was found to have broken the law and violated civil liberties in dealing with Quebec separatist groups and other internal threats.[8]

Support for a new domestic intelligence agency was never as strong as it had been for other major reforms such as the establishment of a Director of National Intelligence. The 9/11 Commission recommended against creating such a new agency, and although discussion continues about whether or not the nation's domestic intelligence structure is adequately organized, there seems to be little impetus for setting up a US version of MI-5.[9]

The most extensive study of the question was conducted by RAND, at the request of the Department of Homeland Security, and resulted in three volumes of reports.[10] RAND was specifically not asked by DHS to offer recommendations, but these reports can hardly be seen as ringing endorsements for the idea of a new domestic agency. When the RAND researchers surveyed a group of experts, most expressed the view that the current organization for domestic intelligence wasn't very good; but they also said they did not think that any reorganization was likely to improve the situation.[11] Gregory Treverton summed up the study this way: "Caution and deliberations are the watchwords for this study's conclusions."[12]

## CURRENT DOMESTIC INTELLIGENCE ORGANIZATION

In its analysis for DHS, RAND outlined what it called the "domestic intelligence enterprise."[13] This enterprise encompasses a complex system that includes counterterrorism organizations led by the NCTC; other federal-level organizations and efforts, including those within the FBI, DHS, and Department of Defense; and state, local, and private sector activities. Some of the experts consulted by RAND saw this domestic intelligence enterprise as problematic because it was uncoordinated and thus potentially ineffective; one described domestic intelligence as "a pickup ballgame without a real structure, leadership, management, or output."[14] But even though our domestic intelligence system may not have a centralized structure, it is more coordinated and also more effective than

most Americans realize, and constitutes a de facto – but little understood – domestic intelligence system.

It is difficult, if not impossible, for the American public to accurately gauge the size of the country's domestic intelligence effort. Much of that effort is deservedly kept secret, as is the overall scope of America's intelligence activities at home and abroad. The size of the national intelligence community is not precisely known, but in 2009 then-Director of National Intelligence Dennis Blair described it as a 200,000-person, $75 billion per year enterprise.[15] By the next year the intelligence budget had grown to $80.1 billion. That number is believed to be twice what it was in 2001, and it is considerably more than the $53 billion spent on the Department of Homeland Security in 2010.[16]

An investigation into the country's intelligence and counterterrorism structure by *The Washington Post* described what it called "a Top Secret America hidden from public view and lacking in thorough oversight."[17] The *Post* found that some 854,000 people hold top secret security clearances, and that at least 263 government agencies and organizations had been created or reorganized as a response to 9/11.

The office of the DNI is itself a large entity, with some 1,800 employees as of 2010, and has come to be considered one of the seventeen top-level agencies of the intelligence community.[18] Within the Department of Homeland Security there are at least nine separate intelligence elements, including the Office of Intelligence and Analysis and intelligence organizations of six separate DHS components: Customs and Border Protection, Immigration and Customs Enforcement, Citizenship and Immigration Services, Transportation Security Administration, the Coast Guard, and the Secret Service.[19]

Since 9/11 the FBI has greatly increased the priority it gives to intelligence and counter-terrorism, setting up a new National Security Branch, increasing the number and status of its intelligence analysts, and establishing Field Intelligence Groups in each of its fifty-six field offices. The FBI has also been busy developing new networks of informants within the United States: its 2008 budget request said that it "recruits new CHS [confidential human sources] every day," and needed more money to do it, with apparently 15,000 sources needing to be validated.[20]

Some elements of national and military intelligence have become more involved in domestic surveillance since 9/11. The National Security Agency (NSA), for example, which was revealed in 2005 to have been involved in what was called the Terrorist Surveillance Program, reportedly continues to conduct a significant amount of domestic intelligence collection.[21] As an indication of the growth in the NSA's business – although presumably much of the growth is in foreign intelligence – the agency is building a new data storage center in Utah that will reportedly cost $1.7 billion and occupy as much as one million square feet of space, larger than the US Capitol building.

Some domestic counterintelligence activities of the Department of Defense have drawn criticism since 9/11, in particular the now-defunct Counterintelligence Field Activity (CIFA). But in general, military and other national security intelligence capabilities have not been utilized domestically to any great degree, because of civil liberties concerns as well as Posse Comitatus restrictions on the use of military personnel for law enforcement. For example, an effort to establish a National Applications Office (NAO) to coordinate the domestic use of reconnaissance satellites failed after members of Congress opposed it.[22] And the US Northern Command, established after the 9/11 attacks to coordinate US military support for homeland defense and security, has been careful to focus most of its intelligence efforts toward homeland defense – focusing on threats from outside the US – and takes a very limited role in domestic intelligence and surveillance (such as helping to coordinate reconnaissance assets when needed to support state and federal authorities following emergencies such as the Gulf oil spill and Hurricane Katrina).

Another area where military capabilities have not seen widespread domestic use is with unmanned aerial vehicles, or UAV. Although UAV have become a mainstay of US military operations overseas, they are little used within the US, even by civilian authorities. United States Customs and

Border Protection does operate small numbers of UAV along the country's northern and southern borders, and a few local law enforcement agencies have experimented with the technology, but they remain an underutilized capability.[23]

A growth area for intelligence since 9/11 has been in the development of national intelligence centers, combining and coordinating efforts of a wide variety of organizations on specific problems. In some cases these centers are new, such as the National Counterterrorism Center and the National Counterproliferation Center. In other cases already existing intelligence organizations have been redesignated as national centers, such as the National Maritime Intelligence Center at Suitland, Maryland, and the National Center for Medical Intelligence at Fort Detrick, Maryland.

There are a number of other new or growing federal intelligence agencies and organizations, including the El Paso Intelligence Center (EPIC), a multi-agency counter drug center run jointly by the DEA and DHS, and the interagency National Gang Intelligence Center. There are also operational organizations that are significant users of intelligence, including the 106 FBI-led Joint Terrorism Task Forces that are critical tools in combating domestic terrorism, and High Intensity Drug Trafficking Area (HIDTA) Intelligence and Investigative Support Centers, which are counter-drug efforts sponsored by the Office of National Drug Control Policy.[24] There are also two Joint Interagency Task Forces (JIATFs), one in Hawaii and the other in Key West, Florida, which are interagency counter-drug organizations nominally under Department of Defense control.

At the next level down from the federal level of intelligence is a network of seventy-two state and local intelligence fusion centers. These centers receive DHS funding and support, and many of them have a DHS intelligence liaison officer assigned to them full time, providing analytical support and reach-back capability to DHS headquarters. These fusion centers are not widely known, but they have had some notable successes in helping to prevent terrorist attacks and assisting law enforcement agencies in capturing criminals.[25]

These fusion centers, however, have also generated controversy.[26] The American Civil Liberties Union argues that:

> The federal government's increasing efforts to formalize, standardize, and network these state, local, and regional intelligence centers – and plug them directly into the intelligence community's Information Sharing Environment – are the functional equivalent of creating a new national domestic intelligence agency that deputizes a broad range of personnel from all levels of government, the private sector, and the military to spy on their fellow Americans.[27]

Bruce Fein, a lawyer and former federal official who is a frequent government critic, testified before the House Homeland Security Committee that the US "should abandon fusion centers that engage 800,000 state and local law enforcement officers in the business of gathering and sharing allegedly domestic or international terrorism intelligence."[28]

The best known of these state and local organizations is actually not part of the national fusion center network: the New York Police Department's intelligence division.[29] The NYPD intelligence effort includes liaison officers in some eleven countries overseas, analysts who reportedly speak more languages than can be found in the New York office of the FBI, and even a program that takes police recruits out of the police academy and places them in undercover positions, in some cases conducting investigations inside mosques in the New York City area.[30]

## BALANCING SECURITY AND LIBERTY

The 9/11 Commission argued that we should not have to trade security for liberty, calling the choice between the two a "false choice."[31] But it seems that the balance and the tradeoff are very real today. There is nothing new in this: as a RAND study notes, "Throughout US history, in times of national security crisis, civil liberties have been curtailed in exchange for perceived greater security, the balance between liberties and security generally being restored after each crisis."[32] What is new today, ten years after the 9/11 attacks, is that

the balance has not yet been restored, and in some ways the balance continues to shift toward greater governmental power.

In some cases, this increased government authority is obvious: more intrusive screening at airports, for example, continues the tilt toward greater security at the expense of liberty (and occasionally, dignity). In other cases, the greater powers of government are less evident. As an example, there is a great deal of attention paid today to the previously little-known Foreign Intelligence Surveillance Court (FISC), which is empowered to issue warrants for domestic searches and surveillance under the Foreign Intelligence and Surveillance Act (FISA). But while fewer than fifty FISA orders were issued in 2006, during that same year the FBI issued more than 28,000 of what are called National Security Letters (NSLs), which can authorize search or surveillance of US persons but do not require review by a court or judge.[33] In 2010 the FBI made 24,287 NSL requests pertaining to US persons, but only 1,579 applications to the FISC for surveillance and search authority.[34]

The FBI is expanding its domestic intelligence and surveillance operations in other ways, as well. It is changing its own internal rules to give its agents more leeway to conduct investigations and surveillance, such as by searching databases or sorting through a person's trash.[35] And it appears to be making greater use of undercover informants in intelligence investigations, leading in some cases to successful arrests and prosecutions, but in others to controversy.[36]

One of the most controversial aspects of domestic intelligence after 9/11 was the Patriot Act, which significantly expanded the ability of government authorities to collect information within the US and lowered the "wall" separating criminal investigation from foreign intelligence gathering. In the years since it was first passed several of the Patriot Act's provisions have been renewed, adding tighter controls of government activity. But in general the government has retained its increased authorities. Several of these provisions, which had been scheduled to "sunset," or expire, were renewed in May 2011, with the renewal receiving as much attention for the way it happened – President Obama, who was in Europe, authorized the use of an autopen machine to sign the bill into law – as for the fact that it occurred at all.[37]

Because so much of intelligence work – including domestic intelligence – needs to be hidden from view, a considerable amount of secrecy might be acceptable as long as the American public could be confident that its legislators or others were watching out for the public. As Gregory Treverton writes, "The public doesn't need to know the details of what is being done in its name. It does need to know that some body independent of an administration does know and does approve."[38] The problem is that Congressional oversight of intelligence matters is widely regarded as weak, and much of the day-to-day supervision of intelligence agencies is conducted by organizations such as the National Security Council, the Office of Management and Budget, and agency inspectors general. Such oversight is often useful, but it still means the Executive Branch is supervising itself.

Concerns over oversight of the national intelligence community are heightened when the focus shifts to state and local intelligence efforts. Although most local fusion centers receive federal funds and receive operating guidelines from DHS and the Department of Justice, they are under state or local control and as such are not subject to any strong, centralized oversight. And programs such as the Nationwide Suspicious Activity Reporting Initiative, which is being implemented in cities and states around the country, show great potential for helping to prevent terrorist attacks and detect other criminal activity, but they also raise questions about civil liberties.[39]

Critics argue that in the past ten years the balance between security and liberty his shifted far too much toward security, leading to a great increase in government power. In the words of Laura Murphy of the ACLU, "It feels as though scissors have cut out whole portions of our liberties in the name of fighting the war on terrorism."[40] This may be an overstatement, but it does seem clear that the development of a vast domestic intelligence structure since 9/11 has moved the balance quite firmly in the direction of more security, and less liberty.

## CONCLUSION: WHERE TO FROM HERE?

By its very nature, domestic and homeland security intelligence is intrusive and risks infringing on civil liberties. As then-Secretary of Homeland Security Michael Chertoff put it:

> Intelligence, as you know, is not only about spies and satellites. Intelligence is about the thousands and thousands of routine, everyday observations and activities. Surveillances, interactions – each of which may be taken in isolation as not a particularly meaningful piece of information, but when fused together, gives us a sense of the patterns and the flow that really is at the core of what intelligence analysis is really about.[41]

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

Unless the threat situation changes dramatically, we are not likely to see a new American domestic intelligence agency anytime soon. In the place of an "American MI-5," however, a huge and expensive domestic intelligence system has been constructed. This system has thus far succeeded in keeping America safer than most experts would have predicted ten years ago, but it has also reduced civil liberties in ways that many Americans fail to understand. Precisely because it was unplanned and is decentralized, this domestic intelligence system has not received the oversight it deserves. In the long run, American liberty as well as security will gain from a fuller discussion of the benefits and risks of homeland security intelligence.

## ABOUT THE AUTHOR

***Erik J. Dahl*** *is assistant professor of national security affairs at the Naval Postgraduate School in Monterey, California, and a faculty member of the Center for Homeland Defense and Security. His research focuses on intelligence, terrorism, and international and homeland security, and he is currently writing a book titled Preventing Surprise Attack: Intelligence Failure and Success from Pearl Harbor to the Present.*

[1] See for example James Burch, "Intelligence and Homeland Security," in *Intelligence: The Secret World of Spies, An Anthology*, 3rd ed., Loch K. Johnson and James J. Wirtz, eds. (NY: Oxford University Press, 2011), 499-516.

[2] Although this essay focuses on domestic intelligence, the debate over the balance between security and liberty touches on many other issues including the proper handling and treatment of terrorism suspects, enhanced interrogation and torture, and overseas military operations such as targeted killings. For discussion of some of these broader issues, see the hearing on "Civil Liberties and National Security" before the House Judiciary Committee Subcommittee on the Constitution, Civil Rights, and Civil Liberties, December 9, 2010, http://judiciary.house.gov/hearings/hear_101209.html.

[3] "America Needs More Spies," *The Economist*, July 12, 2003.

[4] Commission on the Intelligence Capabilities of the United States Regarding Weapons of Mass Destruction (the Silberman-Robb Commission), *Report to the President of the United States* (March 31, 2005), 465, http://www.fas.org/irp/offdocs/wmd_chapter10.pdf.

[5] Posner is a prolific writer on intelligence (and other topics). See for example his "Remaking Domestic Intelligence," American Enterprise Institute working paper #111, June 20, 2005, http://www.aei.org/docLib/20050621_DomesticIntelligence3.pdf.

[6] For background on MI-5 see Todd Masse, *Domestic Intelligence in the United Kingdom: Applicability of the MI-5 Model to the United States* (Washington, DC: Congressional Research Service, May 19, 2003).

[7] Burch, "Intelligence and Homeland Security"; Brian A. Jackson, ed., *Considering the Creation of a Domestic Intelligence Agency in the United States: Lessons from the Experiences of Australia, Canada, France, Germany, and the United Kingdom* (Santa Monica, CA: RAND, 2009).

[8] Gregory F. Treverton, *Intelligence for an Age of Terror* (NY: Cambridge University Press, 2009), 127. Richard Posner also sees value in the CSIS model; see his "Remaking Domestic Intelligence," cited above.

[9] An example of the continuing discussion about domestic intelligence is Eric Rosenbach and Aki Peritz, "Domestic Intelligence," Belfer Center for Science and International Affairs Memorandum, Harvard Kennedy School, July 2009, at http://belfercenter.ksg.harvard.edu/publication/19152/domestic_intelligence.html.

[10] Brian A. Jackson, ed., *The Challenge of Domestic Intelligence in a Free Society* (Santa Monica, CA: RAND, 2009); Jackson, *Considering the Creation of a Domestic Intelligence Agency in the United States*; and Gregory F. Treverton, *Reorganizing U.S. Domestic Intelligence: Assessing the Options* (Santa Monica, CA: RAND, 2008).

[11] Treverton, *Reorganizing U.S. Domestic Intelligence*, chap. 5.

[12] Treverton, *Reorganizing U.S. Domestic Intelligence*, 101.

[13] Jackson, *The Challenge of Domestic Intelligence,* Figure 3.1, p. 52.

[14] Ibid., note 14, p. 72.

[15] Siobhan Gorman, "Spy Chief Says U.S. Hunting al Qaeda More Effectively," *The Wall Street Journal*, September 17, 2009.

[16] Ken Dilanian, "U.S. Reveals Skyrocketing Cost of Intelligence Gathering Since 9/11 Attacks," *Los Angeles Times*, October 28, 2010.

[17] Dana Priest and William M. Arkin, "A Hidden World, Growing Beyond Control," *The Washington Post*, July 19, 2010.

[18] The personnel figures were noted in a speech by David R. Shedd, the Deputy Director of National Intelligence for Policy, Plans, and Requirements, in April 2010: http://www.dni.gov/speeches/20100406_2_speech.pdf. It should be noted that the current DNI, James Clapper, has said he intends to streamline the office.

[19] Mark A. Randol, "The Department of Homeland Security Intelligence Enterprise: Operational Overview and Oversight Challenges for Congress," Congressional Research Service, March 19, 2010.

[20] Federal Bureau of Investigation, *FY 2008 Authorization and Budget Request to Congress*, 4-23 and 4-24, at http://www.justice.gov/jmd/2008justification/pdf/33_fbi_se.pdf. See also the Federation of American Scientists Secrecy News Blog, "The FBI as an Intelligence Organization," August 27, 2007, http://www.fas.org/blog/secrecy/2007/08/the_fbi_as_an_intelligence_org.html.

[21] Siobhan Gorman, "NSA's Domestic Spying Grows as Agency Sweeps Up Data," *Wall Street Journal*, March 10, 2008.

[22] Jeffrey T. Richelson, "The Office That Never Was: The Failed Creation of the National Applications Office," *International Journal of Intelligence and Counterintelligence* 24, no. 1 (2011): 68-118.

[23] Chad C. Haddal and Jeremiah Gertler, *Homeland Security: Unmanned Aerial Vehicles and Border Surveillance* (Washington, DC; Congressional Research Service, July 8, 2010); Peter Finn, "Domestic Use of Aerial Drones by Law Enforcement Likely to Prompt Privacy Debate," *The Washington Post*, January 23, 2011.

[24] The HIDTA program is a combined effort of federal, state, and local law enforcement authorities covering at least part of forty-five states. As of 2010, there were thirty-two Intelligence and Investigative Support Centers in the program. See Office of National Drug Control Policy, *High Intensity Drug Trafficking Areas Program Report to Congress* (June 2010), http://www.whitehousedrugpolicy.gov/pdf/hidta_2010.pdf.

[25] The Colorado Information and Analysis Center (CIAC), for example, was recognized as the Fusion Center of the Year in February 2010 for its support to the Najibullah Zazi terrorism investigation, and more recently it provided information that helped lead to the arrest of a bombing suspect; see "Fusion Centers: Empowering State and Local Partners to Address Homeland Security Issues," DHS blog July 18, 2011, http://blog.dhs.gov/2011/07/fusion-centers-empowering-state-and.html.

[26] Ken Dilanian, "Fusion Centers Gather Terrorism Intelligence—and Much More," *Los Angeles Times*, November 15, 2010.

[27] Mike German and Jay Stanley, "Fusion Center Update," American Civil Liberties Union, July 2008, http://www.aclu.org/pdfs/privacy/fusion_update_20080729.pdf.

[28] Bruce Fein, statement before the Subcommittee on Intelligence Sharing and Terrorism Risk Assessment, House Committee on Homeland Security, hearing on "The Future of Fusion Centers: Potential Promise and Dangers," April 1, 2009, http://hsc-democrats.house.gov/hearings/index.asp?ID=186.

[29] Alan Feuer, "The Terror Translators," *New York Times*, September 17, 2010.

[30] Tom Hays, "FBI No-show in NYC Terror Probe Raises Questions," Associated Press, May 14, 2011.

[31] The National Commission on Terrorist Attacks Upon the United States, *The 9/11 Commission Report, authorized ed.* (New York: Norton, 2004), 395.

[32] Genevieve Lester, "Societal Acceptability of Domestic Intelligence," in *The Challenge of Domestic Intelligence in a Free Society*, Brian A. Jackson, ed., (Santa Monica, CA: RAND, 2009), 90.

[33] U.S. Department of Justice Office of the Inspector General, *A Review of the FBI's Use of National Security Letters: Assessment of Corrective Actions and Examinations of NSL Usage in 2006*, 108, http://www.justice.gov/oig/special/s0803b/final.pdf). See also Edward C. Liu, *Amendments to the Foreign Intelligence Surveillance Act (FISA) Extended Until June 1, 2015* (Washington, DC; Congressional Research Service, June 16, 2011).

[34] See "Domestic Intelligence Surveillance Grew in 2010," entry in the Federation of American Scientists Secrecy News blog, http://www.fas.org/blog/secrecy/2011/05/2010_fisa.html.

[35] Charlie Savage, "F.B.I. Agents Get Leeway to Push Privacy Bounds," *New York Times*, June 13, 2011.

[36] Jerry Markon, "Tension Grows Between Calif. Muslims, FBI after Informant Infiltrates Mosque," *Washington Post*, December 5, 2010.

[37] The three provisions were technically amendments to the Foreign Intelligence Surveillance Act (FISA); two had been originally enacted as part of the Patriot Act, and one had been included in the Intelligence Reform and Terrorism Prevention Act of 2004. For background see Liu, *Amendments to the Foreign Intelligence Surveillance Act*.

[38] Gregory Treverton, "Intelligence Test," *Democracy* 11 (Winter 2009): 65, http://www.democracyjournal.org/11/6667.php.

[39] John Farmer, Jr., "How to Spot a Terrorist," *New York Times*, September 28, 2010.

[40] Laura W. Murphy, "Stopping the Flow of Power to the Executive Branch," testimony before the Subcommittee on the Constitutions, Civil Rights and Civil Liberties, Committee on the Judiciary, U.S. House of Representatives, December 9, 2010.

[41] "Remarks by the Secretary of Homeland Security Michael Chertoff," Bureau of Justice Assistance, March 14, 2006, at http://www.dhs.gov/xnews/speeches/speech_0273.shtm.

# Preventing the Next 9/10: The Homeland Security Challenges of Technological Evolution and Convergence in the Next Ten Years

Rodrigo Nieto-Gómez

The September 10, 2001 edition of *Time* magazine dedicated its cover story to Colin Powell and his "megastar wattage … curiously dimmed" inside of the Bush administration. Of course, no one knew that at that precise moment all the human and technological components for the worst attack ever committed on United States soil were already in place, and imminent danger existed. Discussing General Powell's role inside the White House was a good cover story for September 10th.

Then came the attacks of September 11, 2001 – 9/11.

The catastrophic event occurred without warning. The attacks seemed like a random and unpredictable occurrence; a black hole in our cognition.

But obviously, 9/11 was a complicated event that required the use of many previous steps, many technologies in concert, and many brains working together to achieve that particular end. What we saw that day was only one more step (not even the culmination) of a very long series of converging processes – a deviant result of the innovation process that also fuels progress inside our technologically dependent civilization.

On September 12, 2001 a still perplexed world asked how was it possible that the terrorists' attacks were not stopped; all the clues were there, the dots were waiting to be connected and al Qaeda had already been active and recognized as a threat by the federal government since the 1990s.

On September 14, 2001 *Time* had a new cover. It featured a collapsing World Trade Center – an avalanche of dust, steel and glass.

But if 9/11 was just the visible part of a longer process, were did it all start?

The historic account of the *9/11 Commission Report* finds the roots of 9/11 in the rise of a national resistance against the communist government of Afghanistan in 1978, which would eventually lead to the formation of al Qaeda[1].

I argue that the patterns that lead to 9/11 are much older, but at the same time they are considerably less linear. Therefore, that direct line that the *9/11 Commission Report* traced is nothing more than an illusion produced by what Nassim Taleb calls the retrospective distortion, "or how we can assess matters only after the fact, as if they were in a rearview mirror (history seems clearer and more organized [linear] in history books than in empirical reality)."[2]

This retrospective distortion creates a security ecosystem where homeland security practitioners feel pressured to try to "connect the dots" every time, instead of adapting to an environment of emerging patterns and mutating dots that cannot be connected.

Moreover, certain technologies have been doubling in capacity every few months for many years now and, as a consequence, technology improvement cycles have also shrunk. We have grown used to having a new and improved version of a product that is twice as powerful in just a few months, and radical disruptive propositions every year or two. Because of technological convergence, it is very hard to predict what unintended consequences all those improvements and new technologies will have once they are recombined with others, and what catastrophic possibilities convergence might have that we will miss on the next 9/10. This is the chaotic security environment where homeland security operates today. For the next ten years, homeland security should embrace it.

## 9/11/1973: Why Not?

Romance languages, as well as German, have introduced the neologism of "uchronia" (from *uchronie* in French) in their vocabularies to define the subgenre in fiction where reality as we know it is profoundly altered by a change

in the chain of events. They describe a time that does not exist, or a non-time. In an uchronic novel, reality it is indistinguishable to ours until an event – often called a "point of divergence" or a "Jonbar Hinge" – triggers a series of second and third level consequences that end up creating a reality that it is almost unrecognizable from ours, even though initial conditions were identical.

In Turtledove's novel *How Few Remain*, the south won the American Civil War because of an accidental recovery of a document; in *The Man in the High Castle*, by Phillip K. Dick, a successful assassination plot against President Roosevelt creates an environment that ends up being favorable to the axis powers, who end up winning World War II.

Uchronias make interesting readings (or movies, although some people have trouble enjoying the convoluted plots of time paradox films) because they describe contextual patterns that we all recognize and are familiar with. Then, after a fictional "point of divergence", second and third degree consequences create a believable new environment that is almost unrecognizable from reality as we know it, but that we can accept as a plausible "what if." Uchronias confront us with the fragility of reality and the power of the randomized and chaotic forces that surround us. They contradict the linear nature of historic events; show us how precarious and fluid are "the dots" that have to be connected, and how organic is the nature of any threat. If the briefcase bomb would have been a little to the left (or to the right… who knows?), Hitler would have died; if one of many things described in the *9/11 Commission Report* would have happened (or not happened) on 9/10, we would have continued the discussion about Collin Powell on 9/12.

The innovation cycle is "pushing" Jonbar Hinges on society faster than ever before. Each new or improved technology adds a new series of combinatorial possibilities that can shape society in unpredictable ways. Many technologies today are nothing other than backbones designed to support spontaneous innovation – touch screen blank slates for others to design their apps, in an emerging cycle that feeds on itself.

Millions of people potentially empowered by those backbone technologies mean millions of potential innovators all thinking and doing things that have not been thought or done before.

But those innovations do not happen in a vacuum. Instead, as Brian Arthur explains:

> New technologies in time become possible components – building blocks – for the construction of further new technologies. Some of these in turn go on to become possible building blocks of yet newer technologies. In this way, slowly, over time, many technologies form from an initial few, and more complex ones form using simpler ones as components. The overall collection of technologies bootstraps itself upward from the few to the many and from the simple to the complex. We can say that technology creates itself out of itself. [3]

Ideas – or memes, as evolutionists like to call them – evolve from the simple to the complex. They progress in the sense that whatever was there before will be constantly improved and recombined with new thoughts and ideas making something better that can then be used again to continue this incessant process.

Unfortunately, innovation has a dark side. The same accelerated combinatorial evolution that empowers entrepreneurs to rapidly improve our high tech environment can, and often is, used to harm the innocent.

In fact, I believe 9/11 was the product of thousands of years of innovation in a radical, deadly, and novel way.

The innovative recombination of technology that made those terrorist attacks possible took advantage not only of the knowledge and imagination of Khalid Sheik Mohammed and Osama Bin Laden, but also of Minory Yamasaki (the WTC architect); the ingenuity of the Wright brothers and all the aviation heroes who made flying machines a reality; the hundreds of engineers form Boeing; and, in general, thousands of years of accumulated human knowledge (material engineering, tube frame design, Le Corbusier modernist philosophy, and thousands more innovations, all the way back to the wheel, language and the invention of tools!).

In Uchronia, 9/11/2001 could have occurred on 9/11/1973, just a few months after the ribbon cutting ceremony of the

World Trade Center. By that time, jumbo jets were flying, the Pentagon had been built, and most of the technology that was materially used during 9/11 existed, ready to be recombined in order to achieve a catastrophic result.

But if the technology already existed in 1973, the "9/11 idea" did not. Creativity does not evolve following a linear path of dots and many things had to happen for this complex adaptive environment to evolve towards a state where 9/11 went from being a possibility that lurked in the dark since 1973, to a sad meme of human innovation [4].

That is the paradox. We can easily imagine "planes as weapons" as the *9/11 Commission Report* asked. The meme requires the recombination of just a few previously known ideas: suicide militants, planes, volatile jet fuel, and skyscrapers. But the same thing can be said for Facebook (it is not hard today to imagine an interconnected personal database), Amazon (an online-only retail store), or Netflix (a mail-based rental model that combined the backbone of the postal service with the Internet). Yes, we can imagine all that, but someone imagined it first, recombined technologies and created huge companies out of it. We can all imagine an iPad, but Steve Jobs and the rest of the Apple designers imagined and successfully implemented it first.

Innovation is innovation not because it is impossible to think of something, but because no one else thought of it before.

## WE DON'T REINVENT THE WHEEL – WE APPROPRIATE IT!

Ted Lewis identified the importance of "stigmergy" in the invention-innovation cycle: "invention [works] as the stimulus and innovation as the response. After each cycle, the stimulus-response pattern repeats." [5]

I agree with him that "stigmergic" behavior is one of the patterns that govern the combinatorial evolution process of innovation and the technological environment. Lewis established the reciprocal need inventors and innovators have for each other in a stimulus-response cycle loop, but I believe that there is a third key actor in the invention-innovation cycle: the adopter of the technology. Inventors, innovators, and adopters stimulate each other. Although most adopters will be fairly passive actors, some will adapt the technology to be used as something that neither the inventor nor the innovator thought it could be used for, in a process that Dix refers to as appropriation. [6]

I am convinced that all innovators are also active appropriators – they appropriate existing technologies for their new designs, using them in unanticipated ways.

For example, the designers of the Chevy Volt did not have to reinvent the wheel or velour interiors. On the other hand, I am sure that the inventors of the wheel or the so-called "faux velvet" did not envision an electric car as one of the applications of their technological innovations (none of them knew what electricity or cars would be!). Progressive innovation requires the appropriation of previous technologies to be used differently from what the original designer anticipated.

When a clandestine actor uses infrastructure to do harm, he or she illicitly appropriates the technology to achieve a goal different from what the designers intended. In the online world, we give the name of hacking to that behavior. In the real world, terrorists hack our high tech society every time they are successful and the acceleration of technological development provides the illicit appropriator more building blocks and more possibilities to combine them every day. Combinatorial evolution creates unforeseen convergence that gives to the inventor-innovator-appropriator cycle more uchronic choices.

Terrorism is a technological artifact that results from the appropriation of systems through combinatorial evolution. Forecasting every possible innovation in this context is impossible.

Consequently, while it seems like an easy challenge to imagine planes as weapons (in fact Tom Clancy wrote an almost uchronic novel out of this exact idea), Taleb reminds us "had the risk been reasonably conceivable on September 10, it should not have happened. If such a possibility were deemed worthy of attention, fighter planes would have circled the sky above the twin towers, airplanes would have had locked bulletproof

doors, and the attack would not have taken place, period." He then continues: "something else might have taken place. What? I don't know."[7]

At this precise point, I am sure, many patterns are forming that will create appropriation opportunities in the future, and some of them will be harmful. Which ones will turn out to be relevant? I don't know either.

In this complex adaptive environment of accelerated high tech innovation, the "connect-the-dots" game seems to be the worst possible metaphor. If one has to be found, I would like to offer an "Encrypted letter soup" as a replacement, where all the relevant information of a catastrophic event becomes relevant only after the pattern has been recognized. That is, after the fact.

In this primordial letter soup of catastrophes, the proverbial dots to be connected are encrypted in noise. Worse, because there is no preconceived pattern, the "dots" evolve and change in randomized ways, until one day they acquire meaning.

Connecting every dot is called paranoia. In the case of nation states, institutional paranoia is quite often the foundation of totalitarian regimes that thrive in the waters of the politics of fear.

We cannot anticipate all innovations, and imagination understood as anticipatory forecasting of new threats cannot be bureaucratized.

## CONCLUSION: HOMELAND SECURITY: THE EARLY ADOPTER DISCIPLINE

Combinatorial evolution of technology does not have to favor the illicit appropriator. This randomized environment created by the accelerated pace of technology cycles will favor those who can produce more ideas, and ride the wave of uncertainty instead of opposing it.

While studying the origins of the so-called geniuses, Dean Simonton found that "The more ideas a mind can produce, the higher the odds that those ideas will be original and varied.... Flexibility and originality are both to a very large extent mere consequences of fluency."

His research conclusively demonstrated that:

> The creative process is to a certain extent blind. Even the greatest creators possess no direct and secure path to truth or beauty. They cannot guarantee that every published idea will survive further evaluation and testing at the hands of audiences or colleagues. The best the creative genius can do is to be as prolific as possible in generating products in the hope that at least some subset will survive the test of time.[8]

The homeland security effort for the next ten years must encourage public and private inventors, innovators, and appropriators of new disruptive security ideas to be prolific and then aggregate those efforts. This would allow us to surpass – by a few orders of magnitude – the number of disruptive ideas produced by the clandestine actors.

In the next ten years, the Department of Homeland Security (DHS) should embrace and become the early adopter of almost all new technologies, appropriating them, generating knowledge about them, and proactively thinking how to recombine them with other building blocks in order to make civilization more resilient.

Ten years from now, DHS must be the gold standard of usability labs in order to understand, appropriate, and improve as many new technologies as possible.

We cannot control the complex adaptive environment of technological evolution nor should we try, as positive innovation requires – in Schumpeter's words – creative destruction and chaos.[9] Nevertheless, we can control the government's own pace of innovation, and its rate of technological understanding and adoption.

For the next ten years, the homeland security community should become the most tech-enthusiastic community inside of government. No one – with the probable exception of DARPA – should be more innovative and more "tech savvy" regarding what makes technology usable, why people use a particular technology, and how security can be improved while also improving usability.

In 2021, homeland security should be perceived as a project that has helped

maintain, or even accelerated, the pace of the innovation cycle and not the opposite. A project that has made the backbone of American innovation stronger, more open for positive appropriation, and more resilient for when the unavoidable illicit appropriation does take place.

Homeland security as a doctrine should embrace combinatorial evolution and plan for it. Government projects should be innovative, but also scalable, so they can be adapted to the unexpected, and they should prefer social to centralized deployment of technology. When possible, government should prefer software instead of hardware and off-the-shelf to proprietary. It should also design policy and infrastructure for openness instead of secrecy; there are more good people than bad people, so policies should take advantage of this superiority of numbers and aggregate their knowledge and effort.

Homeland Security technology and strategies (also a social technology) should be easily upgradable. If not, many of them will be will be legacy technology by the time they reach the public. Homeland security decision makers should avoid bloated solutions and examine constantly old security measures to avoid petrifaction. It might even be worthwhile to consider "sunset" security laws and regulations, in order to permanently question if old security layers are still needed in the ever-evolving security environment (we might be able to finally leave our cell phone on during take off…as many iOS users already do, without knowing it![10])

Finally, instead of official futures (we will get them wrong anyway), the homeland security planning process should plan for Uchronia and serendipity. Current scenario planning methodologies are a good starting point, although homeland security practitioners should create their own.

Technological evolution is part of our instinct to explore. It is who we are, and it is part of what makes us better than our previous selves. In 2021, the homeland security project should be the reason why the creative backbone of civilization is stronger and more resilient, so the explorers of tomorrow can perpetuate the very American tradition of thriving in the unknown, pushing the last frontier – the knowledge frontier – further, one innovation at a time.

## ABOUT THE AUTHOR

***Rodrigo Nieto-Gómez*** *is a research professor at the department of National Security Affairs and the Center for Homeland Defense and Security at the Naval Postgraduate School in Monterey, California. His fields of research include border security, the implications of new technologies for security and defense and the geopolitical and strategic implications of homeland security and defense policies.*

[1] The National Commission on Terrorist Attacks upon the United States, *9/11 Commission Report* (July 22, 2004), 47. http://www.9-11commission.gov/.

[2] Nassim Nicholas Taleb, *The Black Swan: The Impact of the Highly Improbable* (Kindle version, 2010).

[3] Bryan Arthur, *The Nature of Technology: What It Is and How It Evolves* (Kindle version, 2009).

[4] The history of aircraft hijacks is the history of a threat evolving from the first hijackings that were conducted by pilots trying to escape from authoritarian communist regimes, to hijacking as an extortion tool, to the first incidents of terrorist sabotage. See: http://fcafa.wordpress.com/2011/03/12/they-flew-to-exile-1950/.

[5] Ted Lewis, *Bak's Sand Pile: Strategies for a Catastrophic World* (Monterey, CA: Agile Press, 2011), 259.

[6] Alan Dix, "Designing for Appropriation," *Proceedings of the BCS HCI 2007 Conference, People and Computers XXI* (London, UK: BCS-eWik), 2, http://www.comp.lancs.ac.uk/~dixa/publist-2007.html.

[7] Taleb, *The Black Swan*.

[8] Dean Keith Simonton, *Origins of Genius: Darwinian Perspectives on Creativity* (Kindle version, 1999).

[9] Joseph Schumpeter might be, from among all the classical economists, the one who best understood the nature of innovation and change. In Schumpeterian terms: "Industrial mutation – if I might use that biological term – that incessantly revolutionizes the economic structure from within, incessantly destroying the old one, incessantly creating a new one. The process of Creative Destruction is the essential fact about capitalism." From: Joseph Alois Schumpeter, *Capitalism, Socialism and Democracy* (Google books version, 2003).

[10] iOS is the operating system that powers most Apple mobile devices, including the iPhone, iPad and iPod Touch. Turning the device off is a two step process that requires that the user hold the off button for four seconds, and then move a virtual button from left to right in the touch screen. I have noticed many times that during take off or landing, when supposedly all electronic devices should be off for the security of the plane, what many iOS users do is to press the off button once. While this behavior darkens the screen, the Apple device is still fully powered. Nevertheless, no accidents have occurred after many years of unintentional violations of the "turn off all electronic equipment" security rule.

# Security Studies: The Homeland Adapts

Stanley Supinski

If there is any advantage to being at war, it is that it creates conditions for exploring new knowledge and gathering disparate players around the flagpole for support.[1] The war and political environment instigated by the events that occurred on Sept 11, 2001 created just such conditions, and academia immediately realized it had an important educational role to fulfill. It was clear from the outset that the nation's capacity to address the overwhelming challenges required for homeland security and defense needed to be significantly bolstered. There were academic programs at the time that focused on terrorism, emergency management, and other related disciplines, but none called "homeland security," and certainly none that covered the wide range of knowledge required. Academia and government joined forces to resolve this intellectual and personnel deficiency and during the past decade homeland security education and research have expanded at a phenomenal rate.

There was historical precedent for leveraging academia to support national needs. During World War II, the scramble to develop an atomic weapon led the government to undertake the Manhattan project, an intellectual and scientific enterprise. Though led by the federal government, academia took on a key role in conducting scientific research and development; their role in this process cannot be understated and the effects were far reaching. Just as significant was academia's part in the Cold War. Education programs aimed directly at supporting that conflict, including those in national security affairs, Eastern European/Soviet area studies, political science, and international relations, flourished nationwide. Academic programs that served to support the war indirectly, such as engineering and basic sciences that built the expertise needed for technological research and development, also expanded. The federal government bolstered these programs with dramatic increases in funding through the National Science Foundation and other means.[2] The Cold War was responsible for an unprecedented growth of academic programs supporting national priorities "both in its material manifestations and through the ideological atmosphere that it was responsible for creating."[3]

The decade since 9/11 has seen a similar response. The federal government and its national security prerogatives helped drive academic priorities, and academia showed that it could rapidly adapt to national needs. The combination of federal support, adaptability, and the intellectual resources that academia provides have resulted in what many view as a new academic discipline.

## A New Requirement – Knowledgeable Homeland Security Professionals

The period immediately following 9/11 saw the enactment of hundreds of statutes and regulations, substantial changes in policy initiatives, the most massive governmental reorganization since 1947, and brought the new business of homeland security to the fore of American consciousness. This new mission set and political environment mandated personnel with an entirely new collection of competencies and knowledge. The new Department of Homeland Security (DHS) required expertise to meld its twenty-two formerly independent agencies into a functional organization. Every federal department assumed new responsibilities; each of the 87,000 government jurisdictions and their entities added homeland security to their mission set; and most major corporations established homeland security offices, all requiring personnel that understood the new way of doing business. Shortly after 9/11, Lee Hamilton, director of the Woodrow Wilson Center for International Scholars, testifying before the Senate Committee on Governmental Affairs recognized that:

> The maintenance of American power in the world depends on the quality of US government personnel, civil and military, at all levels…The US faces a broader range of national security challenges today, requiring policy analysts and intelligence personnel with expertise in more countries, regions and issues…we must take immediate action in the personnel area to ensure that the United States can meet future challenges.[4]

The immediacy of this need made this challenge particularly daunting. Government, academia, and others involved in homeland security did not wait idly by for direction from a coordinating authority to dictate what their programs should look like. In true free enterprise fashion, a wide range of initiatives and approaches were undertaken to address the various aspects of the shortfall, including training, education at both the undergraduate and graduate levels, and various forms of research and technological development. While the effectiveness of the effort to develop homeland security education and training cannot be denied, the lack of a coordinating body, and the inherent breadth of what homeland security entails, has resulted in great inconsistency.

## DEVELOPMENT OF AND INFLUENCES ON THE HOMELAND SECURITY "DISCIPLINE"

The fact that programs do not look alike is not surprising, nor is it necessarily a negative reflection on the homeland security academic community. Various influences have shaped what homeland security education looks like today; government led initiatives, faculty expertise (or lack thereof), and administrative groups have had influence over what and how higher institutions teach.

One example of a government led initiative has been the Center for Homeland Defense and Security (CHDS) at the Naval Postgraduate School, which publishes *Homeland Security Affairs*. CHDS was established in 2002 through a partnership between the Department of Justice, Congress, and the Navy and its sponsorship moved to the new Department of Homeland Security in 2003. This partnership led to the development of the nation's first graduate Homeland Security master's degree program, and other programs emphasizing policy and strategy have used the CHDS curriculum. Additionally, the Center was tasked to use its government funding to assist other academic institutions, at no cost to the institutions, to develop homeland security programs around the country by sharing curriculum advice and course materials.

The Homeland Security/Defense Education Consortium (HSDEC) is an example of an administrative group created to influence homeland security education. In an effort to establish curricular standards, support program development, and provide prospective students with an additional program selection data point, the HSDEC was established by US Northern Command in 2003. The organization morphed into the Homeland Security/Defense Education Consortium Association (HSDECA) and acquired independent, non-profit status in 2007.

A more recent government influence on the shape of homeland security education has come from the Transportation Security Administration's Associates Program. The goal of the program is to generally increase the level of education for TSA personnel, and in particular provide them core homeland security knowledge. At program rollout in the Fall of 2010, the courses were being delivered by twenty-five community colleges in twenty-two states, almost all of which also offered them to their other student populations, especially those in law enforcement, fire science, and related programs. With the expected expansion of the program to all fifty states by the fall of this year, the TSA-driven and funded curriculum will have increased influence at the community college level.

When institutions decide to establish a program, they normally root them in an existing discipline, which offers a pool of potential faculty members and an existing constituency of students and after graduation employers. The majority of homeland security programs in existence today are linked to three primary content areas: public administration, emergency management, or criminal justice. However the breadth of the topic has also led to programs in departments of political science, history, psychology,

public health, law, and many others. For example, The University of Southern California's homeland security certificate is offered within their school of engineering and is influenced by their well-established aerospace program. Penn State's homeland security master's degree is offered within their School of Public Health. With such a disparity of influence, shaped by the unique approach taken by the hundreds of colleges and universities that have zealously pursued developing homeland security related programs, what these programs look like varies significantly across institutions.

In many cases, academic institutions have built these programs for altruistic reasons, but market demands have also exerted a powerful influence. Institutions want to be on the cutting edge of education and support the needs of the job market, but they are also lured by the prospect of high volumes of paying students. The rush to take advantage of the demand has resulted in wide variations in program quality and curriculum, with courses, often taught by faculty with little or no direct professional experience or background. This is also reflected in how programs have been initiated: right after 9/11, most were started bottom-up by individual or groups of faculty members interested in the subject; but as the discipline has evolved, institution administrations have seen the value and program establishment is now more often directed from the top.

So, after ten years, is there a homeland security academic discipline or is it just a collection of components from others? The debate still rages, but considering that it is a branch of knowledge which is taught or researched at over 300 institutions of higher learning, that it is defined by recognized academic journals devoted to the subject, and that there are learned societies and academic departments to which their practitioners belong, it is well on the way. The fact that several schools will be offering doctoral level homeland security programs beginning later this year, including Ole Miss and New Jersey City University, is further testament.

Additionally, although there is no agreement on a standard curriculum or what should or should not be included, ten years after 9/11 a general picture can be drawn. This basic framework, determined by homeland security academics,[5] consists of: current and emerging threats; context and organizations involved; policies, strategies, and legal issues; and processes and management. While this is a pretty generic list, it is the only way to provide an overall summary of what homeland security education looks like. However, this general outline does define the discipline's content, and it affords the flexibility demanded of this very diverse field of study.

## FUTURE CHALLENGES AND CONCLUSION

While many in academia believed that homeland security education, and in fact the term homeland security itself, would be fleeting, the community that has been built is a testament to its value, and there is little doubt that it is here to stay. Nevertheless, making this community a permanent and respected part of the educational and research and development landscape will require more work.

First and foremost, there needs to be agreement on what specific knowledge parameters come with the term "homeland security professional." Despite the various existing influences on the topic, a commonly agreed to core will ensure consistency. Second, a broadly accepted validation authority, in the form of a member run accreditation association, should play a significant role in furthering the discipline. Unless standards are regulated to some degree, inconsistency and examples of poor quality are inevitable. Finally, closely related to the first two issues, is the need to develop a cadre of qualified faculty and researchers. The development of research PhD programs in homeland security, already begun, should address this issue in the long term.

The final question is just how much of a role should government have in the march toward a discipline? Government programs and legislation will always serve to sway the direction academia takes. The shift after Hurricane Katrina from an almost exclusive focus on terror to all hazards was certainly reflected in academic programs. However, shaping academic efforts should not go any further: government's role is to nurture, not to prescribe. We have gone in many

directions as we have developed our programs, and those directions are marked with both successes and failures. But the independence and autonomy of the universities, and those working within all settings of higher learning, must be maintained. Decisions regarding curricular content and assessments of academic excellence must come from within these institutions and from the accreditation procedures and bodies they construct.[6] As our profession of homeland security continues to evolve, these bodies must become more active participants in the standard setting process.

The team effort by government and academia has contributed to developing the knowledge and resource base needed to handle all-hazards homeland security, but educating a workforce and populace is a long-term process. Our terrorist adversaries have shown they have the patience to make this a long-term struggle, and the number of natural hazards we have to contend with continues to climb. Only education can ensure we have the fundamental skills and knowledge needed to minimize loss of life and property and handle the long-term threat most effectively. The academic community capitalized on the sense of urgency created by 9/11; maintaining the momentum is an enduring challenge. However, it is a challenge we as a nation must meet. The Honorable Paul McHale, former Assistant Secretary of Defense for Homeland Defense, clearly recognized the value of educating society and the importance of it to our current effort when he stated: "Terrorism will be defeated by intellect, not dogma."[7]

## ABOUT THE AUTHOR

***Stan Supinski, PhD****, is the director of partnership programs and a faculty member for the Naval Postgraduate School, Center for Homeland Defense and Security, and an associate professor at the Long Island University, Homeland Security Management Institute. He founded and formerly directed the Homeland Security/Defense Education Consortium on behalf of NORAD/US Northern Command.*

[1] R.C. Lewontin, "The Cold War and the Transformation of the Academy," in *The Cold War and the University; Toward an Intellectual History of the Postwar Years,* Noam Chomsky, ed. (New York: New Press, 1997), 1-24

[2] The budgets for colleges and universities increased twenty-fold, in constant dollars, from 1946 to 1991.

[3] Lewontin, "The Cold War and the Transformation of the Academy," 2.

[4] L. Hamilton, *Critical Skills for National Security and the Homeland Security Federal Workforce Act* (s.1800), Congressional Testimony 32Y4136771038 (Washington DC: FDCH, 2002).

[5] Two meetings were held by homeland security educators to determine what topics constitute a quality homeland security academic program. The first, looking at graduate level programs, was held at US Northern Command Headquarters in Colorado Springs in Aug 2005. The second, looking at the undergraduate level, was held at the Naval Postgraduate School in June 2009. Each meeting consisted of twenty-five scholars, and the full results of these efforts can be found at www.uapi.us.

[6] Thomas E. Drabek, "Emergency Management and Homeland Security Curricula: Context, Cultures, and Constraints," *Journal of Emergency Management* 4, no. 5 (2009): 33-42.

[7] Mr. McHale's address to a meeting of the Homeland Security/Defense Education Consortium held at the Uniformed Services University for the Health Sciences, November 2004.

# Inter-Organizational Collaboration: Addressing the Challenge

Susan Page Hocevar, Erik Jansen, and Gail Fann Thomas

9/11 and Hurricane Katrina exposed the United States' vulnerabilities within and across organizational and jurisdictional boundaries. A number of breakdowns in collaboration were evident: a lack of information sharing among agencies, confused inter-organizational relationships, competing roles and responsibilities, and shortcomings in leadership.

In response to these inadequacies in collaboration, scholars have engaged in theoretical and empirical work in hopes of preventing another 9/11 and enhancing overall national security. Studies about the need to collaborate have been the most prevalent. Less prevalent are studies about the "how" of collaboration. To address the "how" of collaboration, we wanted to better understand the enablers and barriers to effective inter-agency collaboration. To address this question, we queried and conducted surveys with homeland security managers across a broad range of organizations and agencies to find out what factors contribute to effective collaboration and what factors inhibit collaboration. The resulting model of collaborative capacity is presented here.

## Inter-Organizational Collaborative Capacity (ICC) Model

The response planning and prevention for both man-made and natural disasters are complex problems that require the capabilities of many disciplines that have both aligned and competing interests and usually function without an over-arching command authority. Because of the lack of an integrating hierarchy, organization theory would define this as an "under-designed system." As such, it requires leadership engagement to guide, motivate, and structure the collaborations needed to be successful in the complex homeland security environment.

We define Inter-organizational Collaborative Capacity (ICC) as "the capability of organizations (or a set of organizations) to enter into, develop, and sustain inter-organizational systems in pursuit of collective outcomes."[1]

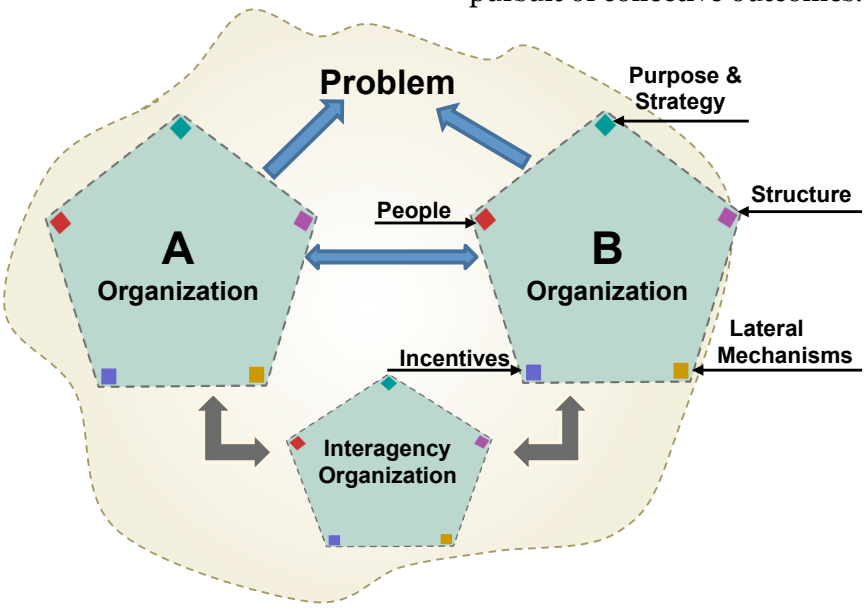


Figure 1: Organizations in a Common Problem Space[2]

Figure 1 illustrates the simplest image of a collaborative context with two participating organizations and an inter-agency organization that share an interest in a problem space. The inter-agency organization can be a temporary task force, convened for a specific time-limited purpose, or a more formally established structure such as an intelligence fusion center. All three organizations depicted have a collaborative capacity that impacts how effectively the problem is addressed. A key assumption of this model is that building collaborative capacity requires deliberate leadership attention and the alignment of organizational design elements toward collaboration. The ICC model provides a mechanism to assess different factors that contribute to an organization's capacity to collaborate with other organizations. It can serve as a framework to diagnose current collaborative capabilities and provide data to guide organizational changes to improve those capabilities. The model is comprised of five organizational domains: Purpose and Strategy, Structure, Rewards and Incentives, People, and Lateral Mechanisms. There are thirteen factors measured by the ICC diagnostic survey that are distributed across the domains of the organizational system as illustrated in Figure 2.

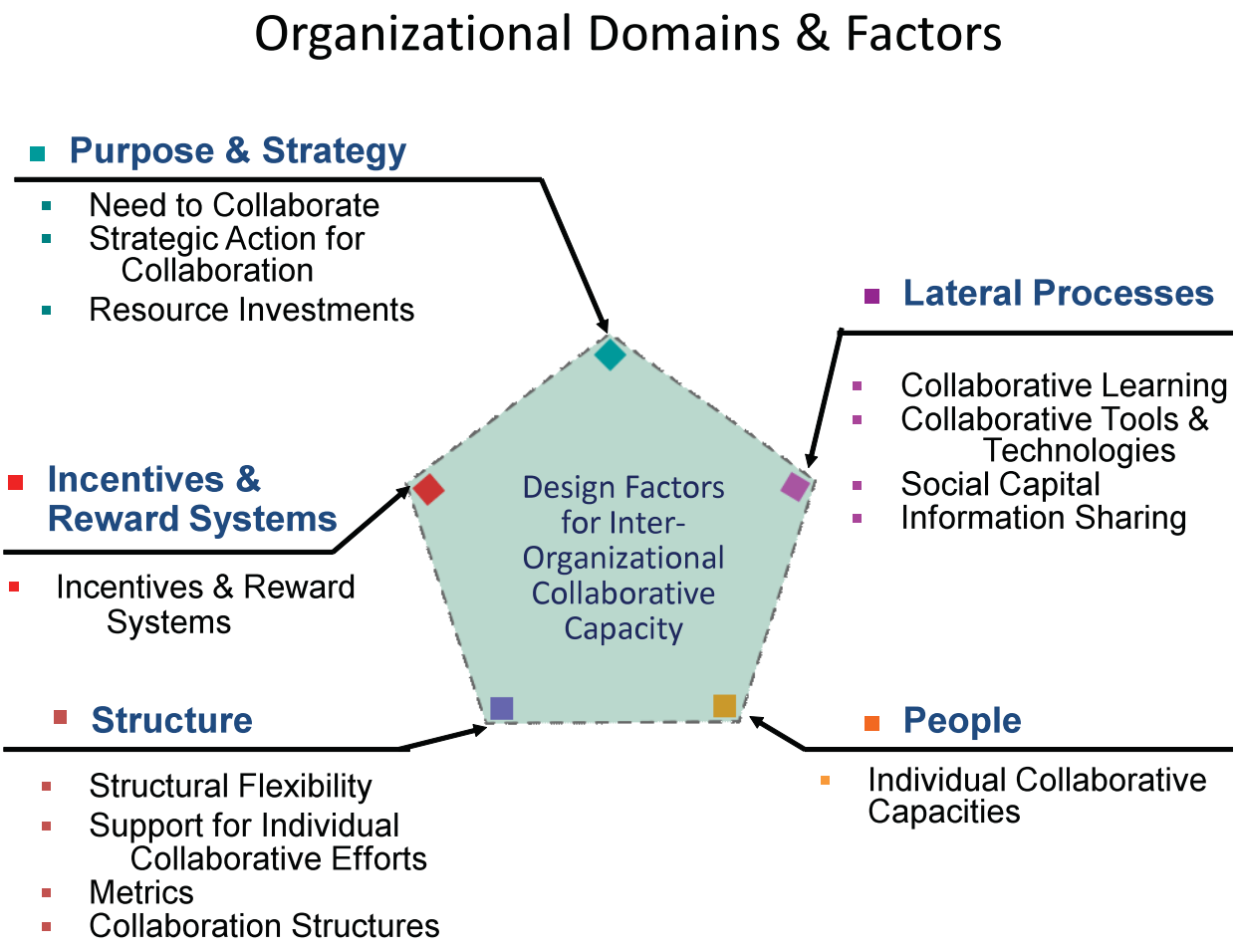


Figure 2: Inter-Organizational Collaborative Capacity Model: Domains and Factors

The ICC model has three factors in the domain of **Purpose and Strategy**: *Felt Need* is the organization's recognition of interdependence with others and the acknowledged need to collaborate in order to effectively accomplish its mission and goals. Felt Need can be derived from a perceived threat or problem and thus emphasizes response capabilities; or it can be motivated by opportunity for pro-action or prevention. *Strategic Actions* include goals for collaboration, demonstrated senior leadership commitment, and the willingness to consider other organizations' interests in planning. The third factor assesses the extent to which the organization makes adequate *Resource Investments* (e.g., budget, personnel) in collaboration. Felt Need to collaborate is typically the initiating factor; but without the additional leadership, planning, and resource commitments, there is inadequate strategic emphasis for building collaborative capacity.

The **Structure** domain is comprised of four factors. *Collaboration Structures* can include liaison roles, participation in inter-agency teams and task forces, clearly established roles for each participating organization, and internal processes that enable effective inter-organizational collaboration. *Structural Flexibility* allows partnerships to adapt as requirements change, demonstrates willingness to adjust procedures to facilitate coordination, and responds to the requirements of other organizations. *Metrics* include established criteria and performance standards for evaluating inter-organizational efforts, and routine mechanisms for assessing outcomes. *Support for Individual Collaboration Efforts* has two facets. The first is how clearly individual collaborative work is structured in terms of clear goals, constraints, and authorities. The second is the strength of the link between personnel in boundary-spanning roles working directly with other organizations and the strategic leadership of their own organization. This is reflected in the extent to which the organization follows through on recommendations of these boundary spanners.

The ICC model focuses on ways organizations align different internal design elements to improve collaboration; thus the **Incentives and Reward Systems** domain considers *Reward Systems* as they impact the organization's personnel. Are employees rewarded for investing time in building collaborative relationships with other organization members and for successful collaborative results? Are collaborative talents and achievements considered when people are reviewed for promotion? There are, of course, external factors that motivate an organization to engage in collaboration (e.g., mandated requirements or financial awards through grants); but these incentives come from the larger organizational context or environment rather than the "managed" reward system inside the organization in the ICC model.

There are four factors that constitute the **Lateral Mechanisms** domain representing both the "hard" and the "soft" aspects of lateral coordination. *Social Capital* represents the social and professional relationships that organizational members have with counterparts in other organizations. It is a basis for awareness and trust building. *Collaborative Tools and Technologies* provide the technical mechanisms for collaboration such as inter-operable information systems and collaborative planning tools. The *Information Sharing* factor represents the organization's norms and values that support information sharing, and the adequacy of access that other organizations have to information relevant to their success in the collaborative activity. *Collaborative Learning* is demonstrated in several ways – joint training, learning about the interests and capabilities (and limitations) of other organizations, and systematic assessment of lessons learned to improve future collaborations.

The **People** domain has only a single factor – *Individual Collaborative Capabilities*. These include the attitudes, skills, knowledge, and behaviors of individual organizational members that impact the organization's ability to collaborate. Examples are conflict management skills, willingness to engage in shared decision-making, respect for the expertise of those in other organizations, and knowledge and understanding of how other organizations work.

## SUPPORTING EVIDENCE FOR COLLABORATIVE CAPACITY FACTORS

Many other scholars have studied the issues contributing to or preventing collaboration. Paul Stockton and Patrick Roberts summarize the findings from a 2008 forum on homeland security convened by Stanford University's Center for International Security and Cooperation (CISAC). They acknowledge the absence of hierarchy that uses a top-down centralized approach to homeland security planning and conclude that the relevant stakeholders (including federal, state, local, and private sector organizations) need to: collectively identify a shared motivation, need and purpose; formulate goals that they will jointly pursue; and use a consensus process for planning the means to accomplish those goals through unity of effort. They also recommend structural mechanisms like an integrated staff organization and the development of doctrine to guide and coordinate operations.[3]

Sharon Caudle cites a study that found the most effective inter-governmental cooperation occurs when participating bodies acknowledge a high level of vulnerability and interdependence and establish formalized partnerships with clear authorities, roles and procedures. She describes additional enabling factors that include: leadership to champion commitment to partnership; governing and decision-making structure; policies, processes and partnership norms; activities to build personal relationships across organizations; strategic goals with designated measures and clearly defined roles, responsibilities and resource commitments; and a performance management system for both organizational and individual-level performance.[4]

Finally, Amy Donahue and Robert Tuohy studied how to better learn from the lessons of disasters. They identify a number of repeating "lessons" that include failed communications, weak planning, uncoordinated leadership, and resource constraints. They propose three recommendations to strengthen the learning process toward actual changes in disaster planning and response practices: (1) recast exercises as learning activities where failures are not punished but used to focus critical analysis; (2) develop robust nation-wide capability to gather, validate, analyze and disseminate information from incidents; and (3) establish incentives to "institutionalize lessons-learning processes at all levels of government."[5]

In 2005, the U.S. General Accountability Organization reported on a study conducted to identify practices to "Help Enhance and Sustain Collaboration among Federal Agencies." It documented the following recommendations:

- Define and articulate a common outcome;
- Establish mutually reinforcing or joint strategies;
- Identify and address needs by leveraging resources;
- Agree on roles and responsibilities;
- Establish compatible policies, procedures, and other means to operate across agency boundaries;
- Develop mechanisms to monitor, evaluate, and report on results;
- Reinforce agency accountability for collaborative efforts through agency plans and reports; and
- Reinforce individual accountability for collaborative efforts through performance management systems.[6]

These eight practices can all be mapped to one of the five domains and thirteen factors of the ICC model. The two domains that are not explicitly included in this list are the Individual Collaborative Capacities and Lateral Mechanisms. However, a more recent GAO report cites four actions that agencies should take to enhance interagency collaboration for national security:

- Develop and implement overarching strategies
- Create collaborative organizations.
- Develop a well-trained workforce.
- Share and integrate national security information across agencies.[7]

These four recommendations repeat the need for attention to strategic and structural requirements for collaboration, and now include two – information sharing and individual capabilities – that represent Lateral Mechanisms (information sharing) and the personnel capabilities specified in the People domain of the ICC model.

## TRENDS IN INTER-ORGANIZATIONAL COLLABORATION

The most significant post-9/11 trend related to this essay is the increasing attention, of scholars and practitioners, to the importance of inter-organizational collaboration for homeland defense and security. As the 2005 GAO report states, "the 21st century will be difficult, if not impossible, for any single agency to address alone."[8] One initial response to heightened awareness of the need for collaboration was to establish requirements through mechanisms such as the *National Infrastructure Protection Plan*. But establishing requirements does not automatically instill the participating organizations with the designed systems, motivation, norms, individual competencies, or strategic appreciation necessary for successful collaboration. So an important related trend is the emphasis on the need for organizational leaders to deliberately attend to the development of collaborative capabilities across all aspect of their organization including strategy, structure, reward systems, lateral mechanisms, and people.

The types of organizations viewed as critical partners for homeland security are expanding. The initial focus was primarily on domestic government agencies at local, state, tribal and national levels. But recent DHS reports emphasize the importance of strengthening collaborative capabilities with the private sector, non-governmental organizations, and international partners.[9] The scope of issues that are seen as pertinent to national security has also expanded to include such concerns as cyber-space, climate change, and the global economy. These new domains require the development of new goals, strategies and linkages with an even broader set of stakeholders. Another recent focus has been on citizen involvement in homeland security. Community Emergency Response Teams (CERT) and America's Waterway Watch offer both prevention and response capabilities that need to be integrated into local and regional collaboration planning and information systems.

A potentially significant challenge moving forward is the resource-constrained environment resulting from the economic downturn. The organizations expected to participate in collaborations are also competing for federal and local funds to support their organization-level operations. To the extent that collaboration is seen as an additional cost that is secondary to the core mission of an organization, commitment to collaboration may wane. A related question raised by Sheryl Jardine's research is whether current regional collaborations will be sustained if and when federal grants for regional planning are reduced or eliminated. Her sample of homeland security managers reported an increased appreciation for the value of regional planning and benefits gained through partnerships that had not previously existed. This is as a direct result of federal funding requirements or support. However, the participating managers also acknowledge the costs and challenges of collaboration. Perhaps the strongest indicator of concern is that a number of the managers said they would not continue in regional collaborations if funding or requirements ended.[10] This is clearly a question that needs further investigation.

The rise of Web 2.0 technologies has suggested the potential for e-government, which in terms of the ICC model, offers potential new tools and technologies that can be harnessed in the critical domain of Lateral Mechanisms. The collaborative efficiencies within and across boundaries resulting from new interactive, Internet technologies can improve information sharing and provide a means of integrating and making sense of information more quickly. Indeed, the new platforms are often called "collaborative technologies." However, the technology investment decisions, which include the technical infrastructure of software, hardware and systems as well as the training and skills to develop, deploy and maintain

those systems, will be a substantial challenge. The new technology has the promise of reaching beyond boundaries to invite new types of collaboration for increased efficiencies and collaboration, but there are few current case studies.[11] Determining the tradeoffs, threats and opportunities of the rapidly changing domains of Internet and mobile technologies represents a major area of interest for practice and research.

## CONCLUSION: WHERE DO WE GO FROM HERE?

What has become evident is just how difficult it is to achieve effective collaboration. In an era of increasing interdependence among organizations and the problems they face, the challenges and opportunities for building inter-organizational collaborative capacity are not going to go away. At least in the near term, the resources available to US government organizations and many of their non-government and international partners are likely to decrease, creating pressures and potential barriers for collaboration. At the same time, the technical systems for enabling collaboration suggest the potential for possible new innovations. If homeland security and defense managers are to be successful in building the inter-organizational collaborative capacity necessary to navigate these new waters, they will need to align the design of their organizations in the critical domains of strategy, structure, lateral processes, reward systems, and people. There may be no greater challenge or opportunity for engaging the complex, uncertain problems that will face us.

## ABOUT THE AUTHORS

***Susan Page Hocevar*** *is an associate professor in the Graduate School of Business & Public Policy at the U.S. Naval Postgraduate School (NPS) in Monterey, California. She received her PhD in business administration from the University of Southern California. Her research and publications are in the areas of inter-organizational collaboration, organization design, and organizational change.*

***Erik Jansen*** *is a senior lecturer in the Graduate School of Operational and Information Sciences at NPS. His PhD is from the University of Southern California. His teaching and research focuses on organizational design and capabilities, primarily in the areas of collaboration and innovation.*

***Gail Fann Thomas*** *is an associate professor in the Graduate School of Business & Public Policy at NPS. Her research and publications are in the areas of strategic communication, conflict management, and inter-organizational collaboration.*

[1] E. Jansen, S.P. Hocevar, R. Rendon and G.F. Thomas, *Interorganizational Collaborative Capacity: Development of a Database to Refine Instrumentation and Explore Pattern,* Technical Report NPS-AM-08-148 (Monterey, CA: Naval Postgraduate School, November 24, 2008).

[2] S.P. Hocevar, G.F. Thomas and E. Jansen, "Building Collaborative Capacity: An Innovative Strategy for Homeland Security Preparedness," in *Advances in Interdisciplinary Studies of Work Teams: Innovation Through Collaboration*, M. M. Beyerlein, S.T. Beyerlein, and D. A. Kennedy, eds. (Oxford: Elsevier JAI Press, 2006), 271.

[3] P.N. Stockton and P.S. Roberts, "Findings from the Forum on Homeland Security After the Bush Administration: Next Steps in Building Unity of Effort," *Homeland Security Affairs* IV, no. 2 (June 2008), http://www.hsaj.org/?article=4.2.4.

[4] S. Caudle, "Basic Practices Aiding High-Performance Homeland Security Regional Partnerships," *Homeland Security Affairs* II, no. 3 (October 2006), http://www.hsaj.org/?article=2.3.7.

[5] A.K. Donahue and R.V. Tuohy, "Lessons We Don't Learn: A Study of the Lessons of Disasters, Why We Repeat Them, and How We can Learn Them," *Homeland Security Affairs* II, no.2 (July 2006), http://www.hsaj.org/?article=2.2.4.

[6] U.S. Government Accounting Office (GAO), *Results-Oriented Government: Practices That Can Help Enhance and Sustain Collaboration amount Federal Agencies,* GAO-06-15 (October 2005), www.gao.gov/new.items/d0615.pdf.

[7] U.S. GAO, *National Security: Key Challenges and Solutions to Strengthen Interagency Collaboration,* GAO-10-822T (June 9, 2010), www.gao.gov/new.items/d10822t.pdf.

[8] GAO *Results-Oriented Government*, 1.

[9] Department of Homeland Security *Bottom-up Review Report* (July 2010), http://www.dhs.gov/xlibrary/assets/bur_bottom_up_review.pdf ; Department of Homeland Security *Quadrennial Homeland Security Review Report: A Strategic Framework for a Secure Homeland* (February 2010), http://www.dhs.gov/xlibrary/assets/qhsr_report.pdf.

[10] S. Jardine *The Impact of Incentives and Requirements on Group Collaboration* (master's thesis, Naval Postgraduate School, September 2010). Jardine's sample was gathered from the Urban Area Security Initiative (UASI) program managers professional group. Of the forty-four voluntary participants, 21 percent said they would not continue collaboration if requirements or funding stopped.

[11] For two case studies at opposite ends of the spectrum, see: B.S. Noveck, *Wiki Government (*Washington, DC: Brookings, 2009); M. Zook, M. Graham and S. Taylor, "Volunteered Geographic Information and Crowdsourcing Disaster Relief: A Case Study of the Haitian Earthquake," *World Medical & Health Policy* 2, no. 2 (2010): 7-33.

# Reflections on 9/11: Looking for a Homeland Security Game Changer

Samuel H. Clovis, Jr.

*The public school is at once the symbol of our democracy and the most pervasive means for promoting our common destiny.*
Felix Frankfurter, 1948

When invited to write an essay reflecting on the tenth anniversary of 9/11 I, like many of my colleagues I am sure, had mixed emotions. The events of that day still make me weak-kneed as I remember seeing so much destruction by resolute attackers who showed imagination and persistence. As a member of the military, I came into the service during the Viet Nam War, and was on active duty for the Iran hostage affair, the Beirut bombing, Grenada, Desert Storm, and operations in the Balkans. I was the quintessential Cold Warrior until my retirement from the service in 1996, but I had not experienced anything like what happened on that fateful day. I was a civilian teaching at a small college in the Midwest and happened to be taking my stepson to school when the first airplane hit the World Trade Center tower. I listened incredulously to radio reports, but as time moved on, so my thinking turned to experiences I had as a war game designer. I simply could not believe that individuals bent on our demise actually perpetrated events we had imagined in the comfort of a conference room. From that day forward, things have not been the same.

As fate would have it, I became involved in "homeland security" in the wake of the attacks. I left the intellectual protection of academia and returned to government contract work right after the Department of Homeland Security was established. My first task with my new employer was to learn as much about the new organization as I could. Contractors from all over the country were flocking to the new revenue troughs to feed on what appeared at the time to be a never-ending flow of funds to support the new mission space. The White House and the new department were issuing national documents like confetti at a ticker tape parade. We had strategies, goals, guidance, directives, lists and plans – all of which were focused on diminishing or eliminating terrorism as a threat to Americans at home or abroad. We jumped into a war in Afghanistan and then one in Iraq. We are still in both places.

Over time, state and local governments began to absorb "homeland security" mission space into their already robust public safety and emergency management operations. Their focus, for the most part, moved to all-hazards, of which terrorism was but one. At the national level, however, the central government maintained (as it does to this day) a primary focus on anti- and counter-terrorism. Playing nice with others dissolved into traditional institutional pathologies with the national government focusing on a top-down, one-size-fits-all approach to homeland security while the state and local governments worked on improving inter-local cooperation and enhancing capacities to deal with higher probability events, usually the result of nature. Though the above might represent a skeptical outlook on how things stand today, there have been some measurable improvements in homeland security.

The current established state of homeland security "normal" offers some hope for a safer, more secure nation, but we are a long ways from where we might be. The nation's economic woes have put a strain on homeland security resources at all levels and forecasts indicate these conditions are not likely to change in the near future. With resources so constrained, how are jurisdictions to maintain, let alone grow, responder capacities that enhance community resilience and the security of citizens? Are the precious resources of our cities, counties and states being spread too

thin because we are not addressing public policy reforms that would genuinely reduce the cost of governance? I submit that public education reform is the investment with the highest potential return.

Several years ago, I was asked by the Preparedness Division of DHS to examine possible alternatives for distributing state homeland security grant funds. One of the tasks was to determine if different formulae could be developed that would essentially lead to a more equitable distribution based on risk or other factors that might be appropriate. Specifically, I was asked to develop a method that would allow an "apples-to-apples" comparison of jurisdictions that might better inform the grant distribution process. As often happens in academic research, one often stumbles across something that was wholly unexpected. When comparing jurisdictions, the one attribute that seemed to influence all others was the level of educational attainment of residents in that jurisdiction. I have since been tinkering with developing mathematical models to help me validate my original findings, and I am making progress. I am convinced that a strong public education system could have the single largest impact on the security of the United States. Public education reform, then, could be a game changer for homeland security. Through more effective public education, the nation could lower the social costs that are now applied to welfare, income security programs, public safety, and health care. With every marginal improvement in public education, the nation reaps a geometric reduction in the cost of social programs, thus freeing those resources to be applied to other public goods and services.

Last fall, I started a lecture series on the Constitution, government, and governance in America today. Over the course of the nine part series, it became apparent that discussing education reform would be required in separate seminars. In the spring, I delivered two lectures on education reform that drew the largest crowds of the entire series. Because every American goes to school, all are familiar with the education system. What many citizens do not know, however, is the current state of public education in this country. Here are some highlights:

- Public education represents the highest outlay for state and local governments (25 percent of budgets), outstripping Medicaid (13 percent).[1]
- Of the 62 million children between the ages of three and nineteen in this country, 11 percent go to private schools, 3 percent attend charter schools, and as many as 6 percent are now home schooled. The remaining 80 percent attend public schools. Of those children age three to seventeen, 94 percent are in school. Of those ages eighteen or nineteen, only 69 percent are still in school.[2]
- Over 31 million children are on some form of federally funded school meal program. These are means-tested programs for children from households that have incomes at 130 percent of the poverty level or below.[3]
- For the past forty years, overall academic performance in American schools has not improved. Forty years ago, the United States was number one in academic performance in the world. Today, the US ranks twenty-fourth is math and twenty-fifth in science.[4]
- Fewer than 35 percent of students achieve basic proficiency at grade level.[5]
- The overall high school graduation rate for the country is around 70 percent. Some 1.2 million children drop out of school during each academic year. Dropout rates among minorities is alarming, with Native Americans' dropout rate at 49 percent, African Americans' at 45 percent, and Hispanics' at 44 percent. Of all individuals incarcerated in the country, 68 percent lack a high school education. No major city in the nation has a graduation rate above 64 percent. Detroit, Los Angeles, and San Antonio have graduation rates of 38 percent, 44 percent, and 47 percent, respectively.[6]
- Closing the performance gap between the US and other developed nations – between minorities and between similar schools – would add $2.31 trillion to the

gross domestic product of the nation.[7] This would mean an additional $415 billion in revenue at the national level and $138 billion at the state and local level.[8]

- Current unemployment rates for individuals with less than a high school education is 16 percent, nearly twice the national rate.[9] Those with less than a high school education earn less than 6 percent of the national income and see no appreciable increase in earning ability for the first thirty years of their working lives.[10]
- High school dropouts are more likely to have children out of wedlock (costing $110 billion annually), higher health costs (now nearly all on Medicaid), and are far more likely to be incarcerated.[11]

In my research, I found that those jurisdictions with the highest educational attainment levels also had, for the most part, the lowest poverty rates, the lowest crime rates, and the highest volume of goods and services provided by government. How does this "discovery" impact homeland security and community resilience, however?

By using a simple mathematical model, I was able to compare jurisdictions of similar characteristics. I examined fifty cities across the country that had populations of between 100,000 and 500,000. I used an array of demographic and economic characteristics to build the comparisons. Of the fifty cities examined, thirteen had distinctly lower "scores" than the other thirty-seven. I then looked for a "test case" and decided to include New Orleans in my calculus. Having few examples of "failed" governments in times of crisis, I compared pre-Katrina New Orleans with two of the "at risk" jurisdictions that had nearly identical characteristics. When the model was applied to New Orleans, all three cities had nearly identical scores. New Orleans government and governance failed during that city's crisis, and by extrapolation, the other cities might stumble during crisis as well. Each of the three cities had nearly identical low educational achievement levels and high poverty rates.[12]

The above is by no means a validation of anything other than numbers being applied in a crude model. However, of the fifty cities to which I applied the model, those with the highest educational attainment scored the best. A lot of work needs to be done with the model, but it appears to be a good start.

In David Guggenheim's compelling documentary, *Waiting for Superman*, he chronicles the experiences of several families from large cities as they go through the process of applying for opportunities to be part of lotteries to get into charter schools.[13] These relatively new educational innovations – charter schools – show great promise in raising performance levels for those who attend. Unfortunately, school choice programs across the country offer asymmetrical educational opportunities. Of greatest concern is the seemingly irreversible decline in school performance in our largest cities. As Terry Moe of Stanford University has documented, the gap between minority student performance – with the notable exception of Asian-American students – and that of white students in large cities is continuing to expand.[14]

This brief essay is not intended to argue the merits of school choice, school reform initiatives or the impact of public unions on educational outcomes. My intent is to call the attention of my homeland security colleagues to the idea that public education reform must be part of any serious discussion about national or homeland security. A better-educated citizenry will be less dependent on government and more independent in times of crisis. A better-educated citizenry will be more attentive to issues and challenges at the state and local level and more engaged at the national level. A better-educated citizenry will cost less in public funding and will contribute more to the public coffers. Ultimately, a better-educated citizenry will be the guarantor of security for the nation and liberty for the individual.

## ABOUT THE AUTHOR

***Samuel H. Clovis**, Jr., is professor and chair of the Department of Business Administration and Economics at Morningside College in Sioux City, IA. He holds a doctorate in public administration from the University of Alabama and is a twenty-five-year veteran of the Air Force. Dr. Clovis has been deeply involved in homeland security research and teaching since 2003. He serves as a*

*lecturer for the Center for Homeland Defense and Security at the Naval Postgraduate School and is on the editorial board of the* Homeland Security Affairs.

1 United States Census Bureau, *State and Local Government Finance* (Washington, DC: US Census Bureau, 2010).

2 United States Census Bureau, *Enrollment Status of Three-year-olds and Above* (Washington, DC: US Census Bureau, 2009).

3 Food Research and Action Center, National School Lunch Program (2011), http://frac.org/federal-foodnutrition-programs.html.

4 McKinsey & Co., *The Economic Impact of the Achievement Gap in America's Schools* (New York, NY: McKinsey & Co., 2009).

5 David Guggenheim, *Waiting for Superman* (Los Angeles, CA: Paramount Vantage Studios, 2010).

6 C. Swanson, *Cities in Crisis: Closing the Graduation Gap* (Bethesda, MD: Editorial Projects in Education, 2009).

7 McKinsey & Co., Achievement Gap.

8 These numbers are based on multiplying the overall increases in GDP by 18 percent to estimate federal income tax remittance and 6 percent for state and local income tax remittance.

9 United States Bureau of Labor Statistics, Unemployment in the United States (Washington, DC: US Bureau of Labor Statistics, 2011).

10 McKinsey & Co., Achievement Gap.

11 Fox News, "Study: Divorce, Out-of-wedlock Childbearing Cost U.S. Taxpayers More than $112 Billion a Year" (2008), http://www.foxnews.com.html.

12 Samuel H. Clovis, Jr., "Normalizing Jurisdictional Traits to Expose Governance Vulnerability in Large Urban Settings," paper presented at the Midwest Political Science Association Annual Meeting, April 2008, Chicago, IL.

13 Guggenheim, *Waiting for Superman*.

14 T. Moe, "Collective Bargaining and the Performance of the Public Schools," *American Journal of Political Science* 53, no. 1 (2009): 156-174.

# How Proverbs Damage Homeland Security

Christopher Bellavita

Proverbs express significant truths about a cultural narrative.[1] They communicate values, beliefs and knowledge. John Dewey wrote: "The consequences of a belief upon other beliefs and upon behavior may be so important ... that [people] are forced to consider the grounds or reasons of their belief and its logical consequences."[2] Dewey described the "consideration" as reflective thought, or what a century later is called critical thinking.

Proverbs helped construct homeland security's narrative during its first decade. The ideas they transmitted reduced ambiguity and gave strategic direction to the new national enterprise.

But proverbs can inhibit as much as enhance. Sometimes the "truth" they embody escapes scrutiny, inhibiting efforts to allow a narrative to evolve. Herbert A. Simon wrote: "If it is a matter of rationalizing behavior that has already taken place or justifying action that has already been decided upon, proverbs are ideal.... [They] are a great help in persuasion, political debate, and all forms of rhetoric."[3]

Homeland security's first decade was characterized by "ready, fire, aim." A great deal of work had to be done in a short period of time. Much was accomplished during that decade, and it cost a lot of money. By one estimate more than one trillion dollars was spent on homeland-related programs during the decade.[4] No one knows how much of that money went to ineffective activities because the homeland security enterprise spent more effort firing than aiming.

Homeland security's second decade can productively focus on "aiming." Academics and strategists have an opportunity to critically examine the basic assumptions underpinning the homeland security narrative, and identify evidence that supports or refutes foundational ideas used to guide strategic direction. The purpose of this essay is to illustrate such an examination.

Here are one dozen proverbs that partially outline the homeland security narrative:[5]

1. Intelligence analysts need to connect the dots.
2. They [the "enemy"] hate us for our freedoms.
3. We fight them over there so we don't have to fight them here.
4. Risk is a function of threat, vulnerability, and consequence.
5. All disasters are local.
6. All hazards means *all* hazards.
7. To be prepared get a kit, make a plan, and be informed.
8. If you see something, say something.
9. People are likely to panic in a disaster.
10. Those who would give up essential liberty to purchase a little temporary security deserve neither liberty nor security.
11. Terrorists only have to be lucky once; we have to be lucky all the time.
12. Eight-five percent of US critical infrastructure is owned/controlled/in-the-hands-of/operated by [the verbs change] the private sector.

I think the proverbs are wrong or misleading in important respects. As a consequence, they distort the homeland security narrative and inhibit the search for more effective ideas to protect the nation. My overall claim is based on a mix of anecdote, suggestive evidence, and hunch. I discuss one proverb in depth (*Eight-five percent of US critical infrastructure is owned by the private sector*) and assert the others can also benefit from critical analysis.

The 85 percent figure is probably America's best-known homeland security statistic. The claim appears in the 9/11 Commission hearings, the *9/11 Commission Report*, the 2002 and the 2007 national homeland security strategies, and stacks of related documents.[6] It is parroted by Congress, the DHS, think tanks, academics, trade associations, and other homeland

security residents.[7] Its presence is not restricted to our borders. The number appears also in Canadian and Czech Republic reports about who owns their critical infrastructure.[8]

I will describe my efforts over the past decade to understand what the 85 percent claim means and offer four reasons why uncritically accepting the proverb as truth harms homeland security. I close by suggesting why the other proverbs may also be misleading.

## WHAT DOES THE NUMBER MEAN?

What could the 85 percent number mean, even in principle? Is there a difference that matters between "ownership," "control," "in-the-hands-of," or "operated?"

I can come to terms with the inability to know with certainty what homeland security is. But what explains the difficulty agreeing who or what controls critical infrastructure?

Maybe the quandary rests in how the claim is structured. Sometimes the number refers simply to all "infrastructure."[9] Other times it's about "critical" infrastructure.[10]

But putative distinctions may no longer matter. The initial difference between critical infrastructure and plain vanilla infrastructure seems to have quietly vanished.

Critical infrastructure used to mean what the USA PATRIOT Act directed it to mean:

> Systems and assets, whether physical or virtual, **so vital to the United States** that the incapacity or destruction of such systems and assets would have a debilitating impact on security, **national** economic security, **national** public health or safety, or any combination of those matters.[11] [My emphasis.]

In 2009, a different definition of critical infrastructure appeared in the National Infrastructure Protection Plan:

> Systems and assets, whether physical or virtual, **so vital** that the incapacity or destruction of such may have a debilitating impact on the security, economy, public health or safety, environment, or any combination of these matters, **across any Federal, State, regional, territorial, or local jurisdiction**.[12] (My emphasis again.)

The "flea markets, petting zoos, popcorn factories, hot dog stands or other such facilities" DHS was (unreasonably) criticized for including in a critical assets database a few years ago may turn out to be someone's critical infrastructure after all.[13]

Compounding the semantic problem, how could one even estimate, let alone calculate with any precision, ownership or control?[14] Does one identify every individual provider of goods and services that could be included in the (18, 19, or more) sectors,[15] discover who owns (in some legal sense) each business, and then determine percentages? Does one classify companies and organizations into the sectors first, then figure out who owns the sectors and calculate from that premise? Is ownership equivalent to control? Does ownership or control imply government has little to no say in security practices?

A July 2011 Congressional Research Service Report observed,

> Sharing information with the federal government about vulnerability assessments, risk assessments, and the taking of additional protective actions is meant to be voluntary. However, the degree to which some of the activities are mandated varies across sectors. In some cases, sectors are quite regulated.[16]

The answer to whether the distinction between public or private control has substantive meaning is "yes, no, and it depends."

But what about the 85 percent proverb? How does it harm homeland security?

## WHEN PEDANTRY MATTERS

The word "pedantry" was invented to refer to an excessive concern with petty details.[17] One might say anguishing over 85 percent is pedantry.

One author who writes about critical infrastructure noted,

> Whether this figure is 100 percent accurate or based on any in-depth analysis is debatable but, regardless, little or no infrastructure would function (critical or otherwise) without the efforts of private sector owners and operators.[18]

A senior DHS official addressed my distress more directly a few years ago: "It

doesn't matter whether the 85 percent is right or not," he said. "We're still going to do the same thing."

I believe it does matter. And by "it" I mean the persistence of an idea that impedes considering alternative ideas about how to protect critical infrastructure.

Here are four reasons why the proverb's persistence damages homeland security. A discussion of each reason follows.

1. It gives the impression we know more than we do when it comes to critical infrastructure.
2. It creates a false image about the power relationships between the public and private sectors.
3. It distorts normative understanding about roles and responsibilities.
4. It constrains discussions about policy options.

## THE IMPRESSION OF COMPETENCE

The philosopher Harry Frankfurt writes about the distinction between those who tell the truth or who lie, and those who bullshit. Truth tellers and liars cohere around the truth, either to communicate it or to hide it. One who uses bullshit does not care about the truth or falsity of a claim, but instead cares about the impression the claim makes. Bullshit substitutes sincerity for accuracy.[19]

"Maybe we don't know the truth about critical infrastructure," the reasonable homeland security professional might argue, "but the claim is well-meaning; work with me here so we can do good."

The sincerity underpinning the 85 percent myth gives an impression that when it comes to critical infrastructure we fundamentally know what we are talking about. More specifically, quantifying ownership and control signals someone knows what infrastructure is actually critical, and professionals can thus manage what is vital to the nation's security and well-being.

The number's misguided precision veils what we do know: there is no "one definite prioritized list of critical assets…" and "it would not be possible or useful to develop one."[20]

## PRIVATE POWER, PUBLIC POWER

The 85 percent number conveys an inference about the power relationships between the public and private sector: since the important parts of the nation are owned by the private sector, government ought to "ask" the private sector to help out with this messy security business. The private sector can, of course, decline.

There is another – less discussed – side to the power assessment. The 85 percent benediction does not automatically advantage the private sector. Some infrastructure officials, nominally in the private sector, say the 85 percent figure justifies preventing the private sector from receiving information, grants and other public funds needed to upgrade and secure their facilities.

> The dilemma… has been in encountering an obdurate, logic-proof insistence by cops, fire fighters, emergency managers, fusion center staff, and DHS minions to define my employer and all critical infrastructure stewards as private sector entities… [and thus] unworthy of [receiving] sensitive information… and inherently suspect of being profit driven….[21]

I have not found data describing how well the private sector embraces its sometimes-reluctant partnership in the homeland security enterprise.[22] I have heard anecdotes about industries that take seriously the part they play in ensuring the nation's security.[23] I also hear stories about the predictable cast of characters showing up at regularly scheduled gatherings arranged to praise or encourage public-private infrastructure partnerships.

I have not seen the comprehensive metrics across critical sectors a chief financial officer or board of directors would demand about the impact of those partnerships. But the same can be said for evidence about the public sector's contribution to preparedness and resilience.[24] Maybe when it comes to infrastructure neither sector has as much power as the other believes.

## OWNERSHIP IS NOT RELEVANT

It may be rhetorically convenient to separate public and private sector responsibilities. But assuming what has yet to be demonstrated interferes with determining who has to do what to strengthen protection.

One of my colleagues views the "who owns what" argument this way:[25]

> The argument is bogus: the big stuff, like water, power, energy, transportation is so regulated and controlled by the feds, that the fact that it is owned by someone isn't a factor. If the feds decided to harden power plants, for example, Congress can do what it wants. Isn't this the case already with nukes and the Federal Energy Regulatory Commission? Same thing with transportation, energy, etc.

Another colleague expressed his concern about responsibilities:[26]

> The basic foundation of our society – [the] infrastructure that is essential for public safety and well-being – is owned and controlled by state and local government.[27] .... The underlying premise behind having much of this [infrastructure] under state and local control is they are monopolies or they are so critical that from a societal aspect you cannot have a company that runs any of this infrastructure go [into] Chapter 7.

Critical infrastructure is too critical to be left to the private sector to protect, he argued. Policymakers need to acknowledge the partnership between the invisible hand of free enterprise and another hand:

> There is a second "hidden" [and] "unseen hand" to much of this infrastructure. This is the state regulatory agencies. The regulatory construct is what holds this all together and without which the sectors could not function. Food and agriculture, water systems, health systems cannot function without the regulatory agencies (mostly state government) functioning.

Trying to determine who owns what is less productive than identifying contributions different sectors make to disparate types of security and resiliency:

> [Our] state governments should actually be our primary infrastructure partner and primary partner in [societal] security and resiliency. The private sector who employs most of the work force and generates a huge percentage of GDP should be our primary partner in economic security and economic resiliency. Both are our partners in disaster resiliency. Most of our [critical infrastructure] does not produce GNP it enables GNP but does not produce anything. Thus from an economic standpoint we should focus attention on the GNP producers. This is why separation between enablers and producers is counterproductive.... We have also made a strategic mistake in [putting] all infrastructure into the "private sector" domain regarding business models. State and local government business models and the business model of a company on the stock exchange are completely different.

## HIDING THE NETWORKS

Thinking about ownership and control encourages strategists and policymakers to consider critical infrastructure primarily as a collection of "eaches" – individual farms, water treatment plants, monuments, dams, power plants, manufacturers – to be protected. But "most critical infrastructure spans multiple states." Gas and oil pipelines, electric power grids, telecommunications networks, Internet and computer networks, water supplies, food, chemical and industrial networks "all cross state boundaries."[28]

The "eaches" framework that flows from the 85 percent mantra obscures policy options premised on a network view of infrastructure. Considering infrastructure as networks draws attention to nodes, links, interdependencies, scale free structures, power laws, small worlds, self-organized criticality, sand piles, and related concepts that might inspire innovative approaches to protecting infrastructure.[29]

## WHAT ELSE?

Debate about the 85 percent number is operationally trivial. But questioning whether it is valid can remind those of us in the homeland security enterprise to critically examine what we accept as true. If we got the 85 percent wrong, yet it persists as truth, what else have we missed?

Revisiting the proverbs introduced at the start of the essay suggests possible answers to that question.

1. Intelligence analysts may be expected to connect the dots, but the expectation ignores the complexity of the intelligence task. "[Pleading] for more dots is to mistake the nature of the problem posed by … terrorism, and … even recognizing the significance of the information is a task that exceeds the capacity of a single organization…." [30]
2. One may believe the enemy hates us for our freedoms, but one must also listen to the argument that "blaming our freedoms for Muslim terror is absurd and dangerous." [31]
3. We fight them over there so we don't have to fight them here, but the growing concern about domestic radicalization suggests this proverb needs to be retired. [32]
4. Risk might be a function of threat, vulnerability, and consequence, but in homeland security the nature of, and data sources for, that function remain illusive. [33]
5. All disasters may once have been local, but in homeland security's second decade, one may need to acknowledge "disasters have far-reaching consequences throughout regions, states, the nation and even the globe." [34]
6. All hazards does not really mean *all* hazards. As one of the nation's respected emergency management scholars explained, "*All-hazards* does not literally mean being prepared for any and all hazards that might manifest themselves in a particular community, state, or nation." It does mean developing a general plan that "can provide the basis for **responding** to unexpected events." [35] [My emphasis.]
7. Getting a kit, making a plan and staying informed may be one theory about preparedness, but the advice does not appear to resonate with the American people. One state emergency management director suggested,

   > We need to reframe expectations. A disaster kit, prepackaged and stored away only to be used in a disaster is not practical for many Americans. It is costly and takes time, attention, and desire to maintain…. We must educate the public about the risks they actually face, have an honest discussion with them about what they expect government to do, what they can do and, more to the point, what they must do. Then we need to ask how we can help them be better prepared. But not through another revised seventy-two-hour preparedness campaign with the same messages we are promoting today. [36]

8. If you see something, say something, but what gets said, and with what effect? The Metropolitan Transit Authority created the trademarked slogan shortly after the 9/11/01 attacks. It has since been leased to the Department of Homeland Security. Is this proverb an effective way to engage citizens in homeland security, is it eyewash, or is it pernicious? [37] One security expert cautioned, "if you ask amateurs to act as front-line security personnel, you shouldn't be surprised when you get amateur security. People don't need to be reminded to call the police; the slogan is nothing more than an invitation to report people who are different." [38]
9. The idea that people are likely to panic in a disaster persists in the face of convincing evidence to the contrary. As one example, a study of over 500 disaster events concluded: "panic was of very little practical or operational importance." [39]
10. People who agree with Benjamin Franklin's 1775 homily that "Those who would give up essential liberty to purchase a little temporary security deserve neither liberty nor security," may ignore the suggestion raised by Philip Bobbitt that in *The Wars for the Twenty-First Century* "it is possible to increase the powers of government and, at the same time, increase the rights of the people." [40]
11. The belief "Terrorists only have to be lucky once; we have to be lucky all the

> time" originated in a terrorist message issued after the 1984 Brighton bombing.[41] US policymakers adapted the language and turned it into a strategic proverb.[42] One American WMD expert countered that claim by noting terrorists planning a complex operation have to worry about many pieces coming together. "They have to be right all the time," he said. "We only have to be right once to stop them."[43]

## WHAT IS YOUR CLAIM AND WHY SHOULD ANYONE BELIEVE IT?

The proverbs discussed in this essay may turn out eventually to be approximately right or substantially wrong. As Herbert Simon wrote about a different set of proverbs:

> It is not that the propositions expressed by the proverbs are insufficient; it is rather that they prove too much.... For almost every principle one can find an equally plausible and contradictory principle...and there is nothing...to indicate which is the proper one to apply.[44]

A 2011 study described homeland security as an "anemic policy regime," whose purposes are "poorly understood and not widely shared among different elements of the federal government or at subnational levels." It is characterized by "the weakness of the integrative ideas of 'homeland security' and 'all hazards' preparedness, the lack of a strong constituency for the regime, and the institutional misalignment among relevant subsystems."[45]

That critique does not flatter the organizations and people who shaped the homeland security enterprise. But the study's conclusions are based on evidence not slogans. One can agree or disagree with the authors' assumptions, analysis, and conclusions, but one does not have to guess how those conclusions were derived.

Homeland security's second decade ought to evolve toward a narrative foundation constructed by something more substantial than proof by repeated assertion. One should ask for evidence.

## ABOUT THE AUTHOR

***Christopher Bellavita*** *teaches at the Naval Postgraduate School in Monterey, California, where he serves as the director of academic programs for the Center for Homeland Defense and Security. Dr. Bellavita is the executive editor of* Homeland Security Affairs*, and a contributing editor to the* Homeland Security Watch *blog.*

1 I'd like to thank three reviewers who provided comments that helped improve this essay. I am using proverb in the sense described in the Oxford English Dictionary: "A … concise sentence … stating a general truth or piece of advice…." I think arguments could be made that what I am describing could also be called myth ("a widespread but untrue or erroneous … belief; a widely held misconception…") or meme ("a cultural element … whose transmission and consequent persistence in a population … is considered as analogous to the inheritance of a gene").

2 John Dewey, *How We Think* (Boston: D.C. Heath & Co, 1910), 5.

3 Herbert A. Simon, "The Proverbs of Administration," *Public Administration Review* 6, Winter (1946), 53.

4 John Mueller and Mark G. Stewart. "Balancing the Risks, Benefits, and Costs of Homeland Security," *Homeland Security Affairs* 7, Article 16 (August 2011) http://www.hsaj.org/?article=7.1.

5 Lauren Wollman noted in a personal correspondence that "however empty or inaccurate [the proverbs may be], … they serve the critical function in the emergence of the idea [of homeland security]: they facilitate the construction of a narrative and the transmission of specialized knowledge and lexicon to and from lay-culture…. In some ways… is it not more interesting to know why those particular images and proverbs [were adopted] to begin with? What story they tell, what truths they solidify in our imagination, what truths and facts they create?" She also added "need to know vs. need to share," and "stovepipes are bad, collaboration is good" as candidate proverbs.

6 See http://govinfo.library.unt.edu/911/archive/hearing5/9-11Commission_Hearing_2003-11-19.htm; 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*, 1st ed. (New York: Norton, 2004), 398; United States, *National Strategy for Homeland Security* (Washington, D.C.: Office of Homeland Security, 2002) 33. Homeland Security Council, *National Strategy for Homeland Security* (October 2007), 4.

7 For examples see Christopher Bellavita, "85% of what you know about homeland security is probably wrong," *Homeland Security Watch* (blog), March 16, 2009, http://www.hlswatch.com/2009/03/16/85-percent-is-wrong/, especially the insightful comments. The most recent instance I've seen of the number in print is testimony at the House Committee on Homeland Security Subcommittee on Cybersecurity, Infrastructure Protection, and Security Technologies, March 16, 2011 by James A. Lewis, "Examining the Cyber Threat to Critical Infrastructure and the American Economy," 4. On August 15, 2011, while this paper was being prepared, I heard the number used during a conference of homeland security professionals: "As every one knows," the speaker said, "85 percent of our critical infrastructure is directed by the private sector."

8 For Canada, see http://www.homelandsecuritynewswire.com/unprepared-canada-lacks-plan-protect-critical-infrastructure. For the Czech Republic, see http://bit.ly/ofI5wv.pdf.

9 For example, see Paul C. Robinson, Joan B Woodard, and Samuel G. Varnado, "Critical Infrastructure: Interlinked and Vulnerable," *Issues in Science and Technology*, Fall (1998), www.issues.org/15.1/Robins.htm.2. This article is one of the earliest written examples I've found of the 85 percent number.

10 For example, see "What is CIP?" http://cip.gmu.edu/component/k2/item/118-what-is-cip?

11 As noted in Department of Homeland Security, *Interim National Infrastructure Protection Plan* (February 2005), 3: "USA PATRIOT Act of 2001, 42 U.S.C. § 5195c(e), defining critical infrastructure. This definition is incorporated by reference into the Homeland Security Act of 2002, see 6 U.S.C. § 101."

12 Department of Homeland Security, *National Infrastructure Protection Plan* (2009), 109.

13 Robert Stephan, "Database is Just the 1st Step," *USA Today*, July 21, 2006, 8A.

14 Charlie Jasonberg pointed out (http://www.hlswatch.com/2009/03/16/85-percent-is-wrong/#comment-134580): "One of the GMU CIP reports investigated the 85% claim for the water sector. It used EPA and other data, and learned that 61% of the water sector was owned by the private sector, with 28% owned by local governments. So, the [percent] will vary from industry-to-industry." http://cip.gmu.edu/archive/cip_report_6.4.pdf.

15 John D. Moteff, *Critical Infrastructures: Background, Policy, and Implementation* (Congressional Research Service, July 11, 2011), 17.

16 Ibid., 31

17 Philological Society (Great Britain), *The Oxford English Dictionary; Being a Corrected Re-Issue with an Introduction, Supplement, and Bibliography of A New English Dictionary on Historical Principles* VII (Oxford: At the Clarendon Press, 1933), 606.

18 Timothy P. Clancy, "CI/KR Public-Private Partnerships — Sharing Responsibility, Managing Risk," *The CIP Report* (July 2008), 17.

19 Harry G Frankfurt, *On Bullshit* (Princeton, NJ: Princeton University Press, 2005), 53-56, 65.

20 Moteff, *Critical Infrastructures,* 26. DHS does claim it knows the highest priority sites.

21 Nick Catrantzos quoted in Christopher Bellavita, "85% More From The Private Sector About Critical Infrastructure," *Homeland Security Watch* (blog), March 30, 2010, http://www.hlswatch.com/2010/03/30/85-more-from-the-private-sector-about-critical-infrastructure/.

22 Moteff, *Critical Infrastructures,* 16-31, reviews many of the difficulties encountered trying to create and sustain partnerships.

23 I was told in August 2011 that data do exist demonstrating the information technology (IT) community has "vigorously embraced its security relationship and responsibility with government." Once I find that data I will update this note.

24 See for example Christopher Bellavita, "Homeland Security's War On Subjectivity," *Homeland Security Watch* (blog), October 29, 2009, http://www.hlswatch.com/2009/10/29/homeland-securitys-war-on-subjectivity/.

25 T. G. Lewis, personal correspondence.

26 The three quotations are from personal correspondence with an executive who works with critical infrastructure for a federal agency.

27 Examples include landfills, water systems, reservoirs, wastewater systems, emergency services, roads, bridges, tunnels, airports, ports, parts of the electrical system, mass transit (rail and bus), dams, universities, prison systems, courts – legal system, county administration buildings, state office buildings, state laboratories, and state hospitals.

28 T. G Lewis, *Critical Infrastructure Protection in Homeland Security: Defending a Networked Nation* (Hoboken, N.J: Wiley-Interscience, 2006), 47.

29 See, for examples, Ted G. Lewis, *Bak's Sand Pile* (Monterey: Agile Press, 2011); and Lewis, *Critical Infrastructure Protection in Homeland Security*.

30 Christopher Bellavita, "Nidal Hasan and the problem of connecting the dots," *Homeland Security Watch* (blog), November 12, 2009, http://www.hlswatch.com/2009/11/12/nidal-hasan-and-the-problem-of-connecting-the-dots/ citing Max Boisot.

31 Jonah Goldberg, "Free Speech and Burning Korans," *Townhall*, April 13, 2011, http://townhall.com/columnists/jonahgoldberg/2011/04/13/free_speech_and_burning_korans/page/2, quoting a 2007 statement by Dinesh D'Souza

32 Bob Johnson, "'Fight them there, so we don't have to fight them here' key lie in New Big Fib," *Daily Kos*, September 2, 2006, http://www.dailykos.com/story/2006/09/02/242333/-Fight-them-there,-so-we-dont-have-to-fight-them-here-key-lie-in-New-Big-Fib%C2%A9; Ron Paul, "'Fight them over there vs. over here' a false choice," *The Washington Times*, July 1, 2009, http://www.washingtontimes.com/news/2009/jul/01/fight-them-over-there-vs-over-here-presents-a-fals/; Jonah Czerwinski, "Fight'em Over There," *Homeland Security Watch* (blog), July 1, 2007, http://www.hlswatch.com/2007/07/06/fightem-over-there/; "New Reports on Terrorist Plots and Domestic Radicalization since 9/11," https://hsdl.org/hslog/?q=node/5534.

33 For one example of the variety of risk definitions, see http://www.sarma-wiki.org/index.php?title=Risk#_note-0. See also Unknown, "Incorporating Assessments of Terrorism Risk in Homeland Security Resource Allocation Decision Making: Closing the Gap Between Current and Needed Capabilities" (presented at the Risk Informed Decision Making for HLS Resource, Arlington, Virginia, 2009), 3: "The risk construct presented above [R = T x V x C] is logical, intuitively appealing, and consistent with conceptualizations of risk used in other domains. However, uncertainty inherent in deriving estimates for its components in the case of terrorism risk continues to compromise its usefulness in DHS resource allocation decision making. As a result, terrorism risk assessments have not played the prominent role they were expected to play in DHS resource allocation decision making. More robust and defensible methods for generating required inputs for this terrorism risk construct are required if it is to become an important factor in homeland security resource allocation decision making." For an insightful interpretation of the homeland security approach to risk, see Bob Ross, "The Multiple Levels of Risk Management," *Homeland Security Watch* (blog), April 2, 2009, http://www.hlswatch.com/2009/04/02/the-multiple-levels-of-risk-management/.

34 Jim Mullen, "Not all disasters are local," Washington Military Division; Emergency Management Department, March 23, 2011, http://blogemd.blogspot.com/2011/03/not-all-disasters-are-local.html. For another example, see Ashton B. Carter, Michael M. May, and William J. Perry, "The Day After: Action Following a Nuclear Blast in a U.S. City," *The Washington Quarterly* (Autumn 2007): 22-23.

35 "*All-hazards* does not literally mean being prepared for any and all hazards that might manifest themselves in a particular community, state, or nation. What it does mean is that there are things that commonly occur in many kinds of disasters, such as the need for emergency warning or mass evacuation, that can be addressed in a general plan and that that plan can provide the basis for responding to unexpected events." William Waugh, "Terrorism and the All-Hazards Model," 2004, http://training.fema.gov/EMIWeb/downloads/Waugh%20-%20Terrorism%20and%20Planning.doc.

36 Christopher Bellavita, "From kits to sustainment — reframing preparedness expectations and guidance," *Homeland Security Watch* (blog), March 8, 2011, http://www.hlswatch.com/2011/03/08/from-kits-to-sustainment-%E2%80%94-reframing-preparedness-expectations-and-guidance/, quoting Nancy Dragani.

37 William Neuman, "In Response to M.T.A.'s 'Say Something' Ads, a Glimpse of Modern Fears," *New York Times*, January 7, 2008, http://www.nytimes.com/2008/01/07/nyregion/07see.html. John Solomon, "New Study Indicates Difficulty In Evaluating Effectiveness Of 'See Something, Say Something'-Like Citizen Tips Campaigns," *In Case of Emergency, Read Blog*, September 17, 2010, http://incaseofemergencyblog.com/2010/09/17/new-study-indicates-difficulty-in-evaluating-effectiveness-of-see-something-say-something-like-citizen-tips-campaigns/.

38 Bruce Schneier, "If You See Something, Say Something," *Schneir on Security* (blog), May 12, 2010, http://www.schneier.com/blog/archives/2010/05/if_you_see_some.html.

39 Cited in Erik Auf der Heide, "Common Misconceptions about Disasters: Panic, the 'Disaster Syndrome,' and Looting," in *The First 72 Hours: A Community Approach to Disaster Preparedness* (Lincoln, Nebraska: iUniverse Publishing., 2004), 343.

40 Philip Bobbitt, *Terror and Consent: The Wars for the Twenty-First Century* (Knopf, 2008): 285-288.

41 'Today we were unlucky," [The Irish Republican Army communiqué] said, "but remember, we only have to be lucky once. You have to be lucky always. Give Ireland peace, and there will be no war.'" Jo Thomas, "This Time, the IRA Comes Close to Thatcher," *New York Times*, October 14, 1984, http://www.nytimes.com/1984/10/14/weekinreview/this-time-the-ira-comes-close-to thatcher.html?scp=2&sq=%93Terrorists+only+have+to+be+lucky+once%3B+we+have+to+be+lucky+all+the+time%94+&st=nyt.

42 Sean O'Driscoll, "U.S. Pols Quote IRA Statement," *Irish Voice*, n.d., http://www.irishabroad.com/news/irishinamerica/news/USPolsQuoteStatement.asp.

43 Al Mauroni, personal correspondence, reporting a statement originating from a federal law enforcement agency.

44 Simon, "The proverbs of Administration," 53.

45 Peter J. May, Ashley E. Jochim, and Joshua Sapotichne, "Constructing Homeland Security: An Anemic Policy Regime," *Policy Studies Journal* 39, no. 2 (2011): 302.

# The Post-Tragedy 'Opportunity-bubble' and the Prospect of Citizen Engagement

Fathali M. Moghaddam and James N. Breckenridge

*"The evil that men do lives after them."*
William Shakespeare

The September 11 2001 terrorist attacks are an example of evil that has lived on, echoed in atrocious acts of violence against ordinary people around the globe over the last ten years, most recently, in Oslo. Most Americans remember 9/11 as an exceptional event, a contemporary equivalent to the Japanese attack on Pearl Harbor. From a psychological perspective, however, many aspects of the public's response to 9/11 followed a pattern quite familiar to students of group dynamics and inter-group relations, a pattern that warrants the close attention of leaders at all levels because it reveals an *opportunity-bubble* – a promising, yet fleeting, opportunity to shape the course of subsequent events. In order for leaders to take advantage of this opportunity-bubble in a timely and effective manner, they must first understand it. By studying the group and intergroup dynamics that follow tragedies, leaders can lead in such a way as to ensure the opportunity-bubble leads to constructive rather than destructive outcomes.

One of the most robust and pervasive trends in social behavior is the relationship between perceived in-group threat and group cohesion.[1] Both experimental evidence and historical case studies demonstrate this relationship:[2] when individuals perceive a serious threat to the in-group (such as from an enemy attack or natural disaster), they show greater solidarity with other group members and increase their support for the group leader. "Showing greater solidarity" can mean making enormous sacrifices in order to support the in-group, and standing firmly behind the leader even when mistakes are seen to be made in leadership decision making. It can also mean demonstrating extraordinary resilience in the face of pressures and difficulties. Thus, examples of the kind of "Dunkirk spirit" the British public displayed during the London Blitz bombings in World War II often occur during wars, crises, and disasters.

Judging correctly when and how to make constructive use of the opportunity-bubble after a tragedy is a hallmark of great leadership. Enormous potential for civic generosity and sacrifice is available at the height of an opportunity-bubble, but leaders must choose the kinds of sacrifices and the timing of calls to action carefully. Timing is of the greatest importance: too early, and people – still reeling from the impact of the tragedy – may be unable to respond; too late, and people may have grown too detached from the tragedy and accustomed to non-commitment; even later, people (and the media) may focus critically – and perhaps angrily – on leadership's failure to have asked for more.

We argue that although great crisis will inevitably invite consideration of many alternatives, leadership must pay special attention to opportunities to engage the public as capable *partners* in their country's response to the crisis – calling upon them as citizens with civic duties, as well as rights. Such opportunities will often entail significant sacrifice, which we believe will generally be accepted if the public's role is clearly explained and accompanied by ample means to readily acquire information about the crisis, future threats, and the government's response.

Undoubtedly, in the immediate aftermath of 9/11 Americans were ready and willing to make personal and collective sacrifices. Over the first three weeks following the attacks, the rate of volunteerism increased more than six standard deviations above average throughout the nation.[3] Within only three months, charitable donations for 9/11 victims and their families exceeded $1.5 billion.[4] An

extraordinary, albeit brief, increase in social capital signaled the publics' readiness for civic contribution. Public trust and confidence in government reached a thirty-year peak in the first few weeks following the attacks.[5] Support for leadership was extraordinarily high and widespread. Even prestigious, traditionally skeptical newspapers – for example, *The New York Times* and the *Washington Post* – were uncritically supportive of leadership decisions after 9/11, including the momentous decisions to wage wars in Iraq and Afghanistan, according to retrospect scholarly analysis.[6] Yet, in as little as six months, the large majority of Americans who in early post-9/11 surveys had reported increased trust in government and had sought greater opportunities for political and social engagement simply vanished.[7] The opportunity-bubble had begun to burst.

This is not to say that leadership had not called for civic contributions. In his first State of the Union Address after 9/11, for example, President Bush called on Americans, as a "responsible nation," to commit "at least two years – 4,000 hours over the rest of your lifetime – to the service of your neighbors and your nation" and invited Americans to join the newly created USA Freedom Corps, which would "focus on three areas of need: responding in case of crisis at home; rebuilding our communities; and extending American compassion throughout the world."[8] Nevertheless, in the years to follow, aside from military enlistment, opportunities for civic engagement associated directly with the threat of terror seemed largely confined to calls for increased citizen vigilance. Interviewed on the eve of the Iraq War troop surge,[9] President Bush was asked why, given the importance he often stressed the war on terror represented for the country's future, as well as the disproportionate share the volunteer military and their families had sacrificed relative to the rest of the country, the president had not "asked more Americans and more American interests to sacrifice something," in particular, sacrifices that would "muster the support" and would involve Americans "in the struggle." In response, President Bush referred to his earlier call for volunteerism and his decision to establish the Freedom Corps and asserted that he had strongly opposed what were apparently the primary potential forms of sacrifice considered after 9/11: compulsory military service and tax increases.

American history, however, provides many examples of quite effective alternatives to calls for compulsory public sacrifice. The decision to meet the enormous requirements of the World War II war effort by supplementing taxes with a campaign calling upon citizens in all income categories to make voluntary contributions through War Bonds is particularly instructive. The War Bond campaign was carefully crafted to create an emotionally compelling sense of civic duty and public partnership in the war effort. During an all-day fundraising radio broadcast in 1943, for instance, the popular singer and celebrity Kate Smith explained to her fellow citizens: "when we buy War Bonds, we're not buying tanks and guns and shells and planes. What we're doing is buying our boys back … bringing them home to us, safe and sound once again."[10] The call for voluntary contributions through War Bond commitments generated $98.3 billion by 1945, representing almost half the then Gross National Product.[11]

Our own data, utilizing a nationally representative probability sample of several thousand American adults surveyed in late 2008, underscores the public's sustained desire for and disappointment in the lack of opportunities they believed government offered to serve a meaningful role in the country's response to terrorism.[12] Seven years after 9/11, only 37 percent of Americans adults reported that they had ever made sacrifices on behalf of the "war on terror." While Americans continued to engage in voluntary, unpaid civic services (32 percent), only a few (6 percent) reported participating in volunteer activities directly associated with crisis or disaster preparedness. A slim majority (52 percent) nevertheless indicated a desire for volunteer opportunities designed to prepare for and respond to disasters or acts of terrorism. Moreover, nearly two thirds of survey respondents felt that government had failed to provide or clearly explain ways for average citizens to play a role or participate in their country's defense against terrorism. Most respondents (66 percent) indicated that government had failed to

clearly explain citizens' role in the country's fight against terrorism and even more (74 percent) that government had failed to adequately explain how to prepare for acts of terror.

## PREPARING FOR THE NEXT 'OPPORTUNITY-BUBBLE'

Although social scientists have often helped government craft patriotically appealing and persuasive calls for civic action during national crises in patriotically appealing and persuasive ways, we do not suggest that the results are inevitably effective or desirable. Political scientists contributed to the successful WWII war bond campaign. In contrast, similar efforts by the Federal Civil Defense Administration and the Psychological Strategy Board, designed to engage the public in the Cold War civil defense movement, ultimately backfired. Public outrage and distrust increased as the public's growing appreciation of the catastrophic destructive capacity of nuclear weapons emphatically contradicted the threat minimization and implied survivability underlying civil defense propaganda.[13]

Our main goal in this brief discussion is to call attention to the opportunities and challenges ahead. Tragedies will happen, even with the best planning. But leadership can take advantage of opportunity-bubbles to ensure that citizens are effectively engaged in constructive activities in post-tragedy eras. Thus, our message is that it is not enough to plan ahead to avert tragedies; it is also essential to plan ahead to take advantage of opportunity-bubbles when tragedies do come about.

The present climate of suspicion that pervades public attitudes towards government might well undermine enthusiasm for such planning, as well as confidence in prospects for capitalizing on opportunities. Indeed, distrust has long characterized public attitudes towards government. Throughout the decade following World War II, four out of five Americans reliably claimed broad trust and confidence in their government; by the millennium, only two in five Americans made similar claims.[14] With respect to government institutions charged specifically with homeland security or crisis management and preparedness missions, our own data reveals a parallel and troubling lack of public trust and confidence. Over the years 2006 and 2007, for example, we observed that between 20 and 30 percent of the public claimed "absolutely no confidence" in the Department of Homeland Security (DHS). By December 2008 an even greater proportion (30-46 percent) did not trust DHS would be "open and honest with the public," "provide what was needed when it was needed," or "do the right thing" in the aftermath of a terrorist attack or other crisis – levels of distrust exceeded only by the public's appraisals of FEMA. To make matters worse, popular literature has suggested that government has and will cynically exploit the publics' vulnerability and suffering inflicted by the "shock" of disasters and other crisis to enact highly unpopular political policies.[15]

On the surface, these trends seem disheartening for leadership, because they seem to suggest that citizens will not be influenced by leadership communications. However, to understand why this is not the case, it is useful to remind ourselves of typical behavioral trends in post-tragedy situations. The vitally important feature of opportunity-bubbles is that, for a fleeting period, citizens cast aside their doubts, criticisms, distrust, and negative attitudes, and become ready to sacrifice for the group and strongly support leadership. Thus, although the level of public trust in authorities is generally low at present, we can predict with high certainty that there will be a widespread readiness among the public to make sacrifices for society during the next opportunity-bubble.

## ABOUT THE AUTHORS

***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*** *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) at the Naval Postgraduate School in Monterey, CA.*

[1] A. Stein, "Conflict and Cohesion," *Journal of Conflict Resolution* 20 (1976): 143-172.

[2] Fathali M. Moghaddam, *Multiculturalism and Intergroup Relations* (Washington DC: American Psychological Association Press, 2008).

[3] L. Penner, M.T. Brannick, S. Webb, and P. Connel, "Effects on Volunteering of the September 11, 2001 Attacks: An Archival Analysis," *Journal of Applied Social Psychology* 35, no. 7 (2005): 1333-1360.

[4] Foundation Center, *Giving in the Aftermath of 9/11: Foundations and Corporations Respond* (New York: Foundation Center, 2002), http://www.fdncenter.org/research/trends_analysis/pdf/sept11.pdf.

[5] Pew Research Center, "Trust in Government 1958-2010," in *Distrust, Discontent, Anger and Partisan Rancor: The People and Their Government* (Washington, DC: The Pew Research Center for the People and the Press, 2010), 13-22, http://pewresearch.org/pubs/1569/trust-in-government-distrust-discontent-anger-partisan-rancor

[6] A. Rojecki, "Rhetorical alchemy: American Exceptionalism and the War on Terror," *Political Communication* 25 (2008): 67-88.

[7] T.H. Sander and R.D. Putnam, "Still Bowling Alone? The Post-9/11 Split," *Journal of Democracy* 11, no. 1 (2010): 9-16.

[8] George W. Bush, *State of the Union Address*, January 29, 2002, http://www.whitehouse.gov/news/releases/.

[9] Jim Lehrer, "President Bush defends decision to send additional troops to Iraq," interview by Jim Lehrer, *PBS NewsHour*, January 16, 2007, http://www.pbs.org/newshours/bb/white_house/jan-june07/bush_01-16.html

[10] J.T. Sparrow, "Buying our Boys Back: The Mass Foundations of Fiscal Citizenship in World War II," *Journal of Policy History* 20, no. 2 (2008): 263.

[11] Ibid.

[12] James N. Breckenridge, *The American Perceptions Study: Attitudes and Appraisals of Homeland Security* (Monterey, CA: The Center for Homeland Defense and Security, 2009).

[13] A.D. Grossman, *Neither Dead nor Red. Civil Defense and American Political Development During the Early Cold War* (New York: Routledge, 2001).

[14] Pew Research Center, "Trust in Government 1958-2010," in *Distrust, Discontent, Anger and Partisan Rancor: The People and Their Government* (Washington, DC: The Pew Research Center for the People and the Press, 2010), 13-22, http://pewresearch.org/pubs/1569/trust-in-government-distrust-discontent-anger-partisan-rancor

[15] See, for example, N. Klein, *The Shock Doctrine: The Rise of Disaster Capitalism* (NY: Henry Holt & Company, 2007).

# The Last Days of Summer

James J. Wirtz

Thinking about the recent history and future course of homeland security will be forever tied to a series of events that transpired on a beautiful Tuesday morning in September 2001. The attacks on the United States that day had a profound effect on everyone – witness the outpouring of emotion on the part of the "9/11 generation" following the good news from Abbottabad. But those who grew up in the shadow of 9/11 will never really know what changed that day. Events might suggest to them that people were complacent or careless during the last days of that summer. They also might be forgiven for thinking that people will again become complacent. After all, al-Qaeda is on the ropes and Osama Bin Laden has gone to a watery grave. Why should we continue to care about homeland security? But this would be an incorrect perception of what transpired during the last days of that fateful summer; it is also wrong to use that perception as a guide to the future of homeland security. So what about America and Americans changed on 9/11 and what do these changes hold for the future?

## A Growing Sense of Unease

Looking back on the months leading up to 9/11, it is clear that the intelligence and law enforcement systems were indeed "blinking red." Al-Qaeda was on the move and the United States was failing to take effective action to derail the terrorist network. Scholars have documented that a general feeling of unease had spread across Washington that summer as various government agencies struggled to assess and respond to the emerging threat of transnational terrorism undertaken by non-state actors.[1] The US government was attempting to head off al-Qaeda before the network could act on their nefarious intentions. Ultimately, the government would lose that race.

The academic community also was aware of the emerging threat posed by transnational terrorist networks populated by non-state actors. Although I never considered myself an expert on terrorism, by 9/11 my own work covered several topics that were eerily prescient. I had edited a volume in which one of the authors described the strategic significance and fundamental techniques behind the tradecraft used in 1993 by the terrorists who bombed the World Trade Center.[2] The operatives involved in the September 11 attacks also used the same tradecraft by "hiding in plain sight" to prevent detection by intelligence and law enforcement officials. In the summer of 2001, the US Air Force Institute of National Security Studies also published an edited volume in which I suggested that as the US military bolstered personnel and base security in the Middle East, terrorists might seek "softer" domestic targets within the United States.[3] Neither of these articles came close to predicting actual events, but they do demonstrate that scholars were turning their attention to the threat posed by transnational terrorism.

Two personal experiences in the summer of 2001 also stand out in my mind. The first was a dinner conversation I had with two US Customs officers. The officials had just identified and detained a gentleman from Central Europe who had attempted to use a badly forged Italian passport to enter the United States. The motivations behind the forgery were not particularly threatening, but I do remember expounding at length with the officials about how border security was becoming the front line of American defense. I recognized that it was imperative to stop terrorists from entering the country before they could disappear into various ethnic communities or the anonymity of one of our great cities. The customs officers did not disagree with my position, but they also gave me the impression they thought I was exaggerating the significance of what was to them a rather mundane action.

The second incident was a debate that emerged during a conference sponsored by

the Defense Threat Reduction Agency in Norfolk, Virginia. The debate concerned the likelihood that the United States would suffer a mass casualty terrorist attack. One of the speakers suggested that such an event was unlikely because terrorists lacked the organizational and technical skills needed to orchestrate the use of chemical or biological devices to obtain maximum lethality. The 1996 Aum Shinrikyo Sarin attacks on the Tokyo subway were used to illustrate this point. Despite the fact that the Aum cult possessed significant resources and much technical expertise, their effort to disperse Sarin was rudimentary at best. The other speaker did not dispute this assessment of Aum's prowess when it came to weaponizing Sarin, but instead made a point well known to social scientists: just because something has not yet occurred does not guarantee that it will not happen in the future. Within a few days, this argument would be settled, but not in a way that the conferees had anticipated.

During the final days of that summer, scholars and officials alike were concerned about transnational terrorism undertaken by shadowy groups. "Non-state actor" was a fashionable way to describe non-governmental organizations that were bent on launching destructive or disruptive activities. Officials and scholars also knew that by breaking down barriers to transportation and communication, globalization and the information revolution were making international borders highly porous. For the most part, the availability of these new conveniences was viewed as a positive development. For instance, I remember a trip I made to London in July 2001. I had purchased the plane tickets and made the hotel reservations entirely online. I also abandoned travelers checks for the airport automated-teller machine, which, I was reassured, would allow me to deduct British pounds directly from my American bank account. It was hard to perceive the dark side of this new freedom as one experienced it for the first time. In hindsight, it is easy to see how al-Qaeda was able to "ride the rails" of the information superhighway, but this mixed metaphor itself conveys how difficult it was to envision how terrorists could harness new technologies to create mayhem.

Although some of them were quite novel, all of the pieces of the puzzle were available. There was a growing recognition that globalization and the information revolution were transforming the security landscape. We just lacked a framework to make sense of it all.

## THE NEW AGE

As I watched the World Trade Center collapse, I was struck by the audacity of the terrorists and what I can best describe as hubris, our hubris. We had underestimated our opponents and they had succeeded in striking us in a significant way. Theoretical concepts such as asymmetric attack, porous borders, and "hiding in plain sight" took on a harsh reality as it became clear that we had lacked a sense of urgency during the summer of 2001. We were living on borrowed time and time had run out. It was almost as if Americans were banking on the fact that our opponents would not have the nerve to attack our homeland. Al-Qaeda had plenty of nerve.

It also was immediately clear that our thinking about emerging terrorism was biased towards either well-understood threats (bombing, shooting, hostage taking) or more exotic activities (chemical and biological weapons), not the real problem at hand. Our reality was worse than our imaginations. Al-Qaeda was willing to use locally available materials to create death and destruction. They had identified the high-energy systems that served as the infrastructure of modern society as means to attack the United States. Instead of chemical weapons, for instance, chemical plants now appeared to be a likely terrorist target because they provided access to highly toxic compounds within urban areas. Instead of using time and resources to develop their own weapons, Al-Qaeda recognized that it could weaponize our industrial and transportation infrastructure to attack us. The fact that this infrastructure was not entirely designed to resist unauthorized or unintended uses created a critical problem for the US. Vulnerabilities had to be identified and countermeasures had to be adopted before these weaknesses could be exploited in another devastating attack.

I realized from my previous work on the topic of intelligence failure that it quickly would become apparent that scores of "signals" – accurate and timely pieces of information concerning what was about to unfold – were contained within the files and systems the intelligence and law enforcement communities maintained. Needless to say, officials and analysts had failed to exploit fully the materials that were contained within this "intelligence pipeline." As would become apparent in the following weeks, however, the intelligence problem posed by transnational terrorism was daunting because it crossed scores of organizational and jurisdictional boundaries. Information uncovered by the Central Intelligence Agency, for instance, might have to find its way to a local law enforcement agency to be put to good use, but there was no existing method to move this data in an operationally relevant timeframe. And if the information was highly classified, there was no real way to move the information at all. Local law enforcement officials lacked the required security clearances or facilities to receive or store classified reports. Additionally, local law enforcement agencies were now on the front lines. Information collected during a traffic stop, for example, might be critical to an ongoing analysis by the Federal Bureau of Investigation or Customs officials. But there was no way for local officials to communicate information in an operationally relevant timeframe to federal agencies that focused on international threats. Al-Qaeda was hiding within the operational and jurisdictional seams that existed between the US military, the intelligence community, and law enforcement agencies. The fact that our opponents were exploiting these seams created a critical vulnerability that had to be quickly eliminated.

9/11 did not "change everything," but it demonstrated that the threat posed by transnational terrorism was real and immediate. Our opponents had chosen to attack us; they had chosen war. The idea that we could respond in a leisurely way to the emerging threat, that we were somehow ahead of the terrorists, was gone forever. We could not count on controlling the pace of events. It also quickly became evident that al-Qaeda had chosen to exploit vulnerabilities embedded in the very infrastructure of modern life. Potential threats were intermingled within our cities because scores of high energy or potentially toxic systems permeated our infrastructure. Weapons suitable for mass destruction or mass effect were already in place within the United States. What the terrorists needed was an innovative or cunning plan to gain access to them. Our defenses were poorly configured because they reflected a sharp distinction between foreign threats, which were primarily the responsibility of the military and intelligence community, and domestic threats, which were the purview of law enforcement agencies. There was a distinction between the "front lines" and "the rear" when it came to our thinking about threats. That distinction no longer seemed appropriate, but just about every resource, organization, and concept we possessed reflected distinctions between foreign and domestic security as well as military or intelligence activity and law enforcement. Overcoming these weaknesses, which were exploited by al-Qaeda on 9/11, animated our activities during the first homeland security decade.

## THE FUTURE OF HOMELAND SECURITY

There have been several important developments since that fateful summer. We now recognize the importance of intra-governmental relations in defeating the terrorism threat and the need to share information, resources, and best practices across federal, state, local and tribal jurisdictions and agencies. We now understand the importance of collaboration and cooperation among law enforcement, fire, emergency medical services, public health, and intelligence officials to generate the situational awareness and capabilities needed to combat the terrorism threat. We also recognize that we have to work to bridge the boundaries between jurisdictions and agencies to prevent our opponents from operating within the seams of our defenses.

Today, homeland security programs and policies are less animated by a crisis atmosphere and instead reflect the notion that emerging best practices have to be

embedded within a wider range of intelligence, law enforcement, and other public service programs. In a domestic setting, the activities of most public officials and agencies are directed at meeting myriad demands for support and services that have little to do with transnational terrorism. Programs that are intended to respond to the ongoing threat of terrorism have to help bolster capabilities when it comes to the "all-source threat" focus of the vast majority of law enforcement, fire, public health, and emergency medical service agencies across the country. Instead of remaining an "extraordinary" activity, homeland security in the United States is becoming part of everyday life because it is slowly but surely improving the ability of federal, state, local and tribal agencies to prevent and respond more quickly and effectively to all sorts of threats and incidents.

For theoretical, practical, and operational reasons, incorporating an "all-threat" approach to homeland security is a positive development. From a theoretical perspective, it is difficult to anticipate the exact nature and best response to future threats. It is better to foster broad situational awareness across a variety of jurisdictions and disciplines (e.g., border patrol, public health, or the chemical industry), to look for unanticipated developments or new patterns of potentially disruptive activity. From a practical perspective, it is simply not politically possible to devote large portions of scarce public funds to respond to a mercifully rare type of event (i.e., a mass casualty terrorism attack), while communities suffer from a long list of mundane problems. Homeland security initiatives that help communities respond to local problems will enjoy greater political support than activities that seem to deal with rarified issues of little immediate significance. From an operational perspective, an "all threat" approach can help improve communication across disciplines, agencies, and levels of government because it fosters better interaction in dealing with everyday events. By making data fusion and operational cooperation a matter of routine, "all-threat" collaboration can serve as the basis for prompt detection and defense against a potential terrorist incident.

There is also evidence that our overall situational awareness and response protocols continue to improve. The quick and effective action taken by local bystanders and patrol officers during the 2010 Time Square bombing incident suggests that average Americans feel empowered to respond to suspicious situations and that police and fire departments possess appropriate procedures once suspicious activity is reported. The car bomb in Times Square failed to detonate, but if it had, quick action by the New York City police and fire departments would have helped to limit casualties from a bomb blast.

Because the attitudes of Americans have changed, efforts to improve homeland security are now embedded in a general way in public policy and our attitude towards national security. Ten years after 9/11, the crisis atmosphere has faded, but organizations and agencies everywhere recognize the imperative to strengthen homeland security and to include homeland security "best practices" across a range of public service activities and agencies. The emergence of homeland security as a "process" is a phenomena that will gain strength in the years ahead. This process has already stopped several significant terrorist plots before they could unfold. It also has made the United States a far less hospitable place for clandestine terrorist networks.

## CONCLUSION

Before 9/11 it *might* have been possible to write this essay, but I doubt that it would have been published. The threats described would have appeared implausible. Reviewers might have granted me the fact that launching a mass casualty terrorist attack using materials at hand was possible, but such an act would have appeared to lack strategic justification. I also doubt that manuscript reviewers would have been willing to grant that our opponents possessed the motivation or operational skill to pull off this type of operation, or could easily slip through our security measures. In other words, one could have posited a perfect storm attack, (e.g., terrorists armed only with box cutters succeed in destroying the World Trade Center in a few hours), but it would

have been dismissed as either alarmist or foolhardy.

The fact that we now believe that we could (again) be the victim of a mass casualty terrorist attack and that it is a mistake to underestimate the ingenuity and determination of our opponents marks the most important way Americans have changed in the aftermath of the September 11 attacks. This is the greatest lesson we learned on that last day of that summer. We no longer are living on borrowed time, we are working to recognize and overcome our weaknesses.

## ABOUT THE AUTHOR

***James J. Wirtz*** *is dean of the School of International Graduate Studies, Naval Postgraduate School and director of the Global Center for Security Cooperation, Defense Security Cooperation Agency.*

[1] Stephen Marrin, "The 9/11 Terrorist Attacks: A Failure of Policy Not Strategic Analysis," *Intelligence and National Security* 26, nos. 2-3 (April-June 2011): 185.

[2] J. Bowyer Bell, "Conditions Making for Success and Failure of Denial and Deception: Nonstate and Illicit Actors," in *Strategic Denial and Deception: The Twenty-First Century Challenge,* Roy Godson and James J. Wirtz, eds. (New Brunswick: Transaction Publishers, 2002), 129-162,

[3] James J. Wirtz, "Antiterrorism via Counterproliferation," in *The Terrorism Threat and US Government Response: Operational and Organizational Factors,* James Smith and William C. Smith, eds. (USAF Institute of National Security Studies, 2001).