Notes from the Editor

- Christopher Bellavita

Beyond the HSC/NSC Merger: Integrating States and Localities into Homeland Security Policymaking
- Paul N. Stockton

Merging the HSC and NSC: Stronger Together
- Christine E. Wormuth and Jeremy White

Technology Strategies for Homeland Security: Adaptation and Coevolution of Offense and Defense
- Brian A. Jackson

The Terrorist Threat to Inbound U.S. Passenger Flights: Inadequate Government Response
- Anthony Fainberg

ARTICLES

Just How Much Does That Cost, Anyway? An Analysis of the Financial Costs and Benefits of the “No-Fly” List
- Marcus Holmes

Competing with Intelligence: New Directions in China’s Quest for Intangible Property and Implications for Homeland Security
- Robert C. Slate

Community Health Centers: The Untapped Resource for Public Health and Medical Preparedness
- Karen M. Wood
Notes from the Editor

In this issue of Homeland Security Affairs we offer one essay that outlines some of the important homeland security issues of 2008 and a set of essays that describes a potentially significant change in the national homeland security architecture. This edition also has two essays about homeland security technology. One applies coevolutionary theory to the strategic question of how to defend against an adaptive adversary; the other discusses policy and technology changes that could improve aviation safety. We present an article that demonstrates how to determine the benefits and costs of homeland security spending and an article that discusses threats from China to American corporations and to homeland security. The issue concludes with an analysis of how Community Health Centers can be an integral part of the nation’s public health preparedness.

In our second annual “Changing Homeland Security: Year in Review – 2008” Christopher Bellavita reports on what a selected group of homeland security professionals considered 2008’s top stories. Their survey responses included the presidential election and its impact on homeland security, the terrorist attack in Mumbai, the domestic and international economic meltdown, chaos on the southern border, the continued quest to define homeland security, and an expanding threat spectrum. Bellavita also includes three candidates for the “Homeland Security Image of the Year.”

Should the Homeland Security Council (HSC) and the National Security Council (NSC) merge? As we prepare to publish, most signs indicate the merger will take place. Christine E. Wormuth and Jeremy White present the argument in support of the merger. In “Merging the HSC and NSC: Stronger Together,” the authors note that at the federal level homeland security is essentially an interagency activity. White House leadership is the only practical way to ensure unity of effort among federal agencies. Merging the NSC and the HSC into one organization can end the bifurcation of national security and homeland security. A single council will give the president a way to develop and implement homeland security policy that is integrated with other national security initiatives.

Paul N. Stockton, in “Beyond the HSC/NSC Merger: Integrating States and Localities into Homeland Security Policymaking,” agrees that merging the NSC and the HSC seems inevitable. But the change brings risk. Stockton argues that if the councils are combined, administration officials will need to pay special attention to a number of issues, including the danger that homeland security will take a back seat to traditional national security priorities. The president and the newly structured council will also need to address significant challenges of horizontal integration (i.e., across federal agencies) and vertical integration – the inclusion of state and local representatives in the work of the council. Stockton reviews the possible problems with a merger and suggests solutions.

In “Technology Strategies for Homeland Security: Adaptation and Coevolution of Offense and Defense,” Brian A. Jackson frames the dynamic between terrorist groups and security forces as a coevolutionary process. Highlighting the use of technology by both homeland security organizations and terrorists, Jackson
describes how terrorists adapt to defensive technologies and how homeland security organizations must then develop measures to counter those adaptations. He argues that trying to create impenetrable defenses for every target is futile. Instead he suggests that defensive technology strategies should exploit evolutionary dynamics by shaping adversary choices and by using defensive approaches that are insensitive to terrorist adaptation strategies.

Anthony M. Fainberg’s essay, “The Terrorist Threat to Inbound U.S. Passenger Flights: Inadequate Government Response,” illustrates the interface between technology, politics, and security. He writes that the Transportation Security Administration (TSA) seems reluctant to focus on security for aircraft flying into the United States from abroad. Reviewing the decades-long history of terrorist attacks on commercial aviation, Fainberg notes how al Qaeda has tried more than once to simultaneously destroy several U.S. aircraft, in flight, by using suicide bombers ticketed as regular passengers. He argues that countries from which inbound flights depart should agree to security standards that match those applied to domestic flights, including using explosive trace detectors to inspect passengers and their carry-on items.

In “Just How Much Does That Cost, Anyway? An Analysis of the Financial Costs and Benefits of the ‘No Fly’ List,” Marcus Holmes offers a unique financial cost and security benefit analysis of the United States government’s “no fly list.” On September 11, 2001 the no fly list contained sixteen names of terrorists and other individuals deemed threatening to the states. Since then, the list has had more than 755,500 names. Holmes writes that while there has been considerable interest in the social costs of the list, there has been little attention paid to the financial costs relative to the benefits. He claims it is unclear how one can create a strategy for how national security dollars should be spent without knowing how many dollars are involved and where they are going. Holmes’ study is a path-setting step in asking and answering an important question: what are the costs, relative to the benefits, of anti-terrorism policies and security strategies?

Robert C. Slate is the author of “Innovating with Intelligence: New Directions in China’s Quest for Intangible Property and Implications for Homeland Security.” He argues Chinese corporations that use intellectual property theft and infringement in their business model are significant threats to the intangible property of the American corporate world and pose a serious threat to homeland security. Slate describes how Chinese corporations, universities, and research institutions use intelligence principles to help China become an economic superpower. He calls for the U.S. intelligence community to rethink its traditional approach to collecting and analyzing information about China.

Homeland Security Presidential Directive 21 outlines a new approach to public health and medical preparedness in the United States. In “Community Health Centers: The Untapped Resource for Public Health and Medical Preparedness,” Karen M. Wood writes that the more than 1,200 community health centers (CHC) in the nation are well-positioned to play a significant role in that effort. Wood describes how CHCs can improve biosurveillance, countermeasure distribution, mass casualty care, and community resilience. She argues that aggressive investment in the centers and their emergency management programs can make
public health emergency management more accessible to special-needs populations and support many of the objectives identified in HSPD 21.

We hope you find the articles in this issue of Homeland Security Affairs informative and thought provoking. As always, we invite you to contribute your own research and ideas to the continuing conversation about homeland security.

The Editor

Christopher Bellavita

*Everything we hear is an opinion, not a fact. Everything we see is a perspective, not the truth.*

- Marcus Aurelius (121-180)

What events and trends shaped the homeland security terrain last year?

In December we asked members of the Naval Postgraduate School’s extended homeland security network to respond to two questions:

- *From your perspective – and using whatever criteria you’d like – what would you say was a top homeland security-related issue or story in 2008? And why?*
- *Please identify something you consider to be an emerging homeland security issue. (For the purposes of this question, emerging issues are embryonic concerns that may develop into significant problems or opportunities in the future.)*

Their responses highlighted the 2008 presidential election, the terrorist attack in Mumbai, the economic meltdown, the chaos on the southern border, the continued quest to define homeland security, and an expanding threat spectrum, including the cyber threat – possibly the year’s most underreported homeland security issue.

Taken together, the responses from the NPS community of practitioners and academics who work in and think about homeland security everyday tell a story about the field’s continuing evolution. Before presenting the full survey results, here is the summary of the 2008 story.

THE YEAR IN BRIEF

Barack Obama’s election portends changes in homeland security and in the Department of Homeland Security. The changes might be foundational – for example separating FEMA from DHS – or they may emerge from the muddle of disjointed incrementalism.

Homeland security was not an important issue during the campaign. This and other evidence suggests homeland security has become a second-tier policy issue, more important to a small group of bureaucrats, elected officials, corporations and scholars than to the electorate. One respondent said the public will not pay attention "until we bleed again."

The Mumbai attack reminded us that the bad guys are still around. They do not need nuclear or biological weapons. Low-tech attacks on soft targets in the U.S. can create high-consequence events. Weapons of mass destruction continue to pose a threat to the nation. But attention to WMD threats may distract state, local, and federal agencies from the training, resources, or focus appropriate to prevent Mumbai-like attacks.

The economy presents another challenge to homeland security. The same state and local agencies we rely on to prevent and respond to homeland security incidents face significant budget cuts. Public safety agencies must decide how to provide basic services to their constituents. Increasingly the issue is which people to layoff and which services
to no longer provide. Homeland security is becoming a "nice-to-have" service in a growing number of communities.

Obama has proposed a multi-billion dollar initiative to create jobs and revitalize the nation's infrastructure. Depending how security concerns are incorporated, the program could mitigate or amplify basic homeland security challenges.

Some good things happened in 2008. It was one more year the nation was not successfully attacked at home. The response to the Gulf hurricanes, the Midwest floods and the western wildfires was improved when compared with similar incidents in prior years. Borders are less porous. The numbers of illegal immigrants did not increase substantially and – for a variety of reasons – may even have decreased. Port security has been enhanced. Resiliency has taken on increasing importance. Even the DHS efforts to have September treated seriously as National Preparedness Month may be taking root in the nation.

Americans continue to support government efforts to prevent terrorist attacks. But, as one respondent phrased it: "There does seem to be a sense that America must maintain its moral compass and not alienate itself from the rest of the world.... Being the leader by example of democratic principles for the world is still important."

Coordination and information sharing among federal, state, and local agencies continues to improve. Some of our respondents believe critical problems remain in this domain. One person noted that the Maryland State Police admission that they conducted improper surveillance on Americans could have national implications for fusion center operations.

The homeland security threat spectrum widened in 2008. In part, that may reflect an empirical reality. It may also be the aggregated perception of people whose job is to find threats and prevent them from being realized. More people were killed last year in the Mexican drug wars than died on September 11, 2001. The instability of the southern border presents new opportunities for terrorist safe havens. The specter of homegrown terrorism has not abated. Naturalized citizens of Somali descent traveled to Africa for jihad. One Minneapolis man, Shirwa Ahmed, blew himself up in a suicide attack in Northern Somali. The election of the first black American president may reignite the racial hatred of more traditional domestic terrorist groups.

Secretary Chertoff called cyber security the nation's "last major vulnerability." Cyber is also a global threat. Last year saw an increase in the number of efforts to penetrate government and private sector networks. The penetrations could be reconnaissance probes before a wider domestic operation. According to one of our respondents, during the Russian invasion of Georgia "a criminal network believed to be operating in Russia was conducting cyber attacks against the Georgian government from computer servers located in the United States."

The international scene highlights additional threats. Afghanistan remains Al Qaeda's incubator. In addition to Mexico, trends in China, India, Pakistan, Iraq, Iran, Russia, Africa, and Venezuela remind us that attending to homeland security does not mean looking only within the country's border. The number of nations with a presence in space is growing. There are homeland security implications to this development.

Climate change, economic security, food, water, and energy security are seen by some of our respondents as meta hazards that could have a more significant impact on domestic security than terrorism.
The public health and emergency health infrastructure remains inadequate to prevent and respond to significant mass casualty incidents, biological attacks, drug resistant infectious diseases and related threats. Chemical security remains a national problem. Pirates and their small boats have moved from Disney amusement to global menace.

Thomas Jefferson wrote that a politician looks forward only to the next election; a statesman looks forward to the next generation. American elections provide the opportunity to rejuvenate the nation. The year 2009 brings new women and men to responsible homeland security positions. They have the opportunity to review and learn from the work of the statesmen and women who came before them. Based on what has and has not worked, the nation’s new homeland security leaders at all levels of government can write the next chapter in our continue efforts to, in Jefferson’s words, "insure domestic Tranquility, [and] provide for the common defence."

TOP HOMELAND SECURITY STORIES OF 2008

The people who responded to this year’s survey did not mention every major issue. The findings are as much a function of the interests of people who took the time to respond to a survey during the holidays as they are an unfiltered reflection of empirical reality. If themes you consider important are not mentioned here, you are invited to submit, via email, your thoughts for inclusion in the next issue of Homeland Security Affairs.

The survey respondents' observations that follow are arranged in the following categories:

• The Promise of Obama: The Ambiguity of Change
• The Attack in Mumbai: "This could easily happen anywhere in the US."
• The Economic Crisis: "Bin Laden's victory over America?"
• The Nature of Homeland Security: Now a Second Tier Policy Issue?
• Organizing for Homeland Security: Possible Futures, Emerging Issues
• The Department of Homeland Security: Time of Opportunity
• The Federal Emergency Management Agency: Will You Stay or Will You Go?
• The Good Things
• The Threat: Are We More Vulnerable Now than We’ve Been in the Past Decade?
  o The Southern Border
  o Domestic Threats
  o Cyber Threats
  o Threats From Other Nations
  o Public Health Threats
  o Other Threats
• The Culture of Preparedness: “Waiting until we bleed again”
• Meta Hazards: Things We Do To Ourselves
• Funding Concerns
• Professionalization of Homeland Security
• Information and Intelligence
• Critical Infrastructure: Jobs And Security
• Criminal Justice and Homeland Security
The article closes with three candidates for the “Homeland Security Image of the Year.” But first, here is what our respondents considered to be significant trends and themes for 2008 and the future. These responses are direct quotations, lightly edited for clarity and presented without attribution; each paragraph represents one individual’s thoughts.

**The Promise of Obama: The Ambiguity of Change**

The campaign for and election of the U.S. president represents the top homeland security issue for 2008. The two candidates articulated very different visions for the ongoing war in Iraq. One candidate presented as the man who would continue the fight until it was concluded and the enemy vanquished. The other candidate argued for a quick end to U.S. involvement. Domestic and economic issues – and virtually all talk of terrorism and homeland security – overshadowed this entire issue. Whether this was because of the issue attention cycle, threat fatigue, or economic worry, it was clear that the threat of terrorism was not on the front burner for American voters.

In 2008, the American people voted for a "new narrative" in homeland security and the so-called war on terror. President Obama's statements indicate he understands the current "military only" approach to fighting terrorists is incomplete and counterproductive. Instead, his approach seems to be to meld the hard power of the military, designed to destroy terrorism's hard core, with the so-called soft power of diplomacy, economic assistance, education, and information, designed to strengthen the mainstream in Muslim countries. Opinion polls in the Muslim world indicate the majority of Muslims believe the current war on terror is really a war on Islam by the United States and the West. We will never beat the terrorists until that perception is changed. Mr. Obama promises to make a major address in a Muslim country in the first 100 days of his administration explaining that we are not at war with Islam, but that we are fighting a common enemy: violent radical extremists who seek to hijack Islam and terrorize us all. He appears ready to reverse the cowboy diplomacy of "my way or the highway," with a search for common ground that can stop radicalization in its tracks. The success of this new narrative will determine the security of our homeland for decades to come.

In the national elections of 2008, the American public demonstrated a turning of the popular will against that part of the war on terror represented by the war in Iraq, by changing the executive branch of government from Republican to Democrat, and by increasing the Democrats’ majority control of the Congress.... Despite claims by the outgoing administration that the war in Iraq is critical to the war on terror, these results indicate that, similar to the Vietnam War, the administration has failed to mobilize and sustain the popular will of its constituents. It remains to be seen what war on terror, homeland defense, and homeland security policies the incoming administration will implement.
The primary issue in the 2004 election was the threat of terrorism. The 2008 election seemed to revolve around getting revenge against the president and the other people who have been in charge of the global war on terrorism.

The top story was the one that did not happen during the presidential campaign: the lack of homeland security as an issue for debate. Homeland security was never on the radar screen and seemed to be intentionally not an issue, so the Republican candidate could not get any traction on a substantial tide-turning issue. Just as the economic downturn provided the pivotal momentum for President Obama's success, a terrorist-related event could have turned the outcome to a success for Republicans. Timing is everything in life.

The top story was the lack of focus on homeland security during the campaign and transition. In an attempt to separate candidates from the current administration, both candidates downplayed homeland security issues, with one or two minor exceptions. Some candidates published their [homeland security] positions online. Those documents are no longer available. Other candidates dismissed the issue altogether. Like it or not, homeland security is a major issue at this time in history. While it may not be on the forefront in the public eye, it requires much more attention than it has received.

The election of the first president since the DHS was formed has and will continue to significantly influence the world of homeland security.

The election will bring in a new set of players who will set a new standard for homeland security.

In the latter half of 2008, a number of organizations involved with homeland security focused on political and government transition. There are a number of groups working on documents for President Obama to read. These documents are designed to educate and influence Obama and other newly elected or appointed officials. Are these documents consistent with current direction or are they recommending change? Is there consistency in the message from these multiple documents? One would guess no. A concern that many in DHS and their homeland security partners share is the constant "crazy quilt patchwork" of direction that seems to permeate the overall homeland security effort. Will consistency in direction eventually be achieved and will these [transition] documents be helpful or hinder the efforts of pulling together for the common purpose of securing the homeland?
The Obama administration may move to limit the duplicative bureaucracies the Department of Homeland Security has created since its inception. The new administration may move to decentralized DHS offices and programs out of their cocoon in Washington, DC.

Our homeland security is critically impacted by what other countries (and their citizens) think about the intentions and behavior of the United States. If this new administration can keep the international momentum that has already started, it could have an effect on reducing future threats.

How will Obama treat homeland security? Where will his leadership take us? Will he reconsider describing the fight against terrorists as a "war?"

The [new] administration has already set the tone of debate and what is in the best interest of the country. Those vested with an interest in homeland security should examine their views from the lens of ensuring continued economic prosperity of the nation and preserving the freedoms and liberties set forth in the U.S. Constitution and Bill of Rights, as opposed to maintaining a positional stance.

The administration change will bring new priorities shaped from a liberal socialist rather than a neoconservative perspective. I'm interested to see what the difference is once the politicos fully understand the available intelligence.

The scary thing about the election of Obama is a potential for the revival of domestic terrorists. I would hate to see how we as a nation would respond to the assassination of a president by domestic terrorists.

The Attack in Mumbai: "This could easily happen anywhere in the U.S."

The recent attacks in Mumbai demonstrate that this form of attack is possible in the U.S.A. It appeared to be relatively inexpensive, did not require extensive planning, and the terrorists were able to accomplish their goal – instilling fear and terror in support of their cause. While we look at potential threats, such as nuclear, chemical, bio, and other types of attacks, we should not take our eyes off of this emerging threat of simultaneous "Mumbai style" attacks in various parts of the U.S.A.
The top story was the bombing in Mumbai. This incident marks the evolution of complex attacks in the revival of a fifteen-year-old plan of execution for the terrorist. This incident creates new attack environments for communities to prepare for.

♦♦♦

The Mumbai attack certainly has to be considered for placement on the list because of the effectiveness of the methods used (low-tech, soft target, high consequence), intelligence warning of the attacks (apparently heeded for a few days, then "back to normal" just prior to the attacks), and the apparent lack of readiness by local responders to quickly neutralize the situation (adequately prepared responders were hours away). I’m sure we all thought the same thing when the news broke: "This could easily happen anywhere in the U.S. today."

♦♦♦

What do the Mumbai attacks mean for the future of anti-terrorism and future terrorist tactics?

♦♦♦

The Mumbai attack in India demonstrated again the urban vulnerability to a small band of attackers.

♦♦♦

The Mumbai attacks showed that asymmetric tactics used by a small, determined group can have devastating effect.

♦♦♦

On the maritime side, the top story was the increasing concern relating to the small boat threat; this threat increased even more after the Mumbai incident.

♦♦♦

The tactics used in India were identified by our [NPS] students repeatedly over the last five years as likely next steps by terrorists. I'm interested to see if it actually brings a change in tactics or if this was just a one-off.

♦♦♦

It is too early to see if Mumbai will lead to new trends in attacks, but it seems likely that more quasi-military attacks will be conducted in the future.

♦♦♦

The Mumbai attacks were noteworthy because of the tactics employed. There were no explosives, youthful perpetrators, suicidal bent, technologically advanced means and methods, prolonged implementation... all continue to indicate that the face of terrorism is changing. Relate this to Columbine, the Moscow theater, and the Beslan school killings. We may be directing our training and education efforts to the wrong threats. The local police departments will assume a much larger role than previously anticipated, and they are not ready.
There were several points where the attacks could have been disrupted had people been more sensitized to what was going on (or were less apathetic) or if the police and security forces had more capacity: hijacking of fishing vessels, transfer to small boats, walking from small boats up the pier to get in a cab. The attackers could have been disrupted during each of those steps. Once the attacks began, local law enforcement didn’t have the resources to stop the attack, and it took several days for the higher end forces to get into position and be ready to assault. Why did it take so long? For us, could a similar attack happen? And what capabilities or capacity do we have to prevent or disrupt such an attack?

The Mumbai attacks were a demonstration of the continued preparation and planning that is ongoing by terrorists. The terrorists continue to attack the U.S. even though it is not on our soil. This is a message to the rest of the world, an attempt to turn U.S. allies and their people against the West.

Mumbai has caused all of us to refocus on preventing and responding to low-tech, high-consequence activities by committed terrorists and criminals in the United States. We have devoted substantial resources towards detection, prevention, and response of many WMD events. But if terrorists plan to use low-tech events in the United States (and I don’t see any reason why they would not, especially given the apparent difficulty in conducting IED/WMD events), we will all have to rethink our surveillance and prevention activities if we are to effectively address them. Stop these incidents before they happen; stop them if they happen. This will become an even greater challenge, at least in the short-term, as we all struggle to address the fallout from very difficult economic times – hiring freezes, furloughs, reduction in forces, and so on.

Mumbai: for those doubters, the threat is still here!

The Economic Crisis: "Bin Laden's victory over America?"

The top issue for me is the economy this past year, and how events starting from September 2001 have shaped our financial standing with the world.

I think the top homeland security related issue is bin Laden’s victory over America. After all, he said his goal was "... bleeding America to the point of bankruptcy...." Okay, okay, so I realize we did a lot of this to ourselves with unsound and risky banking and loan policies, but one can’t help but wonder what impact this economic crisis will have on our national security.
I believe the top homeland security-related issue in 2008 is the meltdown of the United States and the world economy. I think it directly affects our national security in several respects. Psychological fear created by the economy further erodes the nation's confidence in the government to take care of any business .... There is less money available for the military, State Department, all hazards and security. ... As if we have not forgotten 9/11 and Katrina enough already, this further takes our eyes off of the ball. As some shrewd politician once said, it is the economy stupid.

The top story is the impact of the economy on homeland security and the sustainment of current capabilities.

The top story was the financial downturn. Public safety agencies at the state and local level are increasingly pressed to maintain basic services, let alone prepare for low-frequency, high-impact operations such as homeland security. Funding is increasingly needed to sustain basic public safety operations, let alone homeland security functions.

The nation's economic downturn is definitely starting to impact homeland security. Many local and state governments have experienced budget cuts that directly affect homeland security capabilities. It is predicted the economy may get worse or maintain its dismal state for a year or more before it will rebound. If this turns out to be true, even greater budget cuts can be expected. The challenge that we currently face is how we will be able to ensure homeland security with a dramatic decrease in resources.

Fire service involvement in homeland security is being affected by the failure to recognize the cost of that involvement. Current fiscal practices require departments to make decisions about the importance of what they should and can be involved in based on constrained funding. Failure to acknowledge personnel costs, which can be ongoing, will affect involvement. Equipment needs can be met, but backfill costs are stripping departments of day-to-day resources, unlike other agencies.

The obvious choice for the top story is the financial meltdown. We cannot run an effective government on any level without the financial machine to sustain it. This creates an opportunity for terrorists.
The economic crisis plays a role in diminishing our deterrence. It has an ongoing impact on funding and preparedness.

♦♦♦

The big story is the effect of the economic downturn on the ability of government to provide funds or prioritize funds for homeland security purposes.

♦♦♦

The looming world economic collapse is going to affect all aspects of our homeland security and defense initiatives.

♦♦♦

The economy will limit our budgets and make us more vulnerable as many of our own newly unemployed population become desperate and/or sick.

♦♦♦

The economic and fiscal crisis will exasperate an already challenged homeland security mission and will force the question of how the nation should optimize its security investment, given its declining strength in the world community. Hard choices will need to be made across government and every organization will fight for survival – especially the active components of the military.

♦♦♦

I think an emerging homeland security issue is how the nation is going to balance expensive national security initiatives with the more pressing social and economic concerns of the citizenry.

♦♦♦

The economy will be the primary driver of emerging definitions of the homeland security mission space in 2009.


Has the bar for national discourse been raised beyond the need for reflective thinking and strategic discussions as it relates to the concept of homeland security? I suggest the top homeland security-related issue of 2008 is that the general concept of homeland security is no longer a compelling national story that provides an impetus for the topic to be discussed in any substantive detail. The presidential election, downturn in the economy, Iraq, and Afghanistan appear to have consumed the nation's attention and left little room for discussions relating to numerous other issues of importance – including homeland security. While this lack of national discourse could be viewed positively – oftentimes such discussions only arrive after a dramatic man-made or natural disaster grabs the nation's attention – it might be argued that such discussions should occur during times of crisis and calm. In September 2008, the third most destructive U.S. disaster, Hurricane Ike, was responsible for eighty-five deaths and caused $27 billion in damage. Yet, like the aftermath of Hurricane Katrina, little national attention has
been given to the slow recovery efforts for tens of thousands of citizens who continue to be displaced from their communities. Based on the enormity and complexity of the issues our nation faces – continuing deaths in a trillion-dollar global war on terror, coupled with a trillion-dollar government bailout and economic stimulus package – I wonder if the nation has become conditioned to giving sustained attention solely to the most significant issues of the day, with homeland security destined to return to the public forum only after the next catastrophic failure.

 três

The most pressing issue in homeland security in 2008 was not an event, but rather the continuing confusion and lack of clarity surrounding the term "homeland security." There is a dysfunctional absence of understanding about what constitutes "national security" and "homeland security," to say nothing of the fact that emergency management finds itself, at the federal level and within some states, buried within departments of homeland security, but not part of the national homeland security strategy (which deals exclusively with terrorism). There has been no national dialogue and consensus regarding the responsibilities of the federal government vis-à-vis state and local jurisdictions in terms of "homeland security." There has been no movement on a workable, comprehensive program that addresses illegal immigration issues, the borders remain porous, and our seaports, rail systems, and other infrastructure remain largely unprotected while the Secretary of Homeland Security has become an expert on the behavior of cyclonic advance and levee construction.

 três

The top story is the emerging requirements of first defining and then structuring exactly what homeland security is. Is it economic, physical, environmental, health, energy... or all of those, with no practical gravitas placed on any one sector? We must nationally identify and modify our current behavior and expectations if we are going to actually have a policy or just another dance with money and innuendo.

 três

Homeland security, conceptually, is about redefining. It is not about the organic creation of inherent value. This is demonstrated by observing that the lessons learned from Katrina were applied to Gustaf and Ike. The preparation and the recognition of responsibility were the two big homeland security milestones in 2008 for the federal government.

 três

Homeland security has become second tier to other issues, such as the new administration, the economy, and housing, just to name a few. This will cause homeland security departments and professionals to compete for attention to get funding support for their programs.
The emerging homeland security issue is a conceptualization of homeland security as a bureaucratic paradigm not a unique theoretical discipline. The value of homeland security is the avenue it creates for government personnel to act non-possessively and, of course, the impetus to act at all.

♦♦♦

The drawdown of forces in Iraq will actually cause a surplus of military personnel in the U.S. We are already seeing that trend in efforts to redefine the military's domestic role. As the active component competes for domestic relevance with the National Guard, you may see these two giants try to remodel homeland security for their own benefit. Some of this is already happening.

♦♦♦

The important emerging issue is the future role of DHS in relation to national security. Think tanks, members of the U.S. Congress, and professional associations, for example, have two basic opposing views on emergency management, the role of FEMA, and responsibility for terrorism, border, and immigration control. In sum, the debate continues about the future organizational structure best suited nationally to deal with these issues. Some states are concerned that removal of FEMA would further erode its ability to deal with disasters. Others think better focus will come with a separate entity reporting to the president. Since Congress neither debated the creation of DHS nor the appropriate organizational government response to 9/11, I predict that 2009 will be the watershed year for debating major homeland security structural, policy, and budgetary changes with the new administration. The new team owes Congress the first ever quadrennial homeland security review, which requires an assessment of homeland security and recommendations for priorities.

♦♦♦

The key emerging issue will be keeping the momentum going in the face of relative calm. We are fortunate not to have had strategic attacks on the homeland since 9/11. In the face of this calm, other competing interests will emerge such as the immigration/border issue, and an increase in global partners pushing back against U.S. requests. The predominant issue (absent an emergency) should be identifying a concise mission for DHS. I feel DHS needs to be engaged in preventing strategic level attacks on the U.S. and not preoccupied with disaster response. Move FEMA out.

♦♦♦

The emerging issue is perception versus reality in terms of to what degree the federal government can or should provide a "national 911." Rather than focusing resources on building capacity at state and local levels, there is a perception (often fostered by self-serving appointees) that FEMA and DHS will "be there for you." This has led to misunderstandings at all levels and the under-funding of state agencies by state legislatures that, in the coming year, will result in diminished capacity to respond.
The time is now to think outside the box, deconstruct unnecessary bureaucracy, develop essential capabilities, and strengthen our communities at the core level.

**Organizing for Homeland Security: Possible Futures, Emerging Issues**

The biggest questions to emerge are how the new administration will handle homeland security, whether budgets will remain at current levels, and whether FEMA will stay in DHS.

The top emerging issue is the collapse of homeland security systems designed and built over the last few years. We've spent billions on homeland security-related issues, building capabilities and capacity on top of those capabilities. We are slowly eroding away the capacity and will be chipping away at capability very soon, capabilities which will take years to rebuild once they are lost.

An emerging issue is the level of interest and funding support for homeland security in the new administration. Public support and interest is at an all-time low and recent polls indicate that over 70 percent of the public feels safe and believes there will not be another terrorist attack. With the Department of Homeland Security barely five years old, this could be a make or break period for the whole concept. Look at the mounting political pressure to remove FEMA from DHS. Short of another attack I see homeland security losing both funding and status. This situation requires a clear perception and expression of homeland security's value by the new president. It also requires a strong commitment to strengthen the leadership and capabilities at DHS.

Because of economic constraints, we should expect more effective collaboration between the federal government and the local governments.

Expect to see more restructuring of homeland security efforts from separate operations into an integrated part of day-to-day operations. This will happen because it is a financial necessity.

A major emerging uncertainty is the future of state and local homeland security-specific offices. Most of them were created in the immediate aftermath of September 11, 2001. As the mission of many homeland security offices has begun to "creep" into the arena of existing state and local emergency management offices, there seems to be increasing discussion about what the future mission of the offices of homeland security should be.
The concept of a "DHS" is fine and there is value to a cabinet level agency with oversight of the U.S. effort. Unfortunately, the turf wars continue and involve the FBI, CIA (and the entire intelligence community), as well as DHS. I doubt there is enough political will to properly align the agencies. The bright spot of the DHS is its legacy components and their mission focus.

A top issue according to several think tanks is merging the Homeland Security Council and the National Security Council (NSC). The announcement of a national security team by the president-elect included no person for a Homeland Security Council role. Merging the two entities would focus national policies and priorities on national security so federal departments and agencies would have a single entity in the White House. It would also focus discussions with Congress, perhaps leading to a reduction in the eighty-six committees and subcommittees dealing with the Department of Homeland Security. And if the incoming administration has an entity within the NSC dealing with homeland security, the governors would have a direct line on homeland security matters and understand the relationship between those issues and national security for budgetary and program decisions.

We are closer than ever to being attacked. Our adversaries will want to test a new president, and terrorism is not his number one agenda item. Jobs for Americans are number one. His national security team is a good one, but without his interest they will not have the success the current administration has not gotten credit for. The emerging issue will be: assuming we are attacked and the administration and Congress will again want to take some action, what should the Department of Homeland Security look like after a reorganization that is intended to better address the threat?

The Department of Homeland Security: Time of Opportunity

The DHS transition is an emerging issue. A radical change at this point will, in my view, waste a lot of money and time while making the country more vulnerable. That transition strikes me as the issue for the next year.

The change in administration represents the first time that another administration will take over DHS and the impending change and speculations about change represent a major issue for this embryonic agency. It is a tremendous opportunity to determine what works, what does not work, and how DHS may be structured and operated moving forward.

I think the issue continues to be the demarcation line between the role of the states and the role of big DHS. DHS does not have a large impact on the states except for the grant money. The [Michael] Sheehan book, Crush the Cell, said it well when
supporting the idea of moving the grant function out of DHS and back to a smaller entity. DHS still needs to decide what the department’s core mission is. The all hazards approach is fine when all is quiet. But when the weather event occurs it draws away from the reason DHS was formed: to deter bad guys from doing bad things. The components that comprise DHS are the true success story. The big DHS is nowhere near as relevant.

Having a new homeland security secretary could change the future of homeland security.

The central question is which aspects of DHS and FEMA policy and structure will be maintained, modified, or overthrown by the new administration?

The election has created an opportunity to look at the Department and mission in a new and innovative way. Good homeland security is fueled by new thought.

The Federal Emergency Management Agency: Will You Stay or Will You Go?

The top story was the discussion regarding whether to move FEMA out from DHS and have it as a stand-alone agency. The discussion took on new energy with the upcoming change in the executive branch.

There is a specter that FEMA may be removed from the United States Department of Homeland Security. This is a significant homeland security concern.

The top story of the year was the resurgence of FEMA. By proving that the "new" FEMA is not the Katrina FEMA, it has practically insured its continued organizational placement within DHS.

The lack of attention being paid to the aftermath of the Gulf hurricane season was a top story. I think I would call it Katrina fatigue. The perceived failures of FEMA are getting little traction in the media, not because they are not failures, but because people are too tired of hearing about debris removal and the lack of housing. Of a similar ilk, I am shocked at how little attention we seem to be paying to bin Laden and al Qaeda. The same kind of fatigue dynamic is at play perhaps.

The issue to watch for is the effort to remove FEMA from the Department of Homeland Security. As DHS is restructured in the new administration, separating FEMA from traditional emergency management might be a defining moment.
At the 2008 International Association of Emergency Managers (IAEM) meeting in Kansas City, the group coalesced around the idea of making FEMA a separate stand-alone department again (separate from DHS). There is evidence that law enforcement is trying to become a solo part of homeland security. And with this development, emergency management agencies think they should be separate too. I am seeing early signs of increasingly fractured homeland security planning focus at the local level. Disciplines want their money and they don’t want to be bothered by anyone while they spend it.

FEMA will stay and remain with DHS. What the [Obama] transition team has realized is that if FEMA were removed from DHS, DHS would essentially become a law enforcement and counterterrorism agency. The result to both agencies and to the homeland security ecosystem would be less collaboration, less resiliency, less flexibility and greater turf issues and resources battles. In fact, maybe DHS should become more FEMA-like.7

The question of "FEMA, in or out," has centered mainly on which bureaucratic organizational arrangement best serves the need for an effective agency to lead federal efforts to support state and local governments during major disasters. While it is apparent to me that FEMA and its representatives in the field will never again have either credibility or authority within either the interagency or intragovernmental worlds while buried deep within DHS, this is not the pivotal issue. The more important issue is to what degree does having FEMA in DHS detract from the secretary’s primary role of preventing the next terrorist attack and protecting the nation? Having the secretary spending three nights in a joint field office during a major hurricane event, with a great probability of being unable to disengage because of the storm, and focused on hurricane behavior and levee construction makes no sense. Governor Napolitano should focus on her responsibilities for our protection and let the FEMA administrator deal with preparing for, responding to, recovering from, and mitigating the effects of any event, man-made or natural.

The Good Things

The lack of a major terrorist incident in the United States was a significant homeland security issue in 2008.

The top issue was that George W. Bush exited the world stage without getting any credit for keeping us safe for over seven years, and especially in the run-up to the 2008 election where terrorists could have influenced the American public into voting for John McCain. That would have provided better opportunities for them to fundraise against someone they have wrongly considered to be an evil president.
The response to the Gulf hurricanes (as well as the Midwest floods, and the Western wildfires) was considerably improved from past disasters. While not of the magnitude of Katrina, the level of coordination and response helped to restore the confidence in government to handle such problems.

The top story is the protection of our nation from dangerous people by effectively controlling the borders. DHS has strengthened the screening processes at border crossings to keep dangerous people out, yet balanced this so as not to hinder commerce and those who seek to come to the United States through legal channels.

A top story is the concept of having a deployable police force that can respond within or outside the state as the need arises. FEMA is studying the Illinois Law Enforcement Assistance System (ILEAS), which was used to deploy over 300 officers to Katrina and 100 to the Republican national convention in St. Paul Minnesota. It is an exciting concept, and to my knowledge no other state has such a versatile law-enforcement group equipped and trained to respond as a single unit. As forest fires, floods, and other such events continue, deployable response forces from the states that can assist in the disaster will, I believe, grow in importance.

Private sector and personal preparedness are getting better. I think September as the DHS preparedness month is getting traction and it needs to catch on faster.

Homeland security has become more than a department or mission. It is a part of everyone’s daily life. Even on cable TV, from the news to the food network, the need to take responsibility for protecting yourself and those around you has become the new culture. It has been a good thing.

Americans are more sophisticated and knowledgeable than they are sometimes given credit for. It seems that Americans still fear terrorist attacks, and support broad efforts at the local, state, and federal level to prevent them. But there does seem to be a sense that America must maintain its moral compass and not alienate itself from the rest of the world. Honesty by its government remains important, and being the leader by example of democratic principles for the world is still important. The emerging issue may be that Americans want strength against
terrorism. But evenhandedness in policy and government accountability is very important to Americans.

The Threat: Are we more vulnerable now than we've been in the past decade?

I believe we are more vulnerable now than we've been in the past decade. The administration change will reduce our capabilities, but even more important, our economic condition makes us an even more inviting target.

The Southern Border

Mexican border security is the top homeland security issue. Currently Mexico is being destabilized by drug cartels. More than 4,000 people were killed in 2008 in Mexican drug wars. This leaves our southern border at risk. The instability of Mexico presents opportunities for safe havens for terrorists to emerge from our southern neighbor.

The escalating violence along the U.S. and Mexican border is a threat. Further excursions and continued drug violence may result in greater opportunities for terrorists and the inevitable presence of federal and military forces. I view border control as a priority focus for the next administration.

The top issue is the Mexican drug war and its possible nexus to terrorism.

The threat to the U.S. southern border by gangs working in cooperation with criminal organizations may become a concern relative to human smuggling as an avenue for terrorists to penetrate the U.S.

Violence in Mexico is an emerging threat. The U.S. does not seem overly concerned about our next-door neighbor’s deteriorating security and the inability of the Mexican government to maintain a monopoly of force. The U.S. counter-narcotics-focused policy for Mexico is inadequate to the task and replicates the disastrous mistakes made in Colombia during the 1990s. The U.S. spent billions of dollars in the counter-drug operations in Colombia without significant results in reducing drug trafficking or increasing security in that country. It was not until the U.S. government changed the focus of the policy to security and reestablishing the Colombian government's sovereignty over its territory (in 2001) that the situation was brought under control. Mexico has become the main avenue for drug trafficking into the United States. Therefore, there are billions of dollars in play, which is giving the traffickers the means to outman and outgun the Mexican government. If the present trends continue and the Mexican government loses
control of its northern border, the United States will have a major security challenge on its hands. An unstable border increases the potential for violence spilling over into the United States, provides smuggling opportunities to terrorists, and increases demand for security resources at the expense of other areas. The Merida Plan will not work until it focuses on increasing the capabilities of the Mexican government to reestablish sovereign control over its territory.

**Domestic Threats**

The top story of the year was U.S. citizens of Somali descent traveling to the corner of Africa to participate in jihad.

♦♦♦

The top story was the growing radicalization of Muslim enclaves in the United States.

♦♦♦

I feel that the prison radicalization of terrorists is an emerging threat to the U.S.A. These prisoners are locked up in our jails and then left there to be forgotten, "out of sight, out of mind." Only later do we find out they are being radicalized in our system. When they are released they are emboldened to cause terror in our communities. This must be dealt with sooner rather than later.

♦♦♦

An emerging issue is the American born and bred terrorists like the KKK and paramilitary groups that will proliferate following the elevation to presidency of a black man. They are the next generation of Timothy McVeighs and Nazi skinheads.

**Cyber Threats**

Emerging to me means maybe we have known about it before, but it has never gone mainstream. I think nonviolent threats such as cyber attacks and financial influence for the purposes of creating fear are emerging homeland security issues.

♦♦♦

Cyber security is the top issue in the most underreported story of homeland security today. There has been some press about the Chinese and quasi-independent entity efforts to penetrate the United States government and private-sector networks. Many of these efforts have been successful and represent a significant threat to homeland and national security. Given the fact that the U.S. is totally dependent on cyber technology to run the security, defense, economy, and infrastructure of the nation, there should be a major synchronized national effort to address vulnerabilities. The cyber realm offers tempting opportunities for sophisticated state and non-state actors to damage the U.S. in the physical, psychological, and economic domains. One needs only to look at Hollywood’s rendition of cyber warfare in the movie *Live Free or Die Hard* to imagine the potential damage that can be inflicted to our nation. Granted, there have been some government efforts in this area, but not the focus and resources that we place...
on WMD or terrorist attacks. What keeps me awake at night is that these penetrations are not seeking to do damage now. Instead, they may be opening doors for future coordinated attack that may inflict severe damage on the nation. If we apply al Qaeda tactics to this domain, these penetrations could be seen as probes, reconnaissance before the big operation.

Information security is a top concern. Currently the United States government does not have a synchronized and unified means to secure the systems that enable all our command and control, operations, administration, and resource management for homeland security.

The cyber security issue is nearly as nebulous and complex as the environment in which it lives. It spans the intersection between the public and the private sectors.

Cyber security and critical infrastructure protection are issues that have received some attention, but I think they will be the next major issues for DHS.

**Threats from Other Nations**

Global issues other than terrorism are significant. Although terrorism is important, there are other longer-range issues we need to pay attention to, such as the emerging powers China and India. Russia is rearing its head too. Although these countries probably will not attack us, they do represent security concerns. They are shifting the balance of power. Proliferation of WMDs – materials and knowledge – is also a concern related to these countries, especially Russia. We may need Russia to help us counterbalance China one day.

American foreign and security policy and concerns tend to be shortsighted. While these are important, we need to look ahead to mid- to longer-range concerns as well. India, Russia, and China (especially) fall into this category. Space security is starting to emerge as an area of concern. More countries, some with WMD, are getting "up" there (in space). What policies and strategies do we have? And also, how are we going to counterbalance China in the future as it is emerging as a "great" power? China is investing in Africa – an area we have long ignored.

A significant emerging trend is the continued evolution from the bipolar world of the Cold War to a post 9/11 "multi- bipolar" or even a "non-polar" world. This has resulted in a rise in the number of actors able to compete with or threaten the interests of the United States across the foreign and domestic divide in homeland defense and security. They range from great power nation states (emerging peer competitors), or even lesser nation states, to "sovereignty-free" actors (criminal, terror networks, super empowered groups, and super empowered individuals).
An example of the emerging capabilities of these new actors occurred with the Russian invasion of Georgia in 2008. On the same day that the American president went on national television to voice support for Georgia against invasion by Russian conventional military forces, a criminal network believed to be operating from Russia was conducting cyber attacks against the Georgian government from computer servers located in United States. This action completely shattered any notion of a foreign-domestic divide in homeland defense and security.

♦♦♦

Asymmetric wars, as opposed to asymmetric warfare, may be our greatest threat. With so many nations, factions, religions, and assorted scoundrels who hate the U.S., the possibility exists of combined nation state financial war, nation state traditional war, WMD by non-state actors, asymmetric warfare by non-state actors, all against the U.S. These will be wars that take advantage of the opportunity of mutual hatred and actions. It could be a feeding frenzy on a much larger, but wounded shark.

♦♦♦

The instability of Pakistan remains a top concern. Pakistan is important because we don’t want to provoke another war; two fronts is enough. But we need to deal with the insurgents who use it as a staging area. This is a very tricky balancing act. We are being spread too thin in the Middle East. The strain is showing. We are on a precipice here, and we need to handle this one very carefully so we don’t exacerbate our overextension, yet still maintain our security and our credibility.

♦♦♦

A critical issue is the potential civil war or war between India and Pakistan.

♦♦♦

The instability of Pakistan, while now a concern, is really just starting to emerge in its seriousness.

♦♦♦

I believe that Russia and Venezuela partnering together is a potential problem for the U.S. The economic downturn may have temporarily mitigated this threat.

♦♦♦

The stability of Iraq is a critical emerging issue for homeland security and is largely dependent upon the U.S. Army successfully mentoring the Iraqi security forces to operate under rule of law. The underlying issue here is the Army’s ability to learn and use civilian law enforcement methods.

♦♦♦

I really believe the threat (poison and hazards) posed by Chinese imports is bubbling under the surface. This is further amplified by the world economy. I believe our government – the FDA – is impotent to really do anything to correct
Chinese behavior because of the sheer volume of the imports, the low cost of products from China, and our insatiable appetite for cheap products.

Public Health Threats

A top homeland security related story for public health is the ongoing discussion of implementation of the Pandemic and All Hazards Preparedness Act. The Act will require a match and maintenance of funding support from the states for programs that had previously not required state funding support at any level. The implementation process has been awkward, with great resistance from the states. The maintenance of funding has a floating target that consists of the average of the funding from the previous two years. There is concern that the required match would then be rolled into the previous year's maintenance of funding numbers, requiring different match sources to be found. Discussions about these issues continue among ASTHO (Association of State and Territorial Health Officials), DHHS (Department of Health and Human Services), ASPR (Assistance Secretary for Preparedness and Response), and CDC (Centers for Disease Control), as well as staffers from Congress.

♦♦♦

The FBI revelations related to the anthrax letter attacks count as a top homeland security issue for 2008. Considering this was the nation's sole data point for an actual bioterrorism event, it is highly significant that the attack originated from inside the U.S. bio defense apparatus. Added significance lies in the fact the event was perpetrated by a U.S. Army scientist responsible for the testing of the anthrax vaccine and that, according to the FBI, the motive was that the vaccine program was "failing" and about to be canceled at the time of the attacks. Considering these facts, the most compelling aspect of this event remains the fact that no one from the government has directed a review of the vaccine program as a result of the FBI revelations, but instead ordered more vaccine, which secures the story as the top homeland security issue of 2008 and likely the decade.

♦♦♦

This problem is not exactly emerging, but it is still a big problem that is getting bigger: the public health and emergency health infrastructure of this nation is inadequate and it is shrinking every year. We don't have enough beds for a mass casualty incident involving tens of people. Hurricane Ike wiped out UTMB [University of Texas Medical Branch, at Galveston], the level one trauma center covering Texas City and Galveston. Should there be an event even a fraction of the size of the Texas City disaster, those casualties would need to be airlifted or driven fifty miles north to Houston for treatment. What other trauma centers are being lost due to budget issues, especially given the economic downturn?

♦♦♦

I think the bioterror lab standard issue is going to loom large in the next year or two.
While threats from intentional use of traditional biological weapons (in particular anthrax) remain a concern, the dramatic increase in drug-resistant infectious diseases adds a different dimension to the bio threat. Such "hardened bugs" (e.g., MRSA, XDR-TB) present a potential threat to the nation (and beyond). This might come through a naturally emerging infection or through an intentional introduction of the pathogen as a terrorist weapon. In either case, the lack of novel antimicrobial therapy for these organisms is a concern and has significant homeland security implications.

**Other Threats**

The recently released WMD prevention report ["World at Risk: The Report of the Commission on the Prevention of WMD Proliferation and Terrorism"] cited rumors of the potential for a tactical nuclear weapons event on domestic soil. As this was the first government-related source I encountered that mentions the possibility, I believe this ranks up there as a significant emerging threat.

One thing emerging is the issue of pirate activity off the coast of Africa. If this catches on worldwide, it could have a significant impact on trade and a snowball effect with other industries (such as oil).

There remains a problem with small boats. It is especially related to the continued success of pirates and the increased successful use of semi-submersible vessels by drug smugglers. Success in both these areas could embolden terrorists to copy and use those tactics to attack the United States.

I believe that as the economic crisis continues domestic acts of piracy and sabotage will likely increase. Homeland security needs to pre-identify [those threat] patterns with an eye toward prevention and response.

The relationship among illegal immigration, extended economic upheaval, and unemployment are ingredients for a "recipe" of significant unrest and fear.

Seeing how Congress and DHS initially made common cause on chemical security issues, only to break ranks, highlights the lack of a consistent approach and the subordination of security issues to petty politics.

From a local perspective, the top homeland security story was the terrorist firebombing attacks in Santa Cruz. Members of an animal rights group were the suspected perpetrators. This was a significant event for the area unrelated to
Muslim extremist organizations. And yet the attacks did not result in any significant alarm for the region.

♦♦♦

Election security was the top issue. Based on the candidates, there was an increased potential for domestic attack intended to disrupt the presidential election. That attack did not happen. Why not?

♦♦♦

An emerging issue is the implications of the potential encroachment of Sharia-compliant banking into world economic systems, particularly our own. Our collective greed does not differentiate between sources of money, even when potentially threatening national security. Our own government is likely to be complicit in advancing this bastardized form of banking and therefore fall prey to the weaknesses it could exploit. The integration of religious zealotry with banking has potentially far-reaching implications: the implementation of subtle strategies to replace capitalism being one of them.

The Culture of Preparedness: “Waiting Until We Bleed Again”

I'm concerned about the incident attention syndrome – our inability to stay focused on the threats. I fear that we are just starting out on our journey with homeland security. Perhaps we will not start paying attention until we bleed again.

♦♦♦

I think that the arrests and conviction of the individuals planning an attack at Fort Dix in New Jersey was the top homeland security-related story in 2008. It was a great example of the use of citizens as points of information, local police as information gatherers, and a federally-led task force to investigate and intercept the attackers before they could complete their plan.

♦♦♦

While not widely reported, the fact that the terror alert color-coded level has been stuck on orange for the whole year in the absence of any specific threat makes a mockery of the entire system of alerts and citizen engagement in the so-called "war on terrorism." We need to change the war metaphor to "The Global Challenge of Terrorism."

♦♦♦

Resiliency seems to be the emerging issue: both how to build resiliency and how to sustain resiliency for responder communities in the nation at large.

♦♦♦

Based on discussions and meetings I've attended, the 2008 themes appears to be about building a culture of preparedness with a focus on improved resiliency. Building resiliency includes developing a disaster mental health focus as well as training and education for responder communities.
What have Americans been asked to sacrifice in combating terrorism at home and abroad?

The further we get away from 2001, the harder it is to get people to care about preparedness or spending time and money to make the nation more secure. We – the government – do a horrible job of conveying the message to the people that we need to stay vigilant, that we need to take preparedness activities to heart. It is a more basic problem than that: we have not figured out an effective way to get our message through to the public so that they will actually listen to what is being said and act accordingly. We do a good job of scaring people; so good that people are ignoring the message, or taking it very cynically. We need to find a way to effectively, realistically, and honestly convey the true risk so that people will believe it, understand what is in it for them, and take the appropriate action. Or perhaps we should just write off this generation and concentrate on the kids, just like we did with seatbelts and bike helmets.

Meta Hazards – Things We Do To Ourselves

The top issue has to do with economic security and infrastructure – water, food, and energy shortages. The implications of an economic fall due to a lack of food, energy, or water are huge. We need to do a better job of addressing these issues long-term.

Economic security and food, water, energy shortages: I think these issues have the potential to cause more harm than all forms of terrorism if they are not addressed.

The fluctuations in the price of oil, the continued instability in the Middle East, and the increasing maritime piracy off the Horn of Africa have highlighted the importance of energy security to U.S. national security and homeland security. The recent drop in oil prices will probably cause most Americans to forget about this threat and, unfortunately, the opportunity to rapidly develop alternatives to foreign oil imports may be lost.

Global warming may have a significant impact on our current all-hazards homeland security environment.

Climate change is the next top story. Its effects on our sources of energy, new international conflicts over natural resources, and migration flows due to sea level rise and desertification will have a direct effect on the security of the United States.
The issue of water is in an embryonic state. Whatever the cause of climate changes, many large population centers, especially in California, are going to be defined by the utilization and access to water. As water becomes more contested, security of the homeland will be more tenuous.

♦♦♦

The emerging issue will be natural disaster preparedness, mitigation, response, and recovery. I believe the severity of storms will increase because of climate warming.

Funding Concerns

A reemerging homeland security issue is the prioritization of funding for prevention, preparation, response, and recovery in an environment where available funds are decreasing. Threat analysis, needs assessments, and the prioritization of resource needs are becoming increasingly important.

♦♦♦

The top story is the bastardization of the UASI [Urban Areas Security Initiative] program by successful law enforcement lobbyists at the federal level. Law enforcement lobbyists carved a 25 percent earmark for law enforcement in the UASI grant program by providing questionable information to grant guidance writers and to Congress. It never” made the papers" that, in many cases, this has had a negative impact at local levels.

Professionalization of Homeland Security

The top story is the absence of a professional development system for homeland security warriors that would serve to develop a homeland security culture and lead to the effective assimilation of the twenty-two disparate legacy agencies into a common culture, while recognizing differences in specific roles and missions (much as the U.S. Army, Navy, Marine Corps, and Air Force have differences). At present there is no real capability for such a professional development system, despite some well-meaning efforts by the executive branch. For there to be a coherent homeland security culture, encompassing federal, state, local, and private-sector players, there must be a system developed that is based on established doctrine, education, training, and field and Washington experience. At present, Washington insiders and youthful staffers have developed plans, procedures, and doctrine based on a total absence of real world experience, understanding of how both the interagency and intergovernmental worlds actually work, and with an arrogance born of ignorance. In the military, admirals and generals become senior leaders and policymakers based on careers of field and headquarters experience and professional education, not totally on political affiliations. The development of such a [homeland security] system will not be accomplished overnight. It will require vision and commitment by Congress and the executive branch to make such a system a reality.
The Department of Defense failed again for the second straight year to use the $3.5 million Congress approved to establish the nation's first homeland security and homeland defense PhD program. Failing to develop a credentialed cadre of competent leaders to educate the current and next generation of homeland security professionals may be the most profound strategic mistake made in 2008.

Information and Intelligence

Overall the term "information sharing" has become more of a buzzword than a reality. There are still too many competing efforts to share information between federal and “state and local” entities (state and local are not the same).

I believe information sharing and intelligence tops the list of homeland security concerns in 2008. Two examples include the lack of information sharing during the Democratic and Republican national conventions. An example of improvements needed in the intelligence field is the recent attacks in India. Similar attacks could happen anywhere in the U.S.A.

The tragedies of 911 have meant the world now has a dramatically different view of national security. Governments must recognize the critical need to share and disseminate information, particularly spatial information across agencies and jurisdictions both efficiently and economically.

I believe there is a critical misunderstanding about the value of information sharing among government as well as private agencies. The lack of communication has reached critical mass.

The top story is the admission by the Maryland State police that they improperly conducted surveillance on activists in Maryland. The lawsuits that result from this issue could have national implications for the operation of state and local intelligence units nationwide. It is not a nationwide story yet, but it will be when the legal proceedings get underway.

Critical Infrastructure: Jobs and Security

A significant aspect of President Obama's economic stimulus plan is to request Congress appropriate hundreds of billions of dollars towards revitalizing the nation’s infrastructure. While much of this money will be devoted to improving existing infrastructure, new energy-conserving and environmentally friendly projects are also being proposed. This program may have positive results for the nation's economy and critical infrastructure viability. But it is conceivable that
these same efforts could introduce predictable and unforeseen homeland security challenges.

♦♦♦

The projected investment in infrastructure renewal by the new administration should be planned in accordance with prioritized national critical infrastructure and security concerns. The concern is not to haphazardly push funding projects for the sake of stimulating the economy.

**Criminal Justice and Homeland Security**

I feel the top homeland security issue is the inability to identify what the differences are between terrorism and criminal activity and how to deal with people who are involved.

♦♦♦

I think there is going to be a very clear nexus between domestic criminal activity (such as fraud, identity theft, and narcotics trafficking) and terrorist activity. Separating the two activities would be a mistake since important indicators may be missed during investigations.

♦♦♦

The top issue is how to deal with detainees held at Guantánamo Bay. Any method of dealing with these folks, whether bringing them to the United States for trial or returning them to their native countries, will have substantial homeland security implications.

♦♦♦

Risk management continues to be an emerging issue. Risk management is the process of identifying, analyzing, assessing, and communicating risk and accepting, avoiding, transferring, or controlling it to an acceptable level at an acceptable cost. Homeland security risks are complex and cross-cutting. No single entity is able to effectively balance these risks independently. Instead risk management depends on being able to integrate a wide range of homeland security activities. In most cases, there are no integrated frameworks in place to ensure a collaborative approach to the analysis, assessment, and management of risks.

♦♦♦

An emerging issue within law enforcement is the standards the National Tactical Officers Association has promoted for SWAT teams. These "national standards" will eliminate SWAT teams in small- to medium-sized jurisdictions, unless there is regionalization, which is fraught with political, training, equipment, response time, and procedural challenges. The elimination of these small SWAT teams will affect homeland security when an event is well outside a large metropolitan or UASI area.

♦♦♦
Security clearances for non-law-enforcement personnel continue to be an issue. The absence of clearances limits information sharing. The goal of timely clearances needs to be achieved to allow better review of information by affected agencies.

THE IMAGE OF HOMELAND SECURITY

This review of homeland security in 2008 closes with three graphics that are candidates for the Homeland Security Image of the Year. The first image portrays in strikingly non-linear fashion the organization of the Department of Homeland Security.9

DHS Operations Community Model

The second picture, from a RAND study, depicts the current U.S. domestic intelligence enterprise. It is an image to be viewed, for the aims of this article, more for its complexity than its detail. The report from which it is derived, along with a very readable copy of the chart, is available elsewhere.\(^\text{10}\)

The final picture is the Transportation Security Administration's visualization of its twenty layers of security. Additional information about the logic behind the strategy is also available elsewhere.\(^\text{11}\)
ONE LAST LOOK AT 2008

As noted in last year's review, a tag cloud is an image that displays a set of words. The size of each word is proportional to the frequency with which it appears. The bigger the word in the cloud, the more frequently it appeared in the article. The following tag cloud depicts the semantic field created from the responses to this year's survey. It represents one integrated perception of homeland security in the year 2008. You are invited to construct, and share, your own story.

“Every person takes the limits of their own field of vision for the limits of the world.”
-Arthur Schopenhauer (1788 – 1860)
Christopher Bellavita teaches in the master’s degree program at the Naval Postgraduate School in Monterey, California. An instructor with twenty years experience in security planning and operations, he serves as the director of academic programs for the Center for Homeland Defense and Security. He received his PhD from the University of California, Berkeley. Dr. Bellavita may be contacted at christopherbellavita@gmail.com.
The seventy-four people who responded to this survey included graduates and current participants in the Naval Postgraduate School’s Center for Homeland Defense and Security’s (CHDS) master’s degree and executive leaders programs, CHDS faculty, Mobile Education Team members, NPS staff, and other people who periodically participate in CHDS homeland security activities. In large measure they are the authors of this review, and I am the amanuensis. However, none of the people who participated in this survey are responsible for my interpretations of their responses; nor do their observations necessarily represent anything other than their personal, not their official, views.


Topics not mentioned include the sentencing of Jose Padilla, Amtrak’s and Washington Metro’s decision to randomly screen carry on baggage, the DNI threat assessment about al Qaeda’s improved ability to attack within the United States by recruiting and training new operatives, organizational clashes between the FBI and the New York City police department over counterterrorism programs, political accommodations in the REAL ID program, the appointment of Kenneth Wainstein as the president’s homeland security adviser (replacing Frances Townsend), changes in the terrorist watch list, the release of more information about the legal opinions that informed the first years of the Bush administration’s terrorism strategy, states and cities objecting to federal security funding program emphasis on terrorism, successes and difficulties with constructing the fence along the Mexican border, an American Association of State Highway and Transportation Officials report indicating that one in four American bridges need major repairs or upgrades, the delay of the proposed Air Force cyberspace command, an active duty Army brigade assigned to NORTHCOM, a conviction in the Holy Land Foundation trial, unsafe produce, Google using web searches to track the spread of flu activity, and homeland security set to become a reality television show in January. There are many other topics that could have been covered. It was a busy year.

This “response” was not generated by the survey. Someone who interviewed a member of the transition team brought it to my attention. I included it in this section for its unique insight into the FEMA and DHS issue.


CORRECTION, February 9, 2009: Thank you to Derek Rieksts for providing the source information for this diagram, which is from a 2006-2007 study, Mission Blueprint, commissioned from Booz Allen Hamilton by the Office of Operations Coordination (OPS) at the Department of Homeland Security.


The list used for the 2008 tag cloud was refined by eliminating common words (e.g., “is,” “the”) and words not directly related to homeland security (such as “ago,” “biggest,” “recently,” et al.). I also eliminated the term “Homeland Security” since it appeared so frequently. The cloud was produced from the online resources at http://www.tagcrowd.com.
Beyond the HSC/NSC Merger: Integrating States and Localities into Homeland Security Policymaking

Paul N. Stockton

The Obama administration has the opportunity to fix a crippling flaw in the homeland security policymaking process. When President Bush established the Homeland Security Council (HSC) to develop policies and integrate U.S. homeland security institutions, White House officials emphasized the importance of including state and local government representation in the council. Their inclusion is vital. Homeland security fundamentally differs from national security in that states and localities play the leading role in many homeland security missions, as opposed to federal agencies. Yet the Bush administration ended up excluding state and local representatives from the HSC and built only weak mechanisms to include their input in Department of Homeland Security policymaking. That exclusion helped produce a string of failures in policy development and institutional integration. Now, regardless of whether President Obama decides to merge the HSC with the National Security Council (NSC), he has the opportunity to make a vital change: the creation of an effective, institutionalized way for states and localities to help shape the policies and programs they implement.

Merging the NSC and HSC is not without risk. I argue that if the councils are combined, administration officials will need to pay special attention to the span of control issues raised by the merger and the danger that homeland security will take a back seat to traditional national security priorities. I also argue that integrating homeland security across the federal bureaucracy – that is, horizontal integration – poses unique challenges that a merged council would need to address.

These problems will be relatively easy to solve, however, compared to the challenge of building effective vertical integration between a merged council and state and local governments. The National Security Council system never created a mechanism to provide for state and local input into security policymaking, because those levels of government played virtually no role in providing for national security. The Bush administration recognized the need to create such mechanisms for homeland security. I will argue, however, that the administration left behind a homeland security system that is fundamentally mismatched with the leading roles that states and localities play in protecting the United States from all hazards. Scholars and policymakers have only begun to examine how to take better advantage of state and local expertise in the policymaking process, and include those levels of government not only in shaping the details of plans and programs, but the overall strategies and priorities that will guide homeland security for years to come. I examine a range of options to institutionalize such a role, regardless of whether the HSC and NSC merge, and propose criteria to help policymakers chose between them.
THE PROBLEMS OF INTEGRATION

President George W. Bush’s creation of the HSC in 2002 was part of much broader change in the way the United States is organized for security. Before 9/11, the Department of Defense, the Department of State, and the Central Intelligence Agency (CIA) were largely responsible for U.S. security and were coordinated by the National Security Council. After 9/11, Bush built a parallel security system to protect the United States from terrorist attack. The Department of Homeland Security (DHS) is only part of that system. The Bush administration has also assigned terrorism prevention functions to the Departments of Agriculture (USDA), Health and Human Services, Interior, and over a score of other federal institutions that have never before played such significant roles in securing the United States from attack.1 Bush established the Homeland Security Council to direct and coordinate this far-flung security system, led by the assistant to the president for homeland security and counterterrorism.2

Numerous recent studies argue that the next president should subsume the Homeland Security Council (HSC) in the National Security Council (NSC), and strengthen the way the White House develops U.S. policy and oversees its execution.3 Merger advocates focus on two problems with the Bush-era council system. The first problem lies in the weakness and understaffing of the HSC compared to the NSC. When President Bush created the HSC, White House officials said it would have a staff comparable in size to the NSC, with the authority and political backing from the president to coordinate the agencies under its purview.4 The HSC actually ended up with a staff one-fifth the size of the NSC’s and had to labor under much more stringent budget and salary constraints.5 Whether or not the councils are merged, the staff responsible for homeland security issues needs to be adequately sized and resourced.

The second problem lies in the integration of the domestic and international components of security policy. Merger advocates contend that by creating two councils and their supporting staffs, the White House has bifurcated its approach to national security issues, even though the issues themselves frequently hinge on interrelated domestic and international factors.6 Effective policy integration across domestic and international lines is indeed essential, and merging the staffs would be a good way to facilitate such integration. But if President Obama were to keep the HSC independent, closer policy integration would still be possible. The NSC and National Economic Council (NEC) forged an effective collaborative relationship across their respective jurisdictional lines during the Clinton administration. Nothing precludes the NSC and HSC from building an equally effective relationship, as long as President Obama and his homeland and national security advisers make doing so a priority.

However, merger advocates have focused far less attention on the integration problems the HSC was created to solve – problems that pose especially urgent challenges today. Those challenges lie in the integration of homeland security efforts across the federal bureaucracy and between federal, state, and local governments.

Horizontal Integration

When President Bush created the HSC on October 29, 2001, he tasked it to “ensure coordination of all homeland security-related activities among executive departments
and agencies,” as well as promote the effective development and implementation of homeland security policies. The council retained that coordination responsibility even after Congress and the president established the Department of Homeland Security (DHS). Indeed, in creating DHS, Congress codified the existence of the HSC into law and specified its responsibility for “effectively coordinating the policies and interests of the United States government relating to homeland security” and other functions as directed by the president.

Congress and the president had good reason to assign that coordination responsibility to the HSC. The federal homeland security system consists of an astounding number of institutions. Over thirty departments and independent agencies perform homeland security functions, creating an almost limitless array of interagency seams and coordination requirements. Making the HSC responsible for meeting these coordination challenges, rather than putting dozens of new agencies under the purview of the National Security Council, limited the risk that the national security advisor would be overwhelmed by span-of-control problems. Merging the two councils would bring span-of-control issues to the fore once again.

The novelty of the security functions performed by these thirty institutions creates further problems for interagency planning and coordination. Until 9/11, departments such as USDA had never served significant security functions; now they play critical roles in protecting U.S. populations and infrastructure from attack. Melding the new security responsibilities of these agencies into an integrated system creates innovation challenges quite different from those posed by the departments overseen by NSC, which have been handling security issues for decades. The institutions under the Homeland Security Council’s purview also share a distinctive internal problem the National Security Council’s departments lack. DOD, the CIA and the State Department focus almost exclusively on security-related issues. Departments such as DHS, USDA and DOJ must not only help secure the United States from attack, but also perform their traditional domestic functions unrelated to (and sometimes in funding and programmatic competition with) their post-9/11 responsibilities. The NSC has never had to deal with such difficult intra-agency tradeoffs between security and non-security functions. Yet agency tradeoffs will need special attention as the Obama administration builds its homeland security policies, especially as budget pressures intensify conflicts over agency priorities.

This is not to argue that the HSC has been fully successful in meeting its federal coordination responsibilities. The Obama administration has inherited an array of unresolved conflicts over department roles and responsibilities for homeland security, including disputes between DHS and the Department of Justice over terrorism prevention and response; between DHS and the Department of Energy over preparing cities against nuclear or radiological attack, and – more recently – over which agency should have primary responsibility to safeguard U.S. bioterrorism research facilities from rogue employees. The administration has also inherited significant gaps in interagency planning for pandemics and other catastrophic incidents.

Merging the NSC and HSC will not automatically solve any of these coordination problems. On the contrary: unless the administration takes special care to avoid span-of-control problems for the national security advisor, providing sufficient attention and
political leverage to resolve agency turf wars and build a better integrated system will become more difficult. Those problems are eminently solvable. For example, if the merged council includes a deputy advisor for homeland security and counterterrorism, ensuring that the deputy has direct access to and strong support from the president for dealing with such issues will greatly aid in their resolution. It is far less clear, in contrast, how Congress and the Obama administration should fix the most serious failing of the HSC system: the integration of federal, state, and local homeland security efforts.

**Vertical Integration and the Paradox of Homeland Security**

The need for integration between different levels of government represents a crucial difference between homeland security and national security issues, and between the coordination challenges confronting the HSC and NSC. National security policies rarely depend on state and local implementation; DOD and other federal departments carry them out. In contrast, state and local governments (and police, firefighters, public health workers, and other professionals they employ) are absolutely vital to homeland security, making vertical coordination more important as a consequence.

The two policy realms also differ in the president’s authority to solve coordination problems. Scholars are fond of noting how little de facto control the president exercises over the federal bureaucracy. Nevertheless, in the national security system, where the primary coordination challenge lies in integrating the work of DOD, the State Department and the CIA, the chief executive – i.e., the president – exercises at least formal authority over that system and can fire department heads who resist coordination. The political context of homeland security is very different. Governors do not work for the president. They are independently elected and are the sovereign chief executives of their states. Homeland security thus entails a paradox. The integration between federal, state, and local governments is vastly more important in the homeland security system than in its national security counterpart. Yet the president has remarkably little authority to impose such vertical integration, especially in comparison with his command over national security institutions.

The Bush administration sought to deal with this paradox when it created the Homeland Security Council. In late September 2001, then-White House Chief of Staff Andrew Card promised that state and local governments would be represented on the council. That representation would help the HSC bring state and local perspectives to bear on building an integrated homeland security system, and would give states and localities a say over the plans and programs they would need to implement. Including state and local representatives also offered a politically astute way to compensate for the president’s lack of command authority over them. By making states and localities party to the decisions the HSC hammered out, the White House could also increase the likelihood that they would support those policies.

The Bush administration’s fulfillment of this pledge on state and local representation fared even worse than its promise of robust HSC staffing. Bush did establish a President’s Homeland Security Advisory Council (HSAC) to make recommendations to the HSC and included state and local officials in that panel, along with private sector leaders, academics, and myriad other participants. The HSAC has issued a number of
insightful policy recommendations, including ones that highlight the need for stronger integration in the homeland security system. But those recommendations are purely advisory and the HSAC lacks any authority over HSC decisions that would affect its state and local members.

In the absence of effective mechanisms for vertical integration within the HSC, the Department of Homeland Security took on increased responsibility to integrate state and local efforts with federal policymaking. The Office of State and Local Government Coordination and Preparedness gave the first secretary of DHS, Governor Tom Ridge, an organization thoroughly dedicated to building effective vertical collaboration. Ridge’s successor, Michael Chertoff, abolished that office and assigned its functions to a DHS Grants and Training organization with many other responsibilities. Yet, the Obama administration has inherited problems for state and local integration that go beyond organizational wiring diagrams. The most important problem is that DHS never built a sustained, institutionalized approach to giving states and localities a voice in the policies they would implement. The development of the National Response Framework (NRF) is a case in point. The NRF is the key plan for melding federal, state, and local agencies into a disaster response system more effective than the one that catastrophically failed in Hurricane Katrina. DHS officials invited state and local representatives to help shape the initial NRF draft, then totally cut them out of the revision process (during which DHS officials made drastic changes), only to reverse course and invite them back into the process when faced with congressional hearings on their exclusion. The Bush administration then failed to meet statutory requirements to provide for state and local coordination as further revisions go forward.

Similarly ad hoc practices have hobbled other DHS policy development efforts, with predictable consequences for programmatic effectiveness. Across an array of initiatives, the Bush administration permitted only limited and sporadic state and local input, producing federal policies and programs that conflict with the requirements of the non-federal agencies crucial to the success of those policies and programs. The Homeland Security Information Network (HSIN) typifies the results of this flawed process. The network is DHS’ key system for sharing homeland security data with states and localities and was supposed to be relied on by state and local officials nationwide. Yet DHS did not coordinate with those officials to develop effective joint policies and procedures, integrate HSIN with existing information sharing systems, and ensure the network would meet state and local requirements. DHS is now replicating the same coordination mistakes in its effort to replace the failed network with the HSIN Next Generation program. Similar coordination failures have produced gaps in U.S. plans for preparedness against pandemic flu; for integrating federal, state and local response efforts against nuclear attack; and for an array of other plans and programs. The overall assessment provided by the National Sheriffs’ Association, the National Emergency Management Association, and a dozen other nationwide associations representing state and local homeland security concerns: the federal government follows “top down” approaches to policymaking that are “uncoordinated and create unintended negative cascading effects.”

---

SOLVING THE PROBLEMS OF VERTICAL INTEGRATION: NOVEL APPROACHES TO AN UNPRECEDENTED CHALLENGE

The Obama administration can only provide for better-integrated policies, plans, and programs by institutionalizing a role for states and localities in shaping them. A variety of means exist for representatives of state and local governments to play this role either in the HSC or in a merged council, including the use of mechanisms authorized by the Intergovernmental Personnel Act. Three problems, however, must be overcome to make such a system work.

The first is cultural. Placing state and local representatives in the merged National Security Council would, at least initially, produce a bizarre clash of political cultures and professional competencies. NSC staffers are vastly more likely to know the name of the president of Georgia (abroad) than the governor of Georgia (at home). That is a good thing. The NSC staff has enormous expertise in dealing with international security issues, and Russia's military incursion into Georgia is a reminder of how dangerous a place the world remains.

But the state of Georgia also involves policy challenges of great importance. Georgia's cities face threats of catastrophic hurricanes and other natural hazards. Mohammed Atta took flying lessons in Georgia before applying those skills to kill thousands of Americans. To protect against both types of threats, it will be essential for the Obama administration to build more effectively integrated local, state, and federal capabilities for homeland security. A merged council would need to be staffed with professionals who speak fluent “state and local,” and for whom a governor's sovereignty is second nature rather than an oddity to maneuver around.

A second and more serious problem is that of state and local capacity to provide representatives. Unlike the Department of Defense, state and local homeland security organizations lack a “float” of personnel who are not currently engaged in operations and can be assigned to other duties. Governors, mayors, and county executives need their homeland security staff available on a sustained basis; there is very little excess capacity to spare for other purposes. The solution – more easily said than done in current budgetary times – is to build that capacity so that state and local representatives could serve in the White House on a rotating basis. Given the importance of providing for state and local input into homeland security policy, that ought to become a federal priority, just has DHS has supported state capacity building for intelligence.

That brings us to the third and thorniest question: how state and local personnel would be selected to help shape policy in the White House. A broad range of associations that represent state and local governments and agencies – from the National League of Cities, to the National Association of County Executives, to the Governors’ Homeland Security Advisors Council – have called for a stronger, more institutionalized role for those levels of government in shaping homeland security policy. But none of these associations has yet specified how that role ought to be structured, or how state and local representatives ought to be chosen. That question is crucial. With over 80,000 state and local jurisdictions in the United States, representing all such jurisdictions in the White House is a non-starter. Moreover, on many issues – most notably that of
federal grant distribution – states, localities, and the associations that represent different first responder agencies frequently clash over homeland security issues.

The November 2008 report by the Project on National Security Reform has offered the most fully-developed proposal to date for the selection process. That report suggests that under a merged “President’s Security Council,” a homeland security collaboration committee would be established to provide for vertical integration. The president would appoint six of the fourteen members of this committee; four each would be provided by the Senate Committee on Homeland Security and Governmental Affairs, and four by the House Committee on Homeland Security. That proposal has the virtue (and vices) of “kicking the can down the road.” The question of which representatives of state and local governments to select would be left to legislators and the president, rather than specifying up front the criteria that would be used in that selection process.

I propose a different approach, which offers a different mix of advantages and disadvantages. The Homeland Security Advisory Council that President Bush established in 2002 was limited in its impact not only by its lack of authority, but also by Bush’s insistence that he select the council’s members. It seems reasonable that the president would have final say over who serves on his White House staff. However, it would also be desirable to have him select from a pool of candidates selected by states and localities. Following that path would bring a more fully-representative perspective to bear on policymaking, and would be more likely to ensure state and local buy-in of the policies their representatives helped develop.

To create the pool of candidates, the Obama administration might capitalize on the fact that states and localities have already organized into associations to build consensus amongst their members and represent their views. These associations are uniquely well-positioned to judge the professional excellence of potential candidates. Of course, the associations can be counted on to bring conflicting preferences to bear on White House policymaking, just as they do in seeking to influence congressional decision making on grant assistance and other homeland security issues. But since 9/11, those associations have also engaged in far more collaborative work than ever before, starting with the creation of the National Homeland Security Consortium. That Consortium has united to call for a stronger state and local role in homeland security policymaking. Now is the time to embrace that recommendation and restructure the U.S. policymaking system to meet the unique integrative challenges of homeland security.

Paul Stockton is a senior research scholar at Stanford University’s Center for International Security and Cooperation (CISAC). He was formerly the associate provost at the Naval Postgraduate School in Monterey, California, and was the former director of its Center for Homeland Defense and Security. His teaching and research focus on how U.S. security institutions respond to changes in the threat (including the rise of terrorism), and the interaction of Congress and the Executive branch in restructuring national security budgets, policies and institutional arrangements. Mr. Stockton received a bachelor’s degree from Dartmouth College in 1976 and a PhD in government from Harvard University in 1986. He may be contacted at pnstock@stanford.edu.

The author would like to acknowledge the critical and very helpful comments to earlier drafts offered by Nancy Dragani, Lynn Eden, Timothy Manning, MG Charles G. Rodriguez, USA, and Mike Walker.
A shorter version of this essay published in the *Washington Quarterly* 32, no. 1 (January 2009).

1 The U.S. Office of Management and Budget (OMB) reports that a total of thirty-one federal agencies conduct homeland security programs, with homeland security defined as “activities that focus on combating and protecting against terrorism” in the United States. The actual number of federal organizations responsible for terrorism prevention is almost certainly larger. For example, OMB does not include the U.S. Postal Service, even though the Service is responsible for preventing terrorists from using the mail to deliver anthrax or other pathogens. U.S. Office of Management and Budget, *Budget of the United States Government, Fiscal Year 2008: Analytic Perspectives - Homeland Security Funding Analysis* (Washington, DC: The White House, 2007), 19, [http://www.whitehouse.gov/omb/budget/fy2008/apers.html](http://www.whitehouse.gov/omb/budget/fy2008/apers.html); U.S. Postal Service: *Guidance on Suspicious Mail Needs Further Refinement* (Washington, DC: U.S. Government Accountability Office, July 2005).


9 OMB, op cit.


14 Becker and Weiner, “A Nation Challenged.”


Although the Department of Health and Human Services (HHS) is tasked to lead the public health and medical response to a pandemic, the DHS Secretary is responsible for critical non-medical pandemic support and response efforts, and has designated a Principal Federal Official to perform other coordination functions. Current pandemic plans fail to adequately explain how these overlapping functions will be de-conflicted, and the Government Accountability Office has found that it is “unclear how they will work.” *Influenza Pandemic: Further Efforts Are Needed to Ensure Clearer Leadership Roles and an Effective National Strategy* (Washington, DC: U.S. government Accountability Office, August 14, 2007), pp 1 and pasim.


All of those associations are represented on the National Homeland Security Consortium and supported its call for much greater state and local input into homeland security policymaking. Consortium, “Protecting Americans,” 2-3. See also IACP and MCCA studies.
Merging the HSC and NSC: Stronger Together

Christine Wormuth and Jeremy White

At the federal level, homeland security is inherently and fundamentally an interagency undertaking. The quality of interagency relationships and processes is central to the success or failure of federal – and national – homeland security activities. Short of giving a single Cabinet secretary directive authority over other Cabinet secretaries during major domestic incidents (which is unlikely given traditional forms of American government) the only way to ensure effective unity of effort at the federal level is to exercise strong leadership from the White House. This kind of leadership is needed not just during an actual catastrophe but also when the government is engaged in the day-to-day activities of working to prevent, protect against, and prepare for such catastrophes. In recent years the White House has not played this role, in large part because of the bifurcation of national security issues into a National Security Council and a Homeland Security Council. One of the most important and most necessary changes the new administration should make is to merge these organizations into a single council with a largely shared professional staff. This newly merged Council should exercise forceful leadership on behalf of the president of the United States in developing homeland security strategy and policy and should closely oversee its implementation.

Why a Merger is Needed

There are three main reasons that the existing Homeland Security Council (HSC) and its staff have not been particularly effective. The first, and perhaps most important, is structural: by establishing a separate council and associated staff to address homeland issues, the White House artificially bifurcated its approach to national security issues, although the issues themselves frequently have both domestic and international aspects that are interrelated. For example, effectively combating terrorism involves targeting terrorists and their support networks overseas, but also addressing the potential for radicalization of individuals inside the United States. Effectively addressing 21st century security challenges requires an integrated approach that considers both sides of a given problem – but such an approach is very difficult to achieve when two different organizations inside the White House are involved. Both council staffs work in the Old Executive Office Building, but they share little more than a mailing address. Each council has a different organizational structure, each staff reports to a different adviser to the president, and each has its own executive secretariat, with separate systems for convening meetings and designating lead directorates on specific issues. The two council staffs don’t even work on the same e-mail system: while the NSC staff does most of its work on the classified e-mail system, the HSC staff works mostly on the “low side,” or the unclassified network. Some coordination between the two staffs does take place, but it occurs largely through the initiative of individual staff members, who must overcome the hurdles presented by the bifurcated structure.

A second major reason for the ineffectiveness of the HSC on many issues is organizational: it is relatively weak, particularly compared to the NSC. A host of dry, technical personnel and budget issues have contributed significantly to this problem.
Unlike the NSC and its staff, the HSC and its staff do not constitute a separate organization inside the Executive Office of the President; as a result, HSC personnel numbers count against the overall personnel ceiling for White House staff and so there is pressure to minimize the size of the HSC organization. While the NSC has more than 240 staff members, the HSC on average has only forty-five. Moreover, as a consequence of HSC’s administrative status within the Office of the President, the council does not have its own budget, which places a tight salary cap on the staff. Although HSC staff members have significant responsibility and work extremely long hours, even the highest paid among them earn less than senior GS-15 civil servants elsewhere in government. This salary gap has added to the difficulty of recruiting the best and brightest to the HSC organization – a task that was already challenging, because the HSC is seen as having less stature than the NSC. As a result, many more HSC than NSC staffers have backgrounds in political campaigns rather than in national and homeland security issues, and frequently they are less experienced overall than their NSC peers.

Finally, the HSC has not been particularly effective in its efforts either to lead the interagency in developing core strategy and guidance on homeland security issues (such as developing an interagency deliberate planning process) or in overseeing implementation of policies once they are developed (such as the range of documents and processes called for in Homeland Security Presidential Directive 8 on National Preparedness that was signed out in 2004). This lack of success can be partly attributed to the HSC’s relatively small and inexperienced staff, but it is also associated with the explicit preference shown by the Bush Administration for “the lead agency approach,” which focuses the NSC and HSC staffs primarily on coordination rather than development of strategy and policy. Historically, some presidents have structured the NSC to take a greater leadership role in driving foreign and national security policy; others have used the NSC primarily as a coordinating body. However, as security challenges become increasingly complex, and as extensive capabilities must be integrated from across the entire federal government, the lead agency model clearly will prove inadequate in many cases. During the Bush Administration, the Department of Homeland Security has served as the lead agency for most major homeland security initiatives, but in the absence of firm backing from the White House and an HSC with the power to quash bureaucratic disagreements, DHS has typically expended a great deal of its efforts on intramural struggles within the executive branch.

What a Merged Council Would Look Like

Merging the two councils is the first step the new administration can take toward creating significantly more unity of effort in government efforts to prevent, prepare for, and respond to a catastrophe. A newly unified NSC and staff should be empowered to lead the interagency in formulating homeland security policy and overseeing its implementation on behalf of the president of the United States. To effect this merger, President Obama will need to ask Congress to amend the Homeland Security Act of 2002 by eliminating sections 901 through 906 of the law, which essentially establish the Homeland Security Council as a distinct organization. Unifying the Homeland Security Council and National Security Council organizations would also require amending the National Security Act of 1947 to make the secretary of homeland security and attorney general permanent members of the NSC. The current practice of inviting other Cabinet
heads to NSC meetings as appropriate to the specific substantive issues under consideration should continue.

The unified National Security Council would be led by the national security adviser (NSA) to the president, as is the case today, but the NSA would have two deputies – a deputy for international affairs and a deputy for domestic affairs. The national security adviser already holds one of the most grueling jobs in Washington, bearing the responsibility for a vast array of issues. Merging the two councils and their staffs would clearly add to this burden, but that disadvantage is more than outweighed by the benefits of addressing security issues holistically at the White House level. Assigning all security issues to a single national security adviser will ensure that the NSA has sufficient authority to resolve conflicts between Cabinet heads, particularly during times of crisis. Moreover, the two deputies would help lessen the challenge for the NSA of dealing with such a broad span of duties. These deputies would also need to be of sufficient stature to work effectively with top government officials, up to and including the level of Cabinet secretaries. During the Bush administration there have been as many as five positions labeled “deputy NSA” at one time; limiting their number to two would give the office more importance, bringing its holders much closer to being true seconds-in-command to the NSA. Moreover, should the international and domestic aspects of a problem seem to give rise to conflicting solutions or to require trade-offs, a single national security adviser with authority over the entire spectrum of issues will be positioned to weigh all elements and make a balanced recommendation to the president. Under the current model, the president has no single adviser whose job it is to weigh the competing domestic and international aspects of a problem and render an impartial judgment – overcoming the disagreements of Cabinet members, if necessary.

Under the merged council construct, with a single NSA and two deputy NSAs, much of the NSC staff would be shared and would report to both deputies. Some staffers might report only to one deputy, depending on their responsibilities. While President Obama should merge the two councils and their staffs, care should be taken to ensure that the “new” NSC organization complements its traditional national security expertise with senior staff who fully understand and possess considerable experience in catastrophe prevention, critical infrastructure protection, preparedness, response, and recovery issues. A merged council that is staffed only with traditional national security experts will not be effective at developing homeland security policy and guidance and would largely defeat the purpose of the merger.

Not only should the merged council include significant staff with expertise in homeland security disciplines, the council also should include staff that provide state and local government perspectives to ensure greater integration of these issues at the federal level. The National Security Education Program codified in Executive Order 13434 provides a mechanism to bring individuals with these backgrounds on to the merged council staff. Through the National Security Professional Development Program, senior state and local officials could join the council staff for a year to serve a detail assignment at the NSC. Under this type of program, senior people serving in the counterterrorism division of the New York City Police Department could spend a year at the White House, working in the merged council. This type of a rotational approach would also create opportunities for professionals at the federal level to serve in key positions in state and local governments, enabling them to use those experiences to
inform their work when they return to the federal government. Although achieving these kinds of opportunities presents a host of bureaucratic challenges, their achievement would be a major step toward creating a truly “joint” homeland security workforce with vertical and horizontal integration that would enhance national preparedness.

In addition to integrating state and local perspectives at the staff level, there are other means of infusing these perspectives into policy-making at the White House level. The next president could reinstate the Homeland Security Advisory Council established to provide advice and counsel to the Executive Office of the President. Re-establishing this council would be another way to craft sensible homeland security policies and create greater buy-in for these policies outside the Beltway. To avoid charges of drawing only on the “usual suspects” at the state and local level for input, the next president should allow organizations like the National Governors Association (NGA), the U.S. Conference of Mayors, and the National Emergency Management Association (NEMA) to choose some of the members of the advisory council. Creating new opportunities for state and local representatives to provide input into policy development at the federal level geared toward implementing a national integrated homeland security system would not only help to increase the feeling of ownership of new policies, but would also generate better understanding at the federal level of how homeland security needs vary by state and region.

**What a Merged Council Would Do**

Whatever the specific organization chosen by President Obama, to generate greater unity of effort the new unified National Security Council must play a much more prominent role in developing strategy and policy, and in overseeing the implementation of that policy, than either the NSC or HSC has done under the current administration. As integrated approaches to address future security challenges are developed, the roles of all relevant Cabinet agencies will not be equal. Some strategies may require that departments take responsibilities that are outside their traditional comfort zones; some resources may have to be shifted from one department to another. To ensure that clear policies are developed, difficult decisions are made, and turf battles are decisively resolved, a robust and unified NSC must act as honest broker and be empowered to carry out presidential decisions once they are made.

Some have argued that a merger is not particularly necessary, because the existence of separate Homeland Security and National Security Councils has not led to any major policy failures. The existence of two separate councils may not have caused any major policy failures, but it has caused the executive branch to miss important opportunities to develop more effective homeland security policy. For example, if the National Response Framework outlines how the federal government will operate with its partners “to the right of the boom,” there is no analogue to how the federal government will operate with its partners “to the left of the boom” – before a catastrophe takes place. There are many reasons the executive branch does not yet have a National Prevention Framework, but in part it is because developing a prevention framework would have required staffs from the NSC and HSC – who come from different professional disciplines and cultures – to work together closely, something they are not used to doing. Merging these staffs into a single organization would bring them together and begin building a corporate culture of
cross-fertilization and integration during policy development, which is sorely needed in
the broader homeland security enterprise.

Just as important as effective NSC leadership during the front-end phase policy
development is attentive NSC oversight of policy implementation. Such oversight does
not imply an operational role for the council and its staff; the pitfalls of an operational
NSC were amply demonstrated by the activities of Lieutenant Colonel Oliver North and
others on the NSC staff during the Reagan administration. But in light of the relative
autonomy of the Cabinet agencies, and the frequency of hard-fought battles over policies
and resources, the only way to guarantee effective implementation is for the NSC staff to
closely monitor the activities of Cabinet agencies. The current HSC organization does
not have the staff, expertise, or stature to perform such monitoring; the current NSC has
the necessary assets but lacks the power (which must be granted by the president) to
execute this oversight role. As a result, turf battles are fought and re-fought, policy
initiatives languish, congressional reporting deadlines are missed, and bureaucratic
logrolling is common.

When a Merger Should Happen

Although considerable progress has been made since the September 11 attacks in 2001,
the country is still not fully prepared to deal with a domestic catastrophe. What
ultimately matters to the American public is not how far we have come, but how far
away we still are from being prepared for the next catastrophe. Homeland security
received scant attention during the 2008 presidential campaign, but the task of readying
the United States to face the threats of the post-September 11 era is an enormous one
and poses a fundamental challenge for the new president. A merged NSC-HSC would go
a long way towards enabling the federal government to do its part to better prepare the
United States to face future challenges. Merging the HSC and the NSC would send a
clear signal that homeland security issues will now be a fundamental part of President
Obama’s mainstream national security policy and will be a top priority for the new
administration.

Christine E. Wormuth is a senior fellow in the International Security Program at the
Center for Strategic and International Studies, where she works on defense and homeland
security issues, including emergency response and preparedness challenges, homeland
security policy development, defense strategy and resources, and the capabilities and
readiness of the U.S. military.

Jeremy White is research assistant in the International Security Program at the Center for
Strategic and International Studies, where he works on issues relating to homeland defense,
Iraq, homeland security policy, and future military readiness. Questions and comments
regarding this essay should be directed to jwhite@csis.org.

1 Christine Wormuth and Anne Witkowsky, Managing the Next Domestic Catastrophe (Washington, DC:
CSIS Press, 2008), 17.

For example, in the Eisenhower and Nixon administrations the NSC clearly played a lead role in formulating foreign policy. The Kennedy administration’s NSC was much smaller, but its staff was dogged in ensuring that the federal departments implemented the president’s policies at the time. In contrast, in the Reagan administration the NSC organization largely shed its policy-making functions and adopted much more of a coordinating role. See The White House, “History of the National Security Council 1947—1997,” http://www.whitehouse.gov/nsc/history.html.


Technology Strategies for Homeland Security: 
Adaptation and Coevolution of Offense and Defense

Brian A. Jackson

Terrorists’ technology choices are a key part of their ability to create fear in target populations and audiences. Terrorists’ interaction with technologies that perform key functions within modern society – e.g., communications or infrastructures – can also be strategies through which they can produce damage and fear. It is the way the terrorist chooses to apply technologies – to cause death and destruction – that sets him apart from the criminal who may be comparably armed and equipped but who uses those technologies for personal or material gain. For homeland security organizations, responses to terrorist threats frequently gravitate toward the use of defensive technical systems. Significant sums of public and private funds have been allocated for development and fielding of security technologies and reduction of societal vulnerabilities. Making good decisions about investments in defensive systems – many of which are costly and intended to reduce the threat of terrorist attack over the long term – requires understanding the interaction between the technology strategies of the terrorist and those of the organizations charged with defending against them.

Technical aspects of the fight between states and non-state groups are frequently portrayed as a discrete interaction between the capabilities of the terrorist and those of the defender. The vehicle bomb is pitted against the perimeter security and any protective blast-resistant features built into its target; the anthrax-containing letter against the detectors in the mail system; the weapon smuggled in hand luggage against the technologies and training of airport security systems and personnel. At the end of this one-on-one interaction between weapon and defense, the attacker and defender step back to see if the terrorist was successful. Drilling deeper, however, makes looking at the fight as a set of discrete interactions appear increasingly artificial. Examination of the technological elements of terrorism invariably highlights the dynamic nature of the problems faced by the defense. The bomb planted by a terrorist group tomorrow will frequently differ from the bomb planted today: the terrorists change the explosive composition, modify the detonator circuitry, and alter the tactics used. The next day, the bomb may be discarded entirely as the group shifts to new attack modes, alternative weapons, and novel tactics.

Some of these adaptations will have nothing to do with the actions taken by the defender, resulting simply from the desire of the terrorists to be more effective or lethal. Detonator modifications may be an attempt to reduce premature explosions that kill only the terrorists. The appearance of a new weapon may simply mean that the group is seizing an opportunity, i.e. through theft, purchase, or gift; the organization obtains a new tool and wants to use it. Frequently, however, terrorists’ adaptation has everything to do with the steps taken to defeat them. New remote-control initiators are needed because the defender is jamming the groups’ current detonator or standoff weapons are acquired because security measures keep the terrorists away from desirable targets.

The opportunity for each side of the conflict to influence the other means the interaction between them is more complex and much richer than merely a sequential set of discrete clashes – and that defensive planning cannot be approached as if the
terrorism problem can be “solved” if simply the right defensive measure can be crafted and deployed. At the minimum, it is a multi-turn game involving many distinct players, where future clashes are informed by past actions – and by attempts to foresee future actions. But the depth of interaction goes further still: neither side limits its activities to perfecting its own future strategies based on the outcome of previous clashes, but also seeks to shape the environment of its opponent, even in the absence of direct interactions between them.

This bi-directional interaction – the terrorist shaping the environment of the defender and vice versa – can be viewed as a process of coevolution. In nature, coevolution is defined as reciprocal changes that occur to species that interact in the same environment. Coevolution occurs between species that compete – e.g., predators and their prey – where changes in one produce selective pressure for changes in the other. In biological processes these changes are genetic and are produced through natural variation, recombination, and selection. Changes arise; those that are beneficial are rewarded with survival and those that are not die out. Similar forces can drive organizational change, with the pressures exerted by each side on the other punishing poor technology or other choices.

It is our argument that thinking about the interaction of terrorist groups and security organizations in these coevolutionary terms is useful, particularly for analysts in organizations charged with designing security approaches and making investments in security technologies. Building on the results of a research effort at RAND focused on terrorists’ technology behaviors, we argue that such approach would appear particularly valuable for understanding threats to the performance of counterterrorism technologies, identifying opportunities to shape terrorist behavior in ways that are advantageous for security efforts, and can to help identify more robust and, potentially, less resource intensive approaches for homeland security technology design. In the following sections, we first explore terrorist choices and their implications for defensive thinking, and then transition to considering paths for creating “evolutionarily robust” defensive approaches.

PRESSURE ON THE DEFENDER – TERRORISTS’ TECHNOLOGY STRATEGIES

Choices made by terrorists are a primary determinant of the value and success of defensive efforts. Seeking to understand the drivers of terrorist technology strategies and identify likely future adaptations creates long-term challenges for security planning. The nature of terrorist groups poses difficulties for doing so, however. Looking across a range of groups and technologies, three central challenges are apparent:

- Terrorist incentives for adopting or rejecting new technologies are rarely observable or obvious, limiting the ability of planners to predict terrorist innovation trajectories;
- Terrorists have strong incentives to adapt well, and have identified multiple strategies for adaptation; and
• Terrorists confront defensive actions directly, degrading the utility and protective value of those actions.

Terrorists Have Varied Technology Incentives

Among analysts examining terrorist behavior, there is broad acceptance that terrorists adapt and evolve over time, though the forces that shape that adaptation are hardly transparent. This lack of transparency has provoked debate about the incentives for terrorist innovation, with evident uncertainty surrounding paths for future innovation. In considering terrorist weapons choices, many analysts have focused on the utility of novel and advanced weapons to terrorist groups, suggesting there will be enduring incentives for terrorist groups to seek them out and use them.5 Others point out that most terrorists appear to be “operationally conservative,” predominantly using basic technologies like the gun and the bomb, suggesting that incentives for innovation may not be particularly strong.6 Debates about the current terrorist threat and the potential for terrorist use of advanced or unconventional weapons can be viewed through this lens – where the view of terrorists as innovative or conservative frames assessment of the level of threat.

Though apparently contradicting one another, these two views of terrorist technology decision making do not, in fact, conflict. In selecting what technologies to pursue, terrorists’ strategies will undoubtedly be governed by a judgment about how the benefits of a technology compare with what is involved in obtaining it, what risks are associated with doing so, and on how attractive a new technology looks compared with other tactical and technological options available to the group. While terrorist groups may not necessarily think about these decisions in these terms, this decision process can be thought of as involving a comparison of the apparent costs and benefits7 of acquiring the new technology.8 Even if that comparison is implicit rather than an explicit, and will almost certainly be based on cost and benefit criteria that are idiosyncratic to the terrorist group, cost/benefit perceptions will underlie decision making. In this paper, we will use the language of costs and benefits to think through terrorist decisionmaking, even if actual decisions in groups may not approach anything like a formal comparison and may involve both costs and benefits that are unique to the groups involved. In some situations, the benefit of novelty will outweigh the costs and risks associated with it;9 in others, “tried and true” technologies will be good enough, particularly if there are many ways to apply those technologies in its operations.

Given the risks inherent to terrorist activities – and the terrorists’ desire that operations be successful – there will always be tradeoffs between novel technologies and dependable alternatives. Similar tradeoffs will exist for individual technology choices, where the terrorists’ assessment of their costs, benefits, and risks will determine whether the group pursues one weapon over another, uses cellular phones for communication or relies on e-mail, and so on. Differences in the environments of individual groups, or of different factions within the terrorist organization, will shape assessments and determine which technology will be chosen.
As a result, while some generalizations about likely terrorist pathways can be made – e.g., analysts can assess the variety of technologies potentially useful to terrorists, articulate why some might be more attractive than others, and rule out some entirely – many possible paths will always remain. The influence of “wild card” external influences, such as other terrorist groups that willingly act as a source of technologies for others, can shift the apparent costs, benefits and risks of technologies and significantly influence such judgments. Differences in groups’ environmental conditions (i.e., factors that shape their decisions about technology acquisition) could therefore produce markedly different outcomes from the perspective of the security planner and make it difficult to put bounds around groups’ likely technology strategies.

Terrorists Have Strong Incentives to Adapt Well and Varied Strategies for Doing So

Returning to the evolutionary analogy introduced in the opening of this paper, when they are challenged by strong anti- and counter-terrorism measures, terrorist groups have strong incentives to adapt to maintain their effectiveness and to survive. When faced by a change in its environment, an organization must adapt quickly. When the stakes are high and the change threatens the viability of the organization, speed is critical. To respond quickly, one of two conditions must exist: (1) a group must already have solutions to problems that can be used immediately, or (2) it must develop solutions quickly. Developing solutions rapidly depends on how well the group learns and implements its learning. Groups that learn well can be proactive in shaping their own environment rather than reacting to exogenous change; those that cannot may be unable to adapt fast enough to survive the environmental shift. Looking across groups that have been successful in their learning efforts, we have defined three broad technology strategies representing different combinations of these two elements:

1. Versatility

Versatile technology strategies focus on technologies that are suitable for a wide variety of operational contexts and tactical applications. “Guns and bombs” are examples of technologies that can be used in many different types of operations. Versatile capabilities are therefore transferable if the operations they are currently employed in are denied to the terrorist. This transferability enables rapid adaptation to certain types of environmental change. For example, it has been observed that many predators in nature are generalists to enable facile switching among prey types as environmental conditions shift. However, relying on versatility may limit the ability to adapt in other circumstances as it depends on the availability of substitute targets or operations where the technology is applicable.

2. Specialization

Specialized technology strategies focus on developing high levels of capability in specific areas. Specialization is required to respond to some types of change. For
example, as a result of jamming of radio detonators for their bombs, many terrorist organizations have been forced to make electronic modifications to circumvent the countermeasures. Doing so requires a level of specialized understanding of those systems, and a group without that knowledge could not adapt. Specialization may therefore enable adaptation in circumstances where relying on versatile technologies may fail. However, it may take time – since adaptation may involve “opening up” and altering the technologies that the group is using. Furthermore, specialization requires resource commitments to develop expertise and knowledge. This trade between the benefits of specialization (getting much better at a given task) and the costs (reducing performance for other tasks) can be observed in natural systems as well. Environmental shifts might also eliminate the value of a specialty (e.g., a group that made the choice to specialize in one attack mode would pay a steep price if security measures subsequently made it impossible to use it on desirable targets).

3. Variety

Variety-based technology strategies focus on maintaining a broad range of technology options to draw upon as required. In some cases, variety can be provided to the terrorist group by the market: when a range of commercial technologies for functions like communications are available, terrorists can switch among them as needed. Maintaining other variety can require on-going resource commitments (e.g., maintaining expertise in small-unit armed assault operations), though others may be less resource-intensive (e.g., groups returning to using command wire bombs as alternatives to radio detonation). The choice by a group to be a “jack of all trades” and maintain many different capabilities may limit its ability to develop high levels of expertise in any one area or technology.

Separating technology strategies into categories does not imply that individual terrorist organizations choose only one of these strategies. Large organizations can pursue more than one simultaneously, e.g., training much of the group in versatile technologies while isolated elements are allowed to specialize. Similarly, how the boundaries are drawn around a “technology” matter – e.g., while bombs as an element of operations are a versatile technology pursued by almost all terrorist groups, bomb components may be the focus of specialization activities.

Terrorists Take On the Defense Directly

Though weapons choices are a key part of terrorists’ technology strategies, a key driver for adaptive behavior and evolution are the actions taken by the defense. Looking across a variety of terrorist organizations, a similar set of strategies can be identified for how these groups evolve in response to defensive measures:

1. Altering operational practices

By changing the ways it acts or designs its operations, a terrorist group may degrade the value of a security measure. Such changes frequently include efforts
to hide from the technologies. Such options are particularly potent for technologies that must be “triggered” by detection of the terrorist (versus static defenses that are “always on”). The observation of such behaviors in biological systems has resulted in definition of a specific category of coevolution, “information coevolution,” capturing the efforts of organisms to hide from others’ detection capabilities (and the resulting pressure on the other creatures to heighten those detection capabilities in response).

2. **Making technological changes or substitutions**

By modifying its own technologies, acquiring new ones, or substituting new technologies for those in use, a terrorist group may be able to neutralize or circumvent a defense. The wide variety of applicable “off-the-shelf” technologies for many terrorist applications facilitates this strategy.

3. **Avoiding the defensive technology**

Rather than modifying how it operates, a terrorist group may simply move its operations to an area not covered by the defense. Such displacement changes the distribution of terrorism and, while this may constitute successful protection in the area where the technology is deployed, the ability to shift operations elsewhere limits the influence the technology can have on the overall threat level.

4. **Attacking the defensive technology**

If appropriate avenues are available, a terrorist group may attempt to destroy or damage a defensive technology. Groups may also attempt to exploit the technology to “turn it against the defender” by creating false alarms to waste resources, tire defenders, or desensitize the system.

Just as the three fundamental offensive technology strategies above constitute a menu from which an organization can build its strategy, groups facing defensive pressures can deploy these strategies in response. Extending the coevolutionary analogy, these mechanisms represent the way the terrorist selectively pressures the defender.

**IMPLICATIONS FOR HOMELAND SECURITY TECHNOLOGY STRATEGIES**

From the perspective of defensive planning, the variation in terrorists’ technology strategies means that homeland security organizations will always face a heterogeneous threat. For any given terrorist cell or group, local influences on costs, benefits, and risks of new technologies will make it difficult to generalize about likely technology strategies. Contemporary shifts in the structures and characteristics of groups – for example, terrorism inspired by broader movements (e.g., global jihadist, radical environmentalism, and others) – reinforce the likelihood of variety in technology decisions as weapon and other technology selections are based on idiosyncratic rationales. For large enough movements, this could produce dynamics not dissimilar
from evolution by natural selection: disaggregated decision making by individual cells producing extremely broad variation in technology strategies, with counterterrorist efforts exerting selective pressure on the results.

Terrorist interaction with defensive measures means that defenders face an additional and varied threat to their own actions and the defender is at a disadvantage. To plan its actions, the defense must attempt to predict the terrorists’ responses. Particularly if defensive measures are open to observation, the terrorists need only to wait and craft appropriate countermeasures. The terrorists are largely in control of when they interact with defensive measures – they get “last move advantage.” For systems that allow repeated interaction at an acceptable level of risk and, therefore, the chance to test them and experiment with countermeasures, this advantage can be important. There are also asymmetries in resource requirements: defensive actions, particularly for large and populous nations like the United States, are frequently costly and require long lead times. Those costs make attempts to defend everything against every threat untenable, while the terrorists’ efforts potentially create a high price for making flawed decisions about how and when to defend specific potential targets.

Given the difficulties posed by terrorists’ adaptive behavior, actions to limit such groups’ ability to adapt and learn are often one goal of counterterrorism action. Given the breadth of the terrorist threat, it is unlikely that such action will significantly reduce the heterogeneity in the threat faced by defenders. How should homeland security organizations responsible for defending the country against terrorism respond to the breadth of terrorists’ technology strategies and their capability to evolve over time? Our recent research suggests three possible paths.

1. Focus on defensive strategies that can adapt, therefore making it possible to counter adaptation by terrorist groups.
2. Accept that terrorist organizations adapt over time, and seek to influence the direction of that evolution.
3. Seek strategies where defensive performance is robust in spite of changes in the terrorists’ strategy or tactics.

The defender has the freedom to pursue one or more of these options when designing a defensive technology strategy. The following sections examine each path and example strategies.

**Designing Defenses That Can Adapt When Necessary**

The risk that adversaries will find ways around defensive measures clearly means that technology design efforts should include focused efforts to identify vulnerabilities that might be exploited and address them before the defenses are deployed. However, just as it is impossible to protect every target from every threat, resource constraints mean it is impossible to make every defensive technology impenetrable. As a result, a prudent homeland security technology strategy will recognize the potential for even well-designed defensive technologies to be circumvented. In that case, the burden is pushed back on the defender and reconstituting protection will depend on the defense’s ability
to learn and adapt. How well it can do so depends in part on the organizations maintaining the defense and the characteristics of the defensive technologies they have installed.

In natural coevolution, how effectively organisms change and respond is framed by how readily they vary, reproduce, pass on valuable traits, and how effectively nature eliminates individuals with poor characteristics. In comparison, organizations can have advantages and disadvantages in the speed and effectiveness of adaptive behavior. Organizations that can spread and implement proven strategies can speed their adaptation, without having to wait for the passage of time or attrition to reinforce good ideas. Conversely, organizations can also choose not to change. Bureaucratic friction, inertia, and politics can produce resistance to the spread of advantageous strategies and many organizations lack strong selective pressures to dispassionately drive poor strategies into extinction. As a result, choices and organizational characteristics that limit adaptive ability become disadvantages.

Given that terrorists will seek to learn their way around defensive measures, technology strategies should be designed in a manner that recognizes this goal. This applies both to individual defensive technology systems and defensive technology strategies. If the characteristics of a technology system are essentially fixed, it is a static target for terrorist adaptive efforts and, once circumvented, may produce little defensive benefit. A focus on ways to build adaptability into defensive systems is therefore an absolute necessity. Similar arguments can be made for flexibility in the way organizations carry out their activities – e.g., how information is analyzed and deployed to counter the terrorist threat – to enable adaptation as circumstances change. Shifts in the ways that terrorists are applying technologies, such as the scenarios explored in our analysis of networked information and communications technologies, also will require agility to expand or change defensive technology portfolios in response.

Forces that limit adaptability must also be considered and hedged against. Decisions that necessitate technological “lock in” and static properties will inevitably produce some vulnerability. The challenge in those situations is to manage that vulnerability to keep it within acceptable limits. Beyond the characteristics of specific technologies, choices made in how technologies are produced and used can also create vulnerability. Increasing dependence on individual systems for detection or communication might be problematic, for example, if a terrorist group learned how to deceive, spoof or penetrate the systems. If the capabilities provided by the technologies are woven too tightly into many preparedness and response systems, it might not be possible to “pull the plug” on the systems if they were compromised. The scale of investments made in specific technologies can similarly produce lock-in that constrains future adaptability. If the defense is pushed into making large-scale investments in a few defensive systems, the sunk costs, associated organizational structures, and commitments that coalesce around major programs may foreclose future alternatives. Depending on the nature of the threat, limiting the scale of current investments could be a strategy for preserving flexibility and adaptive agility.

The argument for flexibility can be made both with regard to individual technologies and to expenditures on security in total. Because the commitment of resources to
security is a major impact of terrorism on targeted nations, preserving the flexibility to scale back security expenditures as circumstances warrant is also important. Decisions that lock-in resource commitments produce friction limiting their movement to other areas (whether for security against other threats or to other more productive applications) and, therefore, significantly limit adaptability and agility. In nature, the tradeoff between commitment of energy and resources to defense versus growth/reproduction is particularly brutal – and devoting too much to defenses can produce negative outcomes as certainly as devoting too little. As a result, organisms are observed to “give up” defensive behaviors or traits because of competing selective pressures to grow and reproduce.28

Just as use of a “variety” strategy by terrorist groups can help them adapt more rapidly to changing circumstances, having a variety of defensive options and diverse technologies available can provide versatility to the defender. In an extended conflict against a given terrorist organization, the terrorist may eventually overwhelm or circumvent even the most adaptable defensive technology. If and when that occurs, new options will be needed. Given the potential for such “adaptive destruction” of individual security approaches, planning must consider defensive technologies as a portfolio, maintaining possibilities for alternative approaches in the event currently effective technologies are neutralized. Such a strategy should ideally be applied to organizational capabilities broadly, rather than narrowly in the technology realm.29

Building such a “palette” of capabilities will rarely be easy. While it may be simple enough to put certain types of technology “on the shelf” to be called upon if needed, capabilities that rely on individuals’ specialized expertise are more difficult to maintain. Preserving capabilities that are not currently high profile may also be difficult given pressures to use resources efficiently. However, this is one area where governments potentially have an advantage over non-state adversaries: large government organizations are more likely to have the resources needed to build and maintain a prudent portfolio of capabilities that can be called upon when needed.

Understanding and Seeking to Influence Adversary Evolution

Research on terrorist behaviors has shown that, even when defensive efforts do not fully “shut down” the activities of a terrorist organization, the nature and deployment of defenses strongly influence the perceived costs, benefits, and risk associated with possible courses of action. In response to defensive changes, groups have aborted operations and shifted their attention elsewhere, pursued new weapons procurement efforts, and instituted major security efforts to protect themselves from infiltration and arrest. This ability to influence behavior is at the heart of why an analogy to coevolutionary processes is useful and demonstrates that defenders have leverage to shape terrorist activities.

To adapt and evolve, terrorist organizations have specific needs for information, capabilities, and other resources. If strategies are devised to prevent fulfilling those needs, their ability to adapt effectively can be blunted. For example, security organizations should consider whether the efficacy of a defensive technology hangs on
the ability to “keep secrets” about how it functions, how such secrets might be compromised, and whether a terrorist group could discern them from the outside. Technologies which rely on such approaches can be fragile. Technology designers should also consider whether testing – such as action-reaction challenging by adversary probes – could provide vulnerability data, whether groups willing to sacrifice low-level operatives in exploratory operations against the system can learn how to evade it, and whether the system’s characteristics are sufficiently observable that an adversary might see how its capabilities might be saturated and overwhelmed. To the extent that features can be incorporated that defeat or degrade the ability to gather such information, the ability of the technology to deter or defeat terrorist operations will be bolstered.

The defense must also remain cognizant of other changes that might facilitate adaptation. For example, our examination of technology-transfer activities between terrorist groups demonstrated that such interactions can be significant influences on group capabilities and that a variety of incentives exist for groups to interact with one another. New technologies can facilitate group evolution as well. The integration of technical components in weapons systems that reduce the need for training and expertise before the systems can be used effectively could make the systems easier for non-state groups to use and increase their attractiveness. Shaping the incentives of potential knowledge sources is therefore important to limit how readily capabilities can spread among non-state groups. Such strategies do not apply where terrorists have many “commercial technology options,” such as information and communications technologies, as the broad availability of these technologies will defeat most attempts at control.

However, the general conservatism observed in most terrorists’ choices of weaponry and acceptable levels of operational complexity – i.e., reliance on “tried-and-true” firearms and explosives applied in straightforward ways – suggests a sensitivity to costs and risks that could also be used to shape terrorists’ behavior. Traditional counter-proliferation measures and efforts to deter specific types of attacks apply this strategy, seeking to limit the availability of key technologies and weapons, or increase the perceived costs and risks of particular courses of action. Our examination of next-generation conventional weapons suggests opportunities for actions to influence terrorists’ calculus about the attractiveness of specific systems. In contrast to weapons they manufacture for themselves, commercial weapons are inherently “black box” technologies for terrorists: without a full understanding of their electronics and other components, the user must trust that the weapons will function as expected. Incorporating technical controls into such weapons (e.g., that provide positional information on the weapon or restrict its functioning to permitted geographic areas through the global positioning system) could increase perceived risks and deter their use. To the extent that such controls can be designed to force terrorists into “all or nothing bets” – the terrorists are uncertain that the weapon will function until it is deployed at the intended target – the deterrent value is likely to be greatest.

Similarly, defensive measures that force terrorists to make focused investments in individual areas can “lock them in” and limit their future options. One advantage the terrorist group has is the ability to walk away from choices that are no longer
advantageous – but, the larger the investment and greater the expertise a group has developed in a specific area, the harder it is to do so. Furthermore, design of defensive technologies that cannot be defeated by a group through a “one time investment” – e.g., even if an adversary develops a countermeasure, implementing it requires ongoing action and commitment of resources – are superior. Depending on the magnitude of its available resources, such a “drag” could constrain the group’s violent activities.

Finally, defensive organizations have to foresee, to the extent possible how defensive choices might change the adversaries’ future incentives. Paradoxically, a group’s efforts to adapt and survive when faced with defensive actions can help it become a more potent threat than before the defenses were deployed. The most basic manifestation of this effect is the selective pressure technologies and other security measures exert on terrorist groups, eliminating the less talented individuals and reducing a group to a hardened core. But defensive measures could also direct terrorists’ choices in directions that are negative from the defenders’ perspective: if a particular security measure pushes terrorists toward attack modes for which no good defensive options exist, a country might be better off not implementing those measures or doing so only selectively–while pursuing the groups through other means that might be less likely to produce negative adaptation on the terrorists’ part. To the extent possible, these later-stage evolutionary pathways should be considered in the design of defensive technologies to ensure that short-term gains in security are not offset by the creation of larger long-term vulnerabilities.

Although the use of defensive measures to shape terrorist behavior could be a useful part of a broad-based homeland security effort, doing so requires that we assess the success and failure of security efforts differently than usual. When used to shape behavior, the goal of technology may not be to prevent every terrorist operation; in some cases technology may explicitly allow certain types of activities by groups as part of an effort to shape their future behavior. From this perspective, “scoring” the conflict between the defender and attacker should not be done based on binary success or failure in preventing individual operations, but on the long-term evolution of terrorist groups and their ability to pose a significant threat to the nation.

Identifying Robust Defensive Strategies

The heterogeneity inherent in the terrorist threat means that homeland security organizations must craft a defensive technology strategy to be robust across a wide threat spectrum, rather than optimized for the threat posed by some particular terrorist group. To the extent that robust solutions can be identified that are not directly tied to the nature or specific characteristics of the threat, defenses will also be less sensitive to any changes individual terrorist groups make that shift the level or type of threat they pose.

Examples of strategies that might provide “cross-resistance” to many threats include the design or retrofitting of fault tolerance and robustness into target systems so that damage will be minimized if attacks are carried out. Similarly, investments in rapid response and repair capabilities to provide resilience if a successful terrorist operation is
carried out provide another option. Such approaches have a number of advantages when viewed with terrorists’ technology strategies in mind. Increases in the robustness and resilience of systems can be implemented via changes that fundamentally alter the characteristics of a potential target – e.g., a critical infrastructure network – and it is therefore difficult for the terrorist to counter the system’s defensive value. Many such measures may in fact be invisible to terrorist efforts to gather targeting information and may deter attack across the system because of the increased uncertainty in outcome. For example, rapid repair of a damaged bridge, which the terrorist hoped would cause severe disruption in transportation systems, will deny the adversary his intended outcome and significantly reduce the effect on the nation, even if the attack itself is not prevented. In circumstances where the outcomes the terrorists desire can be denied, even without acting against or seeking to disrupt the terrorists’ actions directly, the threat posed by the organization can be neutralized without providing it with clear incentives or signals about how to make future attacks more successful.

Beyond general-purpose response strategies, building robustness into defensive strategies can also be achieved by considering individual defensive approaches within an overall “systems view” of homeland security. Though individual defensive approaches may be vulnerable to the counter-technology strategies described above, layered combinations of approaches and measures may be far less so. Implementing this approach requires consideration of the full set of defensive capabilities that can act to defeat or blunt the impact of terrorist action to assess how those capabilities will function as a composite defense. When added together, the effectiveness of defenses should no longer depend on “single links in a chain” – e.g., identification of a suspected terrorist at a border checkpoint or early detection of the release of a biological agent – where successful evasion by the terrorist or a single missed signal negates the value of the entire system. Instead, a focus on how even imperfect performance of multiple layers might reinforce one another and provide successive opportunities to detect and frustrate terrorist action can provide a more fault-tolerant defensive approach.

**CONCLUSIONS**

Thinking about terrorist and counterterrorist conflicts in a dynamic way is superior to viewing them as single, static engagements between adversaries. However, simply saying such a conflict is dynamic and observing that terrorists adapt and change over time helps security planning only modestly. It is indeed true that terrorist threats are heterogeneous and will shift over time, but planners shouldn’t therefore conclude that the answer is that they must protect every target from every conceivable attack mode. Such a strategy would quickly collapse either under weight of the resource levels required or by spreading defenses so thinly that the performance of the entire security effort was put at risk.

In this discussion, we used coevolutionary theory and examples from the natural world to set up a different way to think about such dynamic conflicts. The central advantage of approaching the problem this way is that it helps to break the tendency – particularly in the design of technical systems – of viewing security measures as
“solutions” to particular and static security problems or assuming that a technology that is effective in some part of that problem space now will be effective indefinitely. This sets up different ways of thinking about the efficacy of defensive measures – in terms of the opportunities they provide to shape adversary behavior, the value of defenses being adaptive so they can be retargeted or modified to address changing threats, and the importance of seeking out defensive strategies whose performance is less sensitive to whether terrorist groups evolve or how they do so. Whether pursued singly or in combination, these strategies can each contribute to building overall homeland security policies that are more robust in the face of the “adaptive destruction” threatened by terrorist groups coevolving under the selective pressures those measures exert on them.

Brian A. Jackson is a senior physical scientist and the associate director of the Homeland Security Research Program at the RAND Corporation. His research focuses on the technological aspects of the terrorist threat and design and assessment of homeland security responses. Mr. Jackson can be reached at bjackson@rand.org.

Acknowledgments
The author acknowledges the contributions of other RAND staff members in the overall research effort on which this paper is based. In particular, David Frelinger and Kim Cragin helped to refine the specific ideas and provided valuable input to earlier drafts of the manuscript. The research described in this paper was supported by Contract # W81XWH-05-F-0191 with the Department of Homeland Security, Science and Technology Directorate, Office of Comparative Studies. The views expressed are the author’s and do not necessarily reflect the views or policies of the RAND Corporation, DHS, or any of RAND’s other research sponsors.

1 We have used the plural of this term to emphasize that many organizations contribute to the terrorism defense mission. We will refer to this constellation of organizations as “homeland security agencies” and generically as the “defense” or “defender” in the fight against terrorist organizations.


3 For example, in interviews with the author, law enforcement and intelligence practitioners have frequently cited the selective effect of counter- and anti-terrorism measures for removing less effective and skillful terrorists.


7 Including not only financial costs but also time, personnel, and other resources needed for adoption.

8 For discussion, of costs and benefits from the terrorists’ perspective, see Brian A. Jackson, “Technology Acquisition by Terrorist Groups: Threat Assessment Informed by Lessons from Private Sector Technology Adoption,” Studies in Conflict & Terrorism, 24, 2001, pp. 183-213.

9 Advanced weapons like antiaircraft missiles provide a useful example: clearly their value to some groups is sufficient to enable use, though the spotty results gained by doing so emphasize some of the risks of new technologies. See, for example, Marvin B. Schaffer, “The Missile Threat to Civil Aviation,” Terrorism and Political Violence 10, No.3 (1998): 70-82.


11 This case is analogous to the observation in biology that organisms may maintain traits that are not currently advantageous, but may become valuable if their circumstances change.


15 Similar arguments could be made for terrorists that became specialized in using particular weapons (e.g., mortar experts) or in attacking particular classes of targets (e.g., armed assaults on specific infrastructure targets.)


17 Specialization by the offense can simplify the field for the defender. Resource investments in specialization lock in the terrorist group to some extent along specific trajectories. For a particular group, knowledge of specialization can make it possible to shape more specific defenses to the group’s actions. This therefore exposes a larger fraction of the group’s capabilities to risks (that are difficult for the terrorist to predict) and generate disincentives to specialization for some groups.


23 This creates dynamics on the defensive side regarding how much is revealed and obscured regarding the nature and functioning of defensive measures. To the extent that such secrets can be kept, terrorist learning – and this particular component of the threat – can be blunted or delayed.

24 See Brian A. Jackson, *Aptitude for Destruction, Volume 1: Organizational Learning by Terrorist Groups and Its Implications for Combating Terrorism*, MG-331-NIJ (RAND Corporation, 2005) for additional discussion of targeting groups learning activities as part of counterterrorist efforts.


26 In contrast to the real selective pressure that counterterrorist efforts exert on terrorist organizations and their members – providing mechanisms where poor strategies are indeed eliminated through arrest or attrition.


29 For example, maintaining capability in a variety of intelligence collection and analysis techniques is valuable, even if only a subset of them are high value at a given time. As circumstances change, techniques that are currently not applicable may become important as terrorist behavior changes or new intelligence data sources become available.


31 Both to the effective functioning of the weapon (and, therefore, risk to the success of any operation in which it was used) and security risks to the organization overall through the potential for tracking the weapons.

32 Such arguments similarly apply to defensive measures more broadly, not just those related to controlling the use of advanced weaponry.

33 For example, for a notional terrorist group, the broad implementation of defensive measures against the use of small explosive devices could produce a strong pressure to adopt vehicle bombs to reconstitute the group’s ability to strike attractive targets. Since the use of vehicle bombs would significantly increase the group’s destructive capability and could be more difficult to counter, it might be a better defensive strategy to either not deploy the defenses or do so at only the most vulnerable targets (thereby reducing
the evolutionary pressure on the group to seek out alternative attack modes), while focusing resources to pursing the group’s members through law enforcement action. Though law enforcement action aimed at a group would produce evolutionary pressures of its own, those pressures might be less likely to move the group towards more destructive attack types.

34 Such an approach could be termed building in asymmetry into defensive measures where advantage is preserved for the defender across a range of possible attack options and scenarios. Such strategies are also attractive because they can provide robustness and resilience against threats that have nothing to do with terrorism – e.g., robustness of electricity infrastructures to outages produced by storms or natural disasters – and therefore produce benefit streams to the defender irrespective of the realized terrorist threat environment.
The Terrorist Threat to Inbound U.S. Passenger Flights: Inadequate Government Response

Anthony Fainberg

INTRODUCTION

Seven years have elapsed since Richard Reid, a British citizen partially of Jamaican extraction, tried to detonate a shoe bomb aboard an American Airlines flight departing Paris and bound for Miami. The flight was diverted to Boston after his attempt failed. Reid has since been tried and convicted of attempted mass murder; evidence presented at his trial indicated that he was an al Qaeda operative who acted with technical and logistical help of others in that organization. He had, in fact, proclaimed his allegiance to Osama Bin Laden, had traveled to Pakistan and Afghanistan during the previous year, and has been identified as an al Qaeda trainee, at the least.¹ He had also, apparently as part of his efforts for al Qaeda, earlier assessed air security procedures in Israel and reported that security measures were too stringent to expect a high likelihood of success in an attack on a plane there. So he (and his collaborators) decided to attack a U.S.-flag carrier, departing Charles DeGaulle Airport in Paris. Reid used a now famous, home-made chemical explosive – triacetone triperoxide (TATP) – as a detonator, but the main charge in the shoe was composed of pentaerythritol tetranitrate (PETN), commonly used as both a military and a commercial explosive.

Because of his bizarre behavior and strange travel plans (e.g., no luggage for a transatlantic trip), Reid had been blocked from boarding the flight on December 21, 2001² by the personnel of a security company hired by American Airlines. He had been interrogated for some time, but security personnel could find no incriminating evidence or other reason to persuade the carrier to deny him boarding rights, and so he was permitted to get on the same flight on the following day. He then tried to destroy the aircraft in flight with his bomb. That he failed was not due to classic security measures or systems but rather to the bravery of a flight attendant (who detected his efforts) and several passengers who assisted her in subduing the criminal.

It was unfortunate that French airport security had no explosives detector at hand that could have found the telltale traces of chemicals on Reid or his clothes. If they had, they probably would have detected at least the PETN on Reid’s shoes, if not on other parts of his body or clothing. We know this because traces of this chemical were found in considerable quantity on the inside wall of the aircraft where Reid sat and against which he placed the bomb – his shoe – while trying to set it off. These traces were easily found three weeks after the fact, even following cleaning of the aircraft.³

This essay asserts that the terrorist threat to global civil aviation continues to exist and that the United States aviation system remains a principal target, particularly of al Qaeda. Historical evidence will show that this threat is currently more serious overseas than it is domestically and that the terrorists’ modes of operation often include the introduction of explosives aboard aircraft by passengers. Noting that explosive trace residue detection technology, currently deployed in the United States, could help
mitigate this threat, this essay urges that the United States require the application of such technology overseas on flights inbound to the United States. In the past, the Transportation Security Administration (TSA) has been reluctant to act in this direction, probably out of concerns for the sensitivity of the sovereignty of other nations. However, taking note of the fact that the United States already imposes aviation security requirements on inbound flights, and has done so for years, this essay argues that diplomatic means already exist to improve our response to aviation terrorism overseas and that these means should be applied.

The Historical Problem

Since Richard Reid’s attempt, there has been one other similar and major aviation security incident with a less fortunate result. This was a successful pair of attacks on commercial aircraft in which explosives were brought on board by passengers. Chechen women carried bomb vests on two Russian domestic aircraft on August 24, 2004, detonating them in flight and killing all eighty-nine persons on board the two airplanes. No trace detection systems were in place or used on departure; the women had reportedly bribed air security personnel not to inspect them too closely or demand to see identification.

Attempts to simultaneously destroy many U.S. aircraft simultaneously, with the likely hope of eliminating global commercial air travel for many weeks, date further back, at least to 1995 and the “Bojinka” plot in Southeast Asia. This plan was organized in part by terrorist mastermind Khalid Sheikh Mohammed (identified by U.S. authorities as the main organizer of the 9/11 attacks), along with his nephew, Ramzi Youssef, who also organized the first attack in the World Trade Center in 1993. A stream of known incidents since 9/11 confirms the interest of terrorists in targeting civil aviation. All of these incidents had their origins in other countries, not in the United States. The London bomb plot of August 2006 is perhaps the best known of recent cases. In addition, there was the June 30, 2007 attack on Glasgow airport itself, carried out by Islamic extremists. This latter was not an attempt to bring explosives on an aircraft but did demonstrate the intent to target civil aviation.

Although major aviation-targeted incidents have not come to light every year since 2001, we should not be lulled by the sporadic nature of low statistics. As noted here, and in the endnotes, such incidents have occurred in 2002, 2004, 2006, and 2007. In the field of terrorism, an absence of reported activity for a year or two does not mean that we do not have to worry. Further, government officials may well have more information on the terrorist threat to civil aviation, both at home and overseas, than is publicly available. One may glean this, for example, from worries expressed in a 2002 statement by the Federal Bureau of Investigation and in the much more recent statement of Secretary Michael Chertoff before the National Press Club on September 10, 2008. The focus on civil aviation as a terrorist target is also consistent with al Qaeda’s somewhat unimaginative and obsessive-compulsive practice of repeatedly using an attack tactic – if it appears to them to be a good idea – even when it does not succeed at first.

In the seven years post-Reid and four since the Chechen attacks, the U.S. government – that is, the TSA – has apparently not acted to assure that passengers on all foreign
commercial flights into the United States be subject to screening for explosives, using chemical trace or vapor detectors. This is in spite of the fact that, for years, the TSA has deployed thousands of pieces of such equipment for use in U.S. airports.

Standard risk assessment and risk mitigation formalism indicate that, given equivalent consequences, one should generally try to reduce vulnerabilities where threats are higher. The apparent inaction of the TSA in regard to flights originating overseas appears to violate this principle. Threats to civil aviation are most likely greater overseas than they are in the United States, but the vulnerabilities of U.S.-bound overseas flights to terrorist attacks are greater than threats to domestic flights, not less. This is because equivalent technical security measures applied to civil aviation in the United States are not required for the overseas, inbound flights.

Where is today’s technology relative to that of the recent past? If anything, today’s trace chemical detectors, used in domestic U.S. airports, are even more capable than those of several years ago. They are able to detect TATP, in addition to other explosives and oxidants that have often been used (or planned to be used) to construct terrorist bombs for detonation aboard aircraft.

These detectors are relatively inexpensive ($25,000-40,000 each), quick to acquire, widely used in United States airports, well understood by aviation security authorities, and easy to operate. Any traveler flying commercially in the United States since 9/11 has almost certainly seen these detectors: they are mostly the size and shape of a breadbox – although some more experimental walk-through portal “puffers” are now being tested – and are located at security checkpoints. The breadboxes are characterized by the sad fact that they are used quite rarely.

Furthermore, even though the 2006 plot against U.S. commercial jets was London-based and involved attacking flights originating in the United Kingdom, newer models of detectors devised by the TSA to counter that particular threat are being pilot tested in the United States but are not (as of this writing) being tested abroad. It would appear that the United States is reluctant to deploy effective technologies outside the country, even on a test basis. Unfortunately, at the risk of being repetitious, outside is where the greatest threat currently dwells.

Use of this trace detection technology would have two effects. First, when properly applied, it could effectively detect attempts to bring explosives onboard aircraft. Second, the deployment and use of such equipment would at least deter terrorists from using this pathway to attack civil aviation. In the past, terrorists have used “dry runs” to test the effectiveness of aviation security. The 9/11 terrorists, in particular, ran many such trials. Therefore, yet another advantage of deploying trace detection technology would be that security authorities could then look for attempts by terrorists to probe the effectiveness of this new technology overseas, thus providing another means to counter attempted terrorism.

The Institutional Problem

Why has the TSA decided not to provide passengers on U.S.-bound flights from foreign airports with the same explosives detection equipment required for securing domestic air travel? The answer is unclear. Some reports, mostly from private statements by
government officials, indicate a fear of diplomatic resistance from other nations, who would, it is said, object to the imposition of American security requirements. If true, this concern may be based on a misunderstanding of U.S. ability to impose security on flights into the U.S. from elsewhere. It is true that the sovereignty of other states certainly could become an issue. However, this sovereignty can be and has been respected while, at the same time, assuring desired levels of protection. The U.S. government has taken steps to enable this.

Following a spate of terrorist attacks in the Middle East in the 1980s, including the hijacking of TWA Flight 847 after departing Athens, the U.S. Congress passed the International Security and Development Cooperation Act of 1985, which, as reflected in 49 U.S. Code Section 44907—Security Standards at Foreign Airports—requires the government to assure desired levels of security on flights into this country. If foreign governments do not agree to the employment of such measures, paragraph (d) (1) (D) specifically states:

The President may prohibit an air carrier or foreign air carrier from providing transportation between the United States and any other foreign airport that is served by aircraft flying to or from the airport with respect to which a decision is made under this section.

The authority for U.S. government action unquestionably exists.

On the other hand, perhaps the government feels that, eventually, this problem will be solved by the voluntary actions of foreign airport security authorities. It is true that a few nations have, on their own, begun to use trace detectors on outgoing flights, at least on an occasional basis. But there is no guarantee, or even likelihood, that these detectors will be required by foreign authorities for all U.S.-bound flights in the near future. Nor is there any evidence that the U.S. government has taken steps to assure widespread overseas deployment of such equipment. Such steps should be taken.

In a related context, the TSA has made public its reticence to interfere with the aviation security practices of other nations. It recently stated explicitly, in a report by the Government Accountability Office (GAO), that it will not “impose its security requirements on foreign countries.” This is in reference to a different but equally disturbing security gap—one that continues today, domestically as well as overseas—having to do with inadequate screening for explosive devices in cargo aboard passenger aircraft. Congress has required 100 percent screening of such cargo by August 2010. TSA is now taking steps to meet this mandate for flights originating in the United States, but not for those originating overseas. This method of attack—placing explosives in cargo—has been attempted by terrorists in the past.

Somewhat in contradiction to the TSA statement cited above is the recently announced “Joint Statement of Purpose on Coordination of Efforts to Enhance Air Cargo Security” between the TSA and the Energy and Transport Commission of the European Union. While not specific in technical detail, this accord does express an agreement with other nations to develop “compatible standards and practices to enhance civil aviation security,” aiming at the “rapid introduction” of detection technologies for air cargo security. Thus, at least on this level of generality, and dealing with air cargo, there is a demonstrated willingness on the part of TSA to engage our
overseas aviation partners. Similar efforts could and should be devoted to the use of appropriate technologies for the screening of passengers.

Any reluctance to require other countries to impose U.S.-approved security measures is not ruled by precedent; in fact, it runs counter to past practices. Over the past several decades the U.S. government, through the Federal Aviation Administration, has negotiated bilateral security agreements with several countries hosting the “last point of departure” of a commercial flight into the United States. These accords were usually arrived at in fairly collegial fashion. The hidden, but well-understood leverage for the FAA was the knowledge that, if an agreement were not reached, the United States could and would eventually prevent aircraft from the country in question from landing at U.S. airports. This approach worked quite well in terms of negotiating agreements with a minimum of fuss and discord.

The U.S. government has taken action against some nations for lax security standards. The International Security and Development Cooperation Act, cited earlier, was invoked when flights between the United States and the Murtala Muhammed International Airport in Lagos, Nigeria, were banned between 1993 and December 22, 1999. Milder forms of sanctions have been imposed on other countries from time to time: for example, warning notices have been posted on occasion in U.S. airports to inform passengers bound for Haiti and Indonesia of security concerns there. Similar concerns over airport security – which could have led to such postings – were expressed to the government of Greece in 1996.

Another example of the ability of the United States to affect aviation security practices overseas is secondary screening (that is, screening in addition to that employed at the standard airport checkpoint) on U.S.-bound flights. Such screening has been arranged in the past through FAA-proposed modification of bilateral agreements and practices. This occurred, for example, following the destruction of Pan Am 103 by Libyan-supported terrorists in 1988. The screening was performed by air carrier personnel in some locations and by local authorities in others, where local laws required the use of local nationals in such security roles.

Indeed, in the case of U.S. carriers operating inbound flights, no particular agreement is even needed with the host country: TSA and FAA regulate these carriers when operating either domestically or overseas. Security plans governing overseas security measures for U.S. carriers operating overseas, known as Air Carrier Standard Security Plans (ACSSP), were explicitly approved by the FAA for the U.S. government. Today’s analogous version, with TSA now the cognizant authority, is the Aircraft Operator Standard Security Plan, under 49 CFR Part 1544. Foreign air carriers flying inbound are not de jure regulated. But, de facto, they must submit to U.S. security requirements in that their security measures, listed in Model Security Plans (MSP) must be “accepted” rather than “approved” by TSA if the foreign carrier wishes to land in the United States (under 49 CFR Part 1546).

Additionally, bilateral agreements with foreign partners can formalize and indeed already have formalized security arrangements that the United States desires on inbound flights. This is usually done with respect to assuring practices consistent with recommendations and standards in Annex 17 (Aviation Security) of the Chicago Convention of 1944 on International Civil Aviation and agreed to by the International
Civil Aviation Organization (ICAO). Inspectors from the TSA (formerly from the FAA) are based overseas and visit airports in other countries to assess, for the U.S. government, whether the security practices there conform at least to ICAO standards. In some cases, the standards of Annex 17 are exceeded, following specially negotiated bilateral agreements between the United States and certain countries hosting inbound flights.

There is thus no question that the United States has diverse legal and political means at its disposal to protect its citizens and visitors on inbound commercial aircraft. The only question is exactly what these requirements will be and whether the U.S. government will insist on increased protections when justified by threat assessments, based on past incidents and on present information. What should be required is a set of security measures and technologies equivalent to the ones imposed on air carriers and those practiced at airports domestically. These should include the widespread application of trace chemical detection to (at least) a subset of selected passengers, both for deterrence and as a protective measure. They should also include the congressionally-mandated 100 percent cargo screening on flights into the United States, as well as on domestic flights.

ISSUES

This discussion may be summarized by addressing several questions.

Is there still a terrorist threat to civil aviation and is the international threat more serious than the domestic threat?

Yes and yes. Disrupted plots, incidents that appear to be tests of aviation security systems and actual attempts of various types on civil aviation, have occurred persistently since 9/11. Most of these incidents involved the use or planned use of contraband items smuggled on board by passengers. Occasional statements from official sources, such as the Federal Bureau of Investigation and the Secretary of Homeland Security, indicate that intelligence sources consider that aviation continues to be a terrorist target. Reasonable people would conclude that the threat is real and current.

Nearly all disrupted plots involving U.S. civil aviation were planned to originate overseas (e.g., in London and Paris). A series of bizarre events, referenced in note 5, that appeared to be tests of security systems occurred overseas (Sweden, Pakistan, Morocco, and France). Attacks or planned attacks on aircraft have originated at overseas locations (Kenya, France, United Kingdom). None of these events occurred or had its planned origins in the United States. Jihadi terrorist cells have been broken up in the United States in the past, but no serious round-ups have been reported for several years. Far stricter immigration controls and visa requirements have been imposed in the United States since 9/11. One concludes that the major threat to civil aviation continues to be external to the United States, in great part because of the difficulty terrorists have in developing a strong presence here. This is not surprising given the intensive effort devoted to detecting terrorists and keeping them out – an effort aided by the long distances and logistical problems most terrorists face in getting to the United States.
Of course strategies should not be confined to fighting the last battle or, equivalently, the last mode of terrorist attack. We have to think ahead and plan to protect against new and plausible modes of attack against civil aviation or, more broadly, against the United States and the rest of its critical infrastructure. Nevertheless, we should not leave the last terrorist attack type inadequately defended against, especially since our current adversaries have a tendency to repeat themselves and maintaining inadequate defenses would be an open invitation to strike.

**How many people fly into the United States every year?**

Approximately 6 percent of total U.S. passenger traffic on U.S. air carriers is on international inbound flights. For the first four months of 2008, this amounted to about 15 million persons, assuming half of international flights are inbound and half are outbound and both halves have roughly the same capacity. It is likely the yearly total would be nearly 50 million persons, with a large percentage of these U.S. citizens. There are also a large number of passengers on inbound flights aboard non-U.S. carriers. Although representing only a fraction of the total number of air passengers in the United States, 50 million+ people constitutes a very large number of travelers to put at unnecessary risk.

**Are there currently available detection technologies that could reduce the terrorist threat to international civil aviation?**

There are several such technologies, not only in existence but also widely deployed in the United States. These include computerized tomography scanning systems for checked baggage (which is not required of inbound flights from overseas) and for some cargo; use of canine olfactory capabilities; and various explosive trace residue and vapor detectors for passengers, carry-on baggage, checked baggage, and cargo. Other nations do use some of these techniques, but the United States does not require their use on incoming flights to provide equivalent levels of security to those that exist domestically. The United States could require use of such technologies on incoming flights of foreign origin, as it has for years required other security procedures on such flights.

**How much would it cost it cost to deploy and operate sufficient trace detection systems to screen passengers at all last points of departure to the United States? Is this cost practicable?**

The cost would be approximately one percent of the cost of deploying checked baggage screening systems within the United States, as was correctly and well done by TSA following 9/11. A few tens of millions of dollars in capital cost would suffice, plus several million (conservatively, on the order of ten million) additional dollars per year for operation and maintenance. In comparison, solving the checked baggage problem domestically – an essential step – cost several billion dollars in capital acquisition over several years. Of course, additional diplomatic effort, including discussions with other nations, would have to be expended as well, with resources to this end probably taken out of ongoing operational government funds. The U.S. has supported an overseas civil service infrastructure for years, which maintains aviation security liaisons with nations from which flights to the United States originate.
Are there legal and diplomatic mechanisms available to the United States to ensure the implementation of additional security measures for inbound flights? Have such measures been employed in the past?

Existing legislation and past practices in this regard are cited above. The answers are: yes and yes.

CONCLUSION

There is a continuing terrorist threat to commercial civil aviation. The threat is global, but the United States remains a principal target of such attacks. Many threats, past and future, revolve around the scenario of weapons or explosives brought onto aircraft by passengers. Chemical trace detection equipment, relatively inexpensive and quite effective, could be applied to reduce this threat significantly, both by actual detection and by deterrence. Such equipment is widely deployed domestically by the United States, but it is not broadly used in other countries.

The United States can and should require the use of such equipment to screen passengers on all inbound flights, to avoid repetitions of Richard Reid-type attacks in the future. It should, in fact, take broader steps to require the application of security measures equivalent to those used in the U.S., including the use of appropriate technologies, on inbound foreign flights at their last points of departure.

Anthony Fainberg is a physicist and analyst, specializing in national security affairs. He recently retired from the federal government, following service in several agencies and departments, including the Department of Homeland Security, the Transportation Security Administration, the Federal Aviation Administration, and the Defense Department, as well as in the former congressional Office of Technology Assessment (OTA). He was trained as a particle physicist, earned his PhD at University of California, Berkeley in 1969. He was one of the first to study comprehensively the role of technology in counter terrorism, in OTA reports in 1991-2. His other interests include nuclear non-proliferation and countering nuclear terrorism. Mr. Fainberg can be contacted at fainberg666@comcast.net.

Acknowledgement: The author would like to thank Dr. Fred Roder for reading the manuscript and providing many helpful suggestions.


2 Perhaps not accidentally, this was the 13th anniversary of the destruction of PanAm Flight 103, by Libyan agents, which killed all 259 persons on board as well as eleven more on the ground in Lockerbie, Scotland.

3 The author, while a government official, took the samples on the aircraft and had them analyzed at a competent laboratory.

4 The Bojinka plan, discovered only following an inadvertent fire in the conspirators’ apartment in Manila, envisioned destroying over ten U.S. aircraft in flight from various ports in the region to the United States.
A practice run, on a domestic Philippine Airlines flight to Manila in 1995, succeeded in placing a small bomb under a seat on the aircraft. The passenger in the seat was killed, but the explosion narrowly failed to bring down the aircraft.

www.cbsnews.com/stories/2002/12/24/attack/main534164.shtml reports an FBI warning, on Christmas Eve 2002, of attempts to bring down aircraft through bombs brought on board by passengers. Moreover, a spate of incidents in the late summer of 2002 may indicate an interest, at that time, in testing aviation security on a global level. Best known were an arrest of a Muslim Swedish citizen, on his way to a Salafist conference, for carrying a pistol onto a plane (charges later reduced to a weapons violation) that was scheduled to fly from Vasteras, Sweden to Birmingham, England, (August 29, 2002); an Afghan headed for the United States arrested in Karachi when trying to board an aircraft with a weapon (August 26, 2002); and a quantity of PETN, found during a random test by canines in Nancy, France, aboard a Royal Air Maroc jet that had just landed there on a flight that had originated in Morocco (Sept. 25, 2002). There have been other attacks on aircraft in the interim, including a failed surface-to-air missile attempt against a commercial Israeli aircraft in Mombasa, Kenya, in November 2002. The most famous event since then has been the disruption of the London bomb plot in August 2006 by British M.I.5. Different, liquid-based explosives were planned for this effort, but seven aircraft departing London were apparently targeted for detonations in rapid succession. The detonating chemical in this case was allegedly HMTD (rather than TATP), which is also susceptible to trace detection. Hydrogen peroxide would be similarly detectable. This was another chemical component of the planned explosive device. See E. Sciolino, "In '06 Bomb Trial, a Question of Imminence," New York Times, July 15, 2008. Three participants were convicted in 2008, see http://www.cnn.com/2008/WORLD/europe/09/08/bomb.verdict/index.html.

In response to a question, Chertoff stated, “Al Qaeda continues to focus on the aviation system as an area where they want to target,” http://www.dhs.gov/xnews/speeches/sp_1221138850495.shtm.

Examples of al-Qaeda or al-Qaeda-related personnel behaving in this way are multiple. The attack on the U.S.S. Cole in October 2000 followed a failed attack some months earlier on the U.S.S. The Sullivans, both in Yemen. The London bomb plot recalls the Bojinka effort. The attacks on the U.S. embassies in Kenya and Tanzania in 1998 followed a crackdown on terrorists in the area a few months before. And finally, of course, there is the World Trade Center as target, attacked unsuccessfully by terrorists including Khalid Sheikh Mohammed – later an al Qaeda operative – in 1993 and attacked again in 2001. There are other examples where repeated, similar attacks occur; some actually succeeded, such as the London train and bus bombings following the Madrid train attacks. Experts debate how closely all these efforts are related in terms of planning and direction. For the present discussion, this issue is irrelevant: whatever the specific provenance of the attacks, whether by unitary direction or simply by example, repetitious modi operandi do characterize recent jihadist terrorism. And another leitmotif that constantly recurs is the commercial aircraft as target.


Federal Register / Vol. 64, No. 250 / Thursday, December 30, 1999, 73596.

INTRODUCTION

The purpose of this article is to identify the financial costs relative to the benefits of the “no-fly” list. Numerous scholars, security experts, lawyers, non-governmental organizations (NGOs), journalists, and bloggers have commented on the well-known flaws in the current terrorist watch list system. Lawyers have pointed out the many civil liberty issues associated with the list and its hindrance of due process. The American Civil Liberties Union (ACLU) has repeatedly published the many flaws it sees in the way that the list is administrated. Bruce Schneier, a popular security columnist and blogger, documents the various reasons why the no-fly list serves no benefit at all, providing only “security theatre” rather than actual protection. Each of these analyses is useful and contributes to an understanding of whether or not the no-fly list is, in aggregate, helpful in protecting citizens against terrorism, and at what social and civil liberty cost.

What is missing, however, is an analysis of the no-fly list from a financial perspective. This article is interested in understanding the monetary costs of the program. As such, it seeks to answer some basic and fundamental questions that have not yet been answered (or asked): How much does the no-fly list cost to create and maintain? What are the costs of the consequences, both intended and unintended, of the list? How many resources, both governmental and private, are involved in the operation of the list? And, what are the benefits, both tangible (i.e. monetary) and intangible, that the list provides? This is an important set of questions because without understanding the monetary costs of a protection program relative to the benefits, it is difficult to assess whether or not the program is worth the costs. Further, without such an understanding it is impossible to intelligently decide how anti-terror money should be allocated. It is surprising that, given the importance of these questions, they have not been asked and addressed in a systematic fashion.

Consequently this article represents a “first take” at addressing these questions by assessing the financial costs of the no-fly list program. It does not, however, seek to serve as a comprehensive answer to the question of “is the no-fly list worth the money we are putting into it?” The reason is that one cannot begin to conduct such an analysis without aggregating the costs and benefits first and then placing the no-fly list in context of the other anti-terror programs and their associated costs. The no-fly list might very well be worth the expense if it is the government’s only tool in preventing terrorist attacks. It might also be the case that the list is less valuable given redundancy in the “layered security” model of securing air travel. These are important questions and ones that can only be addressed after having identified the financial costs and benefits of the program. Thus this article should be viewed as the first step in what will hopefully become a systematic and comprehensive approach to understanding whether
or not the no-fly list provides added value in the context of the government’s anti-terrorism campaign.

As will be analyzed below, it is estimated that the costs of the no-fly list, since 2002, range from approximately $300 million (a conservative estimate) to $966 million (an estimate on the high end). Using those figures as low and high potentials, a reasonable estimate is that the U.S. government has spent over $500 million on the project since the September 11, 2001 terrorist attacks. Using annual data, this article suggests that the list costs taxpayers somewhere between $50 million and $161 million a year, with a reasonable compromise of those figures at approximately $100 million. Clearly the no-fly list is a program that is not without substantial cost. It represents, at least financially, a large part of the government’s protection of air travel. In order to begin to analyze whether or not the benefits are worth the costs, both must be identified and analyzed. It is that task to which the article will now turn.

METHODOLOGY

Source Material and Estimation Error

One likely reason for why a financial cost/benefit approach has not been conducted, at least in an unclassified manner, is that it is difficult to do. The biggest reason for the difficulty is that the government does not publish the aggregated costs of programs such as the no-fly list. As will be illustrated below, the no-fly list is a product of numerous government agencies and private sector involvement and thus represents a rather diffuse network of resources working together for common cause. This ensures that a variety of perspectives and sufficient technical expertise are aggregated into the program, but it also means that the no-fly list is not one program represented by a single line-item in a budget request. Rather, it is made up of pieces of multiple programs spanning public and private spheres, many of which are classified and unknown to the public.

The second reason why conducting a financial cost/benefit approach is difficult is that much of the information pertaining to the list is classified. Sources I spoke to between November 2007 and January 2008, who are close to the list, could only provide general feedback and guidance – anything remotely specific would fall under the classified domain. While this guidance was extremely useful, and constitutes one of my main methods of vetting the figures contained in this article, it meant that the data-gathering phase was done without much insight or help from those close to the program. Conducting a cost/benefit analysis when the details of the program are intentionally hidden from taxpayer view is challenging.

The approach taken in this article is to estimate the costs based on what is available and then have individuals close to the list, to the extent that they are able, validate that the estimates are reasonable (or, in some cases, too high or too low). As such, many of the estimates contained in this article are based on data culled from press reports, public interviews with government officials, Congressional testimony, and occasionally specific budget requests and reports. These estimates were then provided to individuals in the private sector security field who proffered limited, but extremely helpful, feedback.
One of the valuable criticisms of such an approach is that it is subject to much subjectivity. That is, choosing one number to represent an estimated cost requires the analyst to pick among many possible variations of cost and use that number to represent an aggregate cost. In anticipating this criticism, costs are estimated across three tiers: low, medium, and high. This is common practice in cost-benefit analyses as well as actuarial assessments and estimations. The low tier represents a conservative estimate, the medium tier represents a reasonable estimation, and the high tier represents a possible estimation. It should be noted that the high tier is not simply an inflated cost that attempts to account for all possible permutations of cost. I have tried to keep even the highest tier within a reasonable range. In cases of a particularly high number of unknown variables, I have tried to err on the side of conservative estimation so as not to inflate the costs due to extreme estimation error. A consequence of this move is that if there is estimation error in this article, it is likely to be biased towards the more conservative tier.

**Choosing a Cost-Benefit Framework**

There are a number of cost-benefit frameworks available to social science scholars. Many are derived from economics and focus on largely tangible (typically monetary) costs and benefits. The difficulty with choosing a framework for this article is that we are dealing with explicit financial costs but both tangible and intangible benefits. That is, we can estimate what the monetary costs of the system are, but in comparing them to the benefits we have both monetary benefits (such as the future realized value of preventing a plane crash) and intangible benefits (such as the ability to monitor potentially dangerous individuals). The two are alike in that they both benefit the U.S. government and citizenry, but unlike in that one can be measured in dollar terms and the other can not. Nevertheless, as Arrow and others argue, in such cases where cost and benefits are assessed in different terms (value in money vs. value in social policy), cost/benefit analyses can still be helpful, and indeed, should be mandatory if not binding.

The Office of Management and Budget, in realizing the importance and difficulty in assessing government policies, has published its own recommended framework for conducting cost/benefit analysis. It is useful for our purpose because it explicitly addresses this problem of tangible and intangible benefits:

> Both intangible and tangible benefits and costs should be recognized. The relevant cost concept is broader than private-sector production and compliance costs or government cash expenditures. Costs should reflect the opportunity cost of any resources used, measured by the return to those resources in their most productive application elsewhere.

Thus, the OMB framework serves as the main methodological framework for this article as it explicitly addresses governmental policy, on the one hand, and intangible as well as tangible costs and benefits on the other.

**Defining Terms**

Finally, before conducting an analysis of the costs of the no-fly list program, it is important to define precisely what it is that is being investigated. The no-fly list is essentially a “watch list” that prevents watched individuals from flying on commercial
aircraft. The list itself dates back to the 1980s in a very limited fashion (on September 11, 2001 only sixteen names were on the list). After the 9/11 attacks the number of the names on the list grew tremendously, with some reports suggesting that the list grew to 755,000+. It is now believed that the list contains roughly 40,000 names after a sustained effort to reduce the list to “key” individuals by scrubbing it of duplicates, reasonably certain safe flyers (such as U.S. Senators), and the like. While the government does not publish how names are put on the list, the public record suggests that the names are compiled from classified evidence conducted by a variety of government agencies. While the Transportation Security Administration (TSA) maintains the list, various agencies (see below) have input into it. It is important to note also that in popular speech the “no-fly list” is often equated with the “selectee list.” The two should be disaggregated. The selectee list is the Secondary Security Screening Selection that randomly selects passengers for additional screening and inspection. These individuals are allowed to fly after they have been cleared through security. Individuals on the “no-fly list” are not allowed to fly until they are cleared from the list and this requires more than a simple x-ray and body search. This article is interested in the costs of the no-fly list in particular, but future work should include an analysis of the selectee list as well.

The broad mechanics of the list have been made available for public consumption. The government sends an updated version of the list to airlines on a regular basis. It is the responsibility of the airlines to check passenger names against the list. It has been noted that TSA has long had plans to take on some of the responsibility of name-checking (particularly of names that are too sensitive to be sent to the airlines), first through the Computer Assisted Passenger Pre-screening System (CAPPS II) program and now through a similar program entitled “Secure Flight.” Development of this system has been delayed and it is unknown when it will be operational. Finally, the government is also developing a program entitled “Registered Traveler,” a public/private partnership between TSA and the Registered Traveler Interoperability Consortium (RTIC), which allows those individuals who pose a minimum security risk to submit themselves to background checks and subsequently submit to an easier and more streamlined airport security checkpoint experience. Having outlined the key aspects of the no-fly list, the article will now turn to estimating the costs of creating, maintaining, and dealing with the consequences of the list itself.

**ESTIMATING NO-FLY LIST COSTS**

**Establishing a Federal Government Resource Burn Rate**

A burn rate, or the cost of a given policy/program in terms of (1) the number of individuals involved, (2) their billing rate, and (3) the number of hours devoted to the project, is a useful way of estimating costs over time. Government agencies require potential contracting firms to provide an estimated burn rate in their response to proposals, and the OMB notes in their literature on conducting cost-benefit analyses the importance of identifying incremental costs over time. Calculating a burn rate for the no-fly list relies on estimating the number of individuals involved in the day-to-day operations of the list, those responsible for dealing with the consequences and ancillary effects of the list, and their respective billing rates. These individuals are
drawn from both the government and private sectors and constitute no-fly list resources.

Estimating the number of individuals associated with the list is difficult because there is no one central agency or contracting firm responsible for its implementation. Sources in the security community and government documents from the U.S. GAO note that there are individuals drawn from over ten government agencies and multiple private firms.\textsuperscript{22} The non-exhaustive list includes: the Department of Homeland Security (DHS), Transportation Security Administration (TSA), National Security Agency (NSA), Federal Bureau of Investigation (FBI), National Crime Information Center (NCIC), Defense Advanced Research Projects Agency (DARPA), National Counterterrorism Center (NCTC), Customs and Border Protection (CBP), Central Intelligence Agency (CIA), and various private government contracting firms such as Acxiom Corporation.\textsuperscript{23}

Given the broad scope of involvement and complexity of integrating the efforts among the various entities listed above, security professionals estimate that it is likely the number of individuals working on the list on a full-time basis is \textit{at least} 250, with another 500 involved in some capacity on a partial-time basis. This represents the conservative or low estimate. Individuals I spoke with at various government contracting firms note that mid-range figures are likely in the 500 full/1000 partial range, with some estimating that the numbers could exceed 1000 full/1500 partial.

Having estimated the number of individuals involved with the list, the next step is calculating their billing rate and amount of time devoted to the project. Turning to rates first, the U.S. Office of Personnel Management (OPM) provides a yearly salary scale ranging from approximately $17,000 to $124,000.\textsuperscript{24} A conservative figure that estimates the cost of government employee benefits is approximately 50 percent (Cox & Brunelli, 1994).\textsuperscript{25} That is, if the salary of a federal employee is $50k/year, the adjusted cost to taxpayers, inclusive of benefits, is approximately $75k/year. Sources in the security community note that among federal employees working on the no-fly list, there are very few at the lower ends of the pay scale, with most falling somewhere in the top third. On the private side, government contracting firms typically bill out their resources somewhere in the $100k-$500k/year range. This number varies depending on the expertise of the contractor, the profit margin of the firm, the type of work being conducted, etc. For the purposes of this article, it is worth using a conservative blended billing rate precisely because there are a large number of factors that lead to billing rate fluctuation. A conservative figure of $100k/year, inclusive of both government employees with benefits and private firm contractors, is a reasonable estimate, but is potentially much higher and not likely to be much lower.

Finally, not all employees mentioned above spend their full-time working on the no-fly list. The nature of the list suggests that there are likely a large number of individuals who do spend most of their time devoted to it, either in creating technology programs to support it, dealing with name removal requests, etc. There are a larger number of individuals, however, who work on the list part-time as needs arise. The FBI, TSA, and DHS, for instance, often collaborate on suspected individuals in order to determine whether or not they should be placed on the list. This type of activity does not consume an employee's entire day, but does require time and effort. Consequently, part-time no-fly list employees can spend varied amounts of their day working on various list...
activities. In order to estimate this amount of work, gradations of time spent on the list will increase as estimates of low/medium/high increase. At the conservative end, it is estimated that partial-time employees spend 25 percent of their time working on the no-fly list; the medium range figure is 50 percent and the high range figure 75 percent. This estimate allows considerable variation in the amount of time required of resources and seems reasonable among the security professionals that have reviewed the numbers.

Having identified the major components of the burn rate and estimated their value, a simple calculation yields burn rate figures for the low, medium, and high estimates. At the conservative end, the burn rate is estimated to be $7.5 million per year. The middle-range figure is estimated to be $20 million per year and the upper-range figure at least $43 million a year. Importantly, these figures only represent the personnel burn rate. They do not include other costs, such as technology systems, costs to non-government employees or costs to the private sector. It is to those costs that we now turn.

**Technology Product Costs**

The no-fly list operates both as a database of names and a system for ensuring that those named individuals do not board airplanes. The first component, the database, is maintained by DHS and TSA. The second component, the method of cross-checking passengers with the database, is maintained by the individual airlines. The government supplies the watch list to the air carrier whose automated information technology (IT) systems screen passengers. According to the GAO, 99 percent of all passengers on domestic flights are screened through the use of these computer systems; the other remaining 1 percent of passengers are “manually screened” because the airlines do not have an automated system. Finally, for international flights, air carriers are required to provide a list of passengers to Customs and Border Protection before take-off.

These two components can be disaggregated and their costs estimated individually. On the government side, the Associated Press in 2006 reported that the TSA had spent more than $200 million on three aspects of the no-fly list: Transportation Worker Identity Credential (a program for allowing “safe” individuals access to secure port areas), Secure Flight, and the Registered Traveler Program (a program that allows individuals to submit themselves to background checks in order to receive less thorough screenings at airports). Once Secure Flight was suspended, in February 2006, Leslie Miller of the Associated Press reported that the total cost of the program was $200 million. Estimating the cost of the government side of the equation then is relatively straightforward. The $200 million in investment of Secure Flight since 2002 presumably includes human resources as well as the technology product, so the cost must be discounted slightly. A conservative estimate of the government’s technology costs for this program is $150 million. A mid-range estimate is $200 million, the quoted cost according to the Associated Press. Finally, an upper-range figure is $250 million which would include any updates and new developments since the AP’s story broke in early 2006.

The airline technology products used to cross-check passenger names with the government-supplied no-fly list is more difficult to estimate because the air carriers...
have not published their compliance costs. Steven Lott of Aviation Daily, a trade journal for the airline industry, notes that as of July 2006 there was no uniform way for airlines to transmit their passenger lists to CBP, which accounts for the numerous in-air diversions and delays (to be discussed below) caused by airlines transmitting passenger lists after takeoff. In order to correct this problem, DHS has asked the airlines to adopt one of two systems. The first would have airlines transmit passenger information individually when each passenger checks into the flight, up to fifteen minutes before departure. Lott estimates the cost of this system to be $189 million in the first year and more than $600 million through 2015. The other solution, called APIS 60, is similar to the current system of sending passenger lists in bulk, but would cost more money to implement as a standardized process. It would require all passenger information to be sent to the government sixty minutes before plane departure. This would likely have an effect on check-in times, requiring passengers to be checked into their flights early in order to provide the sixty-minute window for name processing. Lott estimates $250 million in the first year for this and up to $1.9 billion over the next ten years. On August 9, 2007, DHS announced that the two options had been adopted as a rule and airlines would have to begin procedures to comply. These figures, as part of Lott’s analysis, help us to understand the potential costs associated with compliance, but they also provide a benchmark to estimate current costs. Lott notes that APIS 60 is similar to what airlines currently do, but is more expensive. Given that the more expensive, standardized version is $250 million – for the first year alone – a very conservative estimate for what it has cost the airlines to comply with no-fly list passenger screening to date is likely something well above $50 million. A middle range estimate of $100 million seems more likely, given the six years that have elapsed since 9/11 and the need to get systems up and running quickly across the industry. An upper range figure of $250 million would assume that the one-year cost of setting up this new system, while higher than the current system, is roughly equivalent to six years of running a less costly system.

False Positives

One of the recognized problems with the no-fly list is that, until very recently, the list was exceedingly large and false positives were quite common. In the last few years, stories of Senator Ted Kennedy and a host of other non-terrorist individuals being flagged by the no-fly list and not allowed to fly have appeared in the local and national news. The reason for this is largely because the no-fly list does not list individuals; it lists names, which can lead to the misidentification of individuals. This is most clearly seen in dealing with Arabic names that have a number of English transliterations: in many cases, multiple derivatives of a name are put on the list in hopes of matching a particular individual. The American Civil Liberties Union (ACLU), in attempting to prevent the high number of false positives and attacks on civil liberties, sued TSA and the FBI in April 2003 on behalf of Rebecca Gordon and Jan Adams, two individuals who were not allowed to fly because their names appeared on the no-fly list. TSA and DHS eventually settled for $200,000 in damages and attorney fees. An additional outcome of the case, however, was that it brought into court many previously hidden documents about the inner-workings of the list. One of these documents noted that, in November 2005, TSA indicated that 30,000 people in the previous year alone (from
2004 to 2005) had contacted the agency to have their names removed from the list.\textsuperscript{38} This suggests that, at least until 2005, roughly 30,000 individuals \textit{a year} had been identified as false positives. As the ACLU complaint points out, the only way that one can find out if one is on the no-fly list (other than filing a lawsuit to bring the records into court) is to attempt to fly.\textsuperscript{39} If one is on the list and attempts to fly, he/she is stopped at the airport by local law enforcement and airport security. Having identified how many false positives there are in a given year, we can begin to make sense of the associated costs.

Estimating the cost of these false positives involves a number of disparate activities: the cost of the passenger being detained at the airport and missing his/her flight; the cost of airport security/personnel detaining the passenger; if a false positive, the cost of arriving at the airport early each time one flies to allow time to be cleared; the cost of \textit{not flying} in order to avoid the hassle; and the cost of attempting to get off of the list once one has been identified as a false positive. Before estimating these costs, however, a burn rate for passenger time needs to be established. Similar to the burn rate conducted above for government resources, a similar rate is needed for passengers since their time is valuable as well.

Unlike the difficulty in assessing governmental resource burn rates, doing so for airline passengers is relatively straightforward as the airlines themselves have devoted many research resources evaluating the costs of delays. One estimate is that, on average, airline passenger time can be valued at approximately $50/hour.\textsuperscript{40} With this rate established, we can estimate cost by examining how long each false positive requires of an individual. With respect to the time spent being detained by the local authorities, it is difficult to account for the significant variability in experience. Some individuals report being held for hours in airport back rooms while others are able to leave relatively quickly.\textsuperscript{41} If we assume, for a very conservative figure, an average of two hours dealing with airport security, then we can begin to estimate cost. 30,000 passengers a year who are identified as false positives and spend on average two hours dealing with this hassle, translates to roughly $3 million a year. If we assume, however, that there are fewer false positives now that the list has been scrubbed over the last year, we can discount the yearly figure to roughly $2 million a year. A middle range figure would account for a longer experience in dealing with the false positive because a two hour delay with airport security would undoubtedly mean a missed flight and presumably increased cost. Assuming a longer period of five hours dealing with this problem extrapolates to $7.5 million a year. Finally, a higher range figure of ten hours dealing with each false positive – from the passenger’s perspective – is possible, given the added expense and hassle of missed flights, being forced to fly the next day, etc. Such a figure results in a cost of $15 million a year.

In addition to costs from the passenger perspective, there are also airport/local law enforcement costs in dealing with false positives. When a name is flagged on the no-fly list, local airport security is called in order to detain the passenger in question.\textsuperscript{42} There are approximately 450 commercial airports in the United States, plus approximately 200 international airports with flights bound for the U.S. that would all have local law enforcement in place to deal with false positives on an “as-needed” basis. We can estimate this cost by assuming a standard airport security salary of $35,000/year on the conservative end, plus security officials working on no-fly related issues, including
false positives, on a part-time (25%) basis. This equates to approximately $5.5 million a year in no-fly list associated costs for the use of airport security personnel.

Finally, a large cost associated with false positives is passengers attempting to be removed from the list. One of the criticisms of DHS has been that if a passenger is placed on the no-fly list mistakenly, it can be a very laborious process getting off of the list. There are reports of individuals being asked to sign notarized copies of documents and letters, producing birth certificates, copies of passports, and – reportedly – even voter registration cards. There is a cost entailed in producing each of these documents, but the largest cost undoubtedly is the time required to gather the respective documents. DHS does not publish how many individuals attempt to be removed from the list each year, but given the known number of false positives, we can base cost estimates on that figure. If, for instance, 10 percent of the 30,000 individuals on the false positive list attempt to be removed from the list, and gathering the required documents takes approximately ten hours per individual, the cost translates to approximately $1.5 million/year. A less conservative estimate of the number of individuals attempting to be removed from the list is a quarter of this number, or 7,500. This translates to a cost of $3.75 million/year. Finally, if we estimate an upper-range figure of approximately 50% of the false positives pursuing the process of name removal, the cost is $7.5 million/year. Granted, there is undoubtedly fluctuation in these estimates because it is unclear whether or not the 30,000 false positives represent distinct individuals or some individuals being flagged more than once in a given year. This estimate, however, does provide an approximation of the cost at the three probability levels.

**Flight Diversions and Delays**

One of the ramifications of the no-fly list over the last several years has been the number of flight diversions and delays due to list operations. A KLM flight from Amsterdam to Mexico, on April 10, 2005, is a representative example. The plane was en route from Amsterdam to Mexico and was due to cross over U.S. airspace. The U.S. government ordered the plane to return to the Netherlands before reaching the United States because it said two of its passengers were barred from entering U.S. territory. The plane had been in the air for more than four hours before returning to Europe and caused 278 passengers delays of approximately twenty-four hours. The Washington Post reported, in July, 2005, that the two men removed from the flight were questioned but not arrested. In sum there have been seven total diversions, and presumably countless delays, due to no-fly list processing incidents that are not reported. The aim of this section is to assess the costs of these delays.

One of the better estimates of the cost of flight diversions comes from the medical community. Medical events constitute the major recurrent reason for flight diversions. From heart attacks to seizures, passengers routinely get sick on airplanes and the aircraft diverts to a close airport in order to seek medical attention for the sick individual. A study of neurological sickness diversions estimates that the cost of each diversion is somewhere between $15,000 and $893,000, depending on the route (international vs. domestic), the length of the delay, whether or not fuel must be dumped to achieve optimal weight before landing, etc. For our purposes a reasonable range for the cost of diversions is likely $500,000-$893,000, as all seven known
diversions have been on international flights. Extrapolating a conservative figure of $500,000 per diversion, this results in a total cost of $3.5 million since 2002 ($500,000 x 7 diversions). A medium-range figure of $700,000 per diversion results in a cost of $4.9 million. Finally, at an upper limit of $893,000 per diversion, the total cost due to the no-fly list is roughly $6.25 million. As discussed above, these figures only represent actual diversions, instances where the plane was forced to land somewhere other than its intended destination. The figures do not include delays due to no-fly list processing, as that data is not published by the airline industry.

Other Costs

Finally, there are other costs associated with the no-fly list that will not be examined thoroughly here because assessing a financial figure for each of them is difficult. Lawsuits against U.S. government agencies, typically DHS, TSA and the FBI, with respect to no-fly list related issues (such as harassment) are numerous and presumably quite costly for both sides of the case. A recent search in the WestLaw database identified fourteen disparate case filings against the U.S. government regarding the no-fly list. One prominent case, filed by the ACLU, resulted in a settlement of $200,000 by TSA and DHS for the victims of unnecessary harassment and detention.47 It is unknown how many resources are spent responding to these cases, but the numbers are likely significant48 and a potentially fruitful area of further research.

ANALYSIS OF NO-FLY LIST BENEFITS

The government’s cost-benefit framework suggests that just as costs can be tangible (such as money spent on a particular product) and intangible (such as opportunity costs), so too can the benefits of a particular policy. Therefore in analyzing and assessing the benefits of the no-fly list, it is important to cover not only the financial returns, or tangible benefits to taxpayers, but more intangible benefits as well, such as the use of the list as a deterrent to committing terrorist acts with airliners. Arguably the intangibles of the no-fly list provide greater benefit, since the aim of the list is prevention and not necessarily a monetary return on investment. It is to those intangible benefits that we shall turn first.

Stopping/Deterring Potential Plots

If the no-fly list is successful in what it aims to do, the largest benefit to the country is stopping potential plots that are in the works by not allowing dangerous individuals to board airplanes and commit terrorist attacks on/with the aircraft. The argument is straightforward: if the current implementation of the no-fly list existed on September 11, 2001 and the would-be hijackers were on the list, it would have been impossible for them to fly. This is the argument that is made by Kip Hawley, TSA Administrator. In an interview with Bruce Schneier, Hawley noted that the no-fly list is worthwhile “because it works.” Hawley further pointed out that “[TSA does] not publicize how often the no-fly system stops people you would not want on your flight. Several times a week would low-ball it.”49 Two questions immediately arise from these comments: is it true that the no-fly system works in preventing would-be terrorists from boarding airplanes, and, what is to be made of the claim that “several” potentially dangerous individuals are prevented from boarding airplanes a week?
The problem with the first claim, that the no-fly system works, is that it is relatively easy to bypass the system with a little ingenuity. For instance, the no-fly list’s core mechanism is a matching a name to photograph identification. As noted above, the process is for a passenger’s name to be cross-checked against the list and then verified as the name matching the individual by checking photo identification. This process assumes a number of key points. First, an assumption is made that the ticket was purchased using the passenger’s real name. If a would-be terrorist knows that he or she is on the no-fly list, the next logical step would be to purchase the ticket under an assumed name that is not on the list. Second, the process also assumes that the photo ID is real and represents the true identity of the individual in question. It would be relatively easy, for instance, for someone to make a reservation under an assumed name and either manufacture an ID or use the real identification of the assumed individual. Third, this process is made easier by the increase in “print-at-home” boarding passes, which are easy to forge and allow would-be terrorists to put any name they like on the boarding pass. These three aspects of the no-fly list make it simple for an individual to purchase a ticket under someone else’s name, use a real ID to enter the boarding terminal with a forged boarding pass, and then fly on the ticket that has someone else’s name. Some security experts have gone so far as to create a “fake boarding pass generator” on the Internet to illustrate how easy it is to forge a boarding pass. Importantly, this is not just a theoretical exercise. A CBS affiliate in Kansas City, in an undercover investigation, was able to enter the TSA secure area by producing a fake ID. The undercover individual was not stopped or asked any additional questions. Thus, if the no-fly list is stopping individuals who wish to commit terrorist attacks, those individuals have not employed all of the strategies that are at their disposal; this should raise questions as to whether or not the no-fly list achieves the benefits its administrators claim.

The second claim made of the no-fly list is that it does stop terrorist events, or at least dangerous individuals, on a routine basis; we do not hear about them because the government keeps that information close to the vest (except when questioned, such as in the Schneier interview). Three questions arise from this claim. First, why would the government want to keep such information secret? Perhaps more importantly, why does the empirical record of other terrorist prevention activities suggest that the government’s strategy is very often the opposite? It lets everyone know about potential activities before they are well formed. Finally, if what Hawley claims is true, are there many more potential terrorists in this country than is commonly believed (since they are being stopped several times a week) or is the no-fly list ineffective at stopping terrorists? Is it casting a much wider net and catching non-dangerous individuals as well?

With respect to publicizing no-fly list successes, it would seem that as a deterrent mechanism the government would want would-be terrorists to know that the no-fly list works; that it catches dangerous individuals, and therefore, it is not wise to try to fly if you have thoughts of committing a terrorist act. This is particularly true given the amount of information available on the Internet about how to bypass the no-fly list, such as the forged boarding pass generator. If the government wanted to counteract the effect of that type of information being available, it would seem reasonable to show the public that despite these apparent flaws, the no-fly list works well in stopping
dangerous individuals. A response to this argument is that there is greater benefit derived from keeping the successes of the list relatively secret because it keeps terrorists continually guessing and unsure about how effective the government is at tracking them and preventing their action. This argument might have some merit, but the empirical record of the government with respect to publicizing potential terrorist threats and foiled plots suggests that they do not subscribe to the secrecy strategy.

There are numerous examples of the government pursuing a strategy of publicity rather than secrecy when it involves letting the country know about terrorist plots and threats. Two examples, one from a small-scale potential attack and one from a large-scale potential attack, should illustrate the point. In June 2005, the U.S. government held a press conference in Lodi, California to make public a foiled terrorist plot that involved Hamid Hayat and his father Umer, who had allegedly had connections to Pakistani terrorist camps. The FBI chief of Sacramento said in the public statement that Al Qaeda was active in the Lodi, California area and it included “individuals who have received terrorist training abroad with the specific intent to initiate a terrorist attack in the United States.” The subsequent investigation and trial did not elucidate any specific intent, but rather revealed an individual who may or may not have been sympathetic to Islamic jihad. Nevertheless, in this case the government, without any direct knowledge of a specific threat or imminent attack, made public the information they had, thus belying the argument that secrecy over publicity is the preferred strategy of deterrence.

The second example is drawn from a much larger potential terrorist attack originating in the United Kingdom. From August 9 to August 10, 2006, British authorities arrested twenty-four suspects alleged to have been plotting an attack against the United States using U.S.-bound aircraft and liquid explosives. A day later Michael Chertoff, head of DHS, called the plan “sophisticated” and “imminent,” with the plan “getting really quite close to the execution phase” and “in the final stages of planning before execution.” The subsequent investigation of the plot revealed that the government had no solid evidence the plan was close to execution. Specific planes or a date had not been set, a number of the suspects did not have passports, and, perhaps most important, British authorities had been monitoring the group for months and were confident that an attack was not imminent. Nevertheless, as was the case with Hamid and Umer Hayat, the government came forth before all of the facts were available and noted that a potentially very serious threat had been thwarted.

These two examples of the government making public potential threats before they are imminent raises the question of why there is a disconnect between the no-fly list secrecy strategy, as verbalized by Hawley, and the publicity strategy pursued during other cases. It could be that the government makes the secrecy/publicity decision on a case-by-case basis and thought there was value in notifying the public of the first two threats, but not no-fly list threats. It is conceivable also that the government only wants to alert the public to specific threats. That is, someone being stopped at the airport because he/she might be dangerous can be conceived of as a threat, but it is a diffuse threat. There are no specific plans or intentions that are automatically divined by stopping someone from boarding an aircraft; the individual may or may not have had intentions of wrongdoing even though they were on the list. Yet the empirical reality seems to suggest that the government sees value in making anti-terror successes
public. Given the two examples above, one could reasonably come to the conclusion that if the no-fly list had stopped a significant threat, we would have heard about it.

The more confusing aspect of Hawley’s statement is that the no-fly list stops “several” individuals the government does not want flying a week. This would suggest that there are potentially would-be terrorists attempting to board aircraft on a routine basis. Empirically this is difficult to reconcile with the FBI’s own admission that they have found zero terrorist cells in the United States since 9/11, and Al Qaeda operatives seem to be focusing their energies on Iraq. Presumably, if these individuals who are being stopped are terrorists, the FBI’s statement would no longer be correct. If terrorists are prevalent enough to be boarding aircraft multiple times a week, then is it still reasonable to assert that zero terrorist cells have been found in the U.S.? Another explanation for the high-number of individuals being stopped is that they are on the list, but not necessarily terrorists. As noted above, even with the “scrubbing” that has occurred, the list is still quite long and it is not entirely clear that everyone on the list poses a threat to the US. Thus, while it might be true that the no-fly lists stops individuals on a routine basis, the extent to which those individuals posed a danger to the aircraft they were about to board remains in question.

Finally, with respect to stopping potential plots, the effectiveness of the no-fly list is questionable because of the unknown danger posed by those on the list. As Bruce Schneier points out, the no-fly list is “a list of people so dangerous they cannot be allowed to fly under any circumstance, yet so innocent we can’t arrest them even under the Patriot Act.” This is a real and important critique. If the individuals on the no-fly list are dangerous, and we have information to suggest that they are dangerous, why aren’t they arrested and at least brought in for questioning? Again, the empirical record suggests that the government’s approach when dealing with potential terrorists is to bring them into custody in order to figure out how real the threat is. This is what occurred with the Hayats and the would-be U.K. bombers. This remains an important question about the benefits of having the no-fly list: how dangerous are the individuals on the list? Presumably if they posed an immediate threat to the United States they would be arrested and the government would not wait for them to turn themselves in by attempting to fly. One response to this question is that a benefit of the no-fly list is not just in arresting individuals, but rather tracking their movements.

**Keeping Individuals In/Out**

One argument for the potential benefit of the no-fly list is that it allows the government to track and keep individuals inside the United States. If an individual is believed to have connections to terrorist training camps in Pakistan, there might be value in preventing that individual from going to Pakistan to be trained, aid in training, or otherwise conduct dangerous activities. The problem with this argument is that it is belied by actual law enforcement experience. Sources in the security community note that, in general terms, it is better to have dangerous individuals outside of the United States rather than inside. While the government might be able to keep better track of individuals within its borders, the individual’s ability to conduct terrorist activities against the U.S. is hampered if that person is residing outside its borders. From this perspective the no-fly list does not provide substantial benefit by keeping individuals in the country, since it is preferable to keep terrorists out, not keep them in.
corollary to this argument is that keeping terrorists out of the country is beneficial. A no-fly list, operationalized in international airports with flights bound for the U.S., might help to keep dangerous individuals from reaching U.S. soil.

Further, even if those on the no-fly list do not pose an immediate and credible threat to the U.S., there might be value in the government’s ability to keep track of potentially harmful individuals. For instance, if there are individuals living in Western Europe who are believed to harbor resentment against Western society, there is value in the United States being notified of their movement and intent. If one of these individuals arrives at an international airport attempting to board a flight to the United States, the threat may not be specific to that particular flight or any particular plot against the country of departure, but nevertheless information about the movement of individuals on the list is worthwhile. High-level government officials and security experts routinely discuss the merits of layered-based security. By building and maintaining movement information on suspected individuals, the government is able to derive an additional knowledge-based layer of security. This would seemingly serve a real benefit in the government’s campaign to better know and understand the enemy.

**Psychological Benefits of Security**

Finally, as alluded to earlier, some analysts have argued that the no-fly list and other aspects of airport/flying security provide an intangible psychological benefit. Bruce Schneier has termed this concept “security theatre.” Schneier argues that security countermeasures utilized by the government after September 11 have been intended to provide the feeling or perception of improved security, without doing anything to actually improve tangible security. Given the criticisms that have been levied at the no-fly list’s effectiveness, particularly as it relates to the rise of print-at-home boarding passes and the ability to use fake IDs, etc., the no-fly list is, according to Schneier, an excellent example of security theatre.

From a psychological perspective it may be that security theatre serves a legitimate function in what scholars have called “ontological security.” Ontological security is a mental state derived from the feeling of continuity and stableness in one’s life. Just as humans require physical security with our bodies, so too do we require that our day-to-day existence not be scarred by outlying events. It is possible to conceive of security theatre as a mechanism for providing ontological security to flyers and the general public. If individuals are convinced by the security they see that they are safe, they might be more likely to feel protected and go about their business than if their ontological security is threatened.

Further, security theatre can also theoretically deter actors from taking certain risks. If, for instance, would-be terrorists perceive significant security measures in place, they might be less likely to follow-through with terrorist acts. In this example the security need not be “real” in any meaningful sense; it must only present a feeling of a securitized situation that would create a level of risk for a would-be terrorist. Retail stores have long adopted this stance, using such things as fake video cameras to dissuade shop-lifting, for instance.

This is not to say, however, that security theatre provides only positive psychological effect. As Schneier argues, security theatre can lead to increased perception of risk. Consider, for instance, visible measures of security such as armed guards.
might reassure the public, from an ontological security perspective, it might contribute to a sense that there is a real risk associated with the activity they are engaged in. With respect to the no-fly list this might obtain from the existence and public knowledge of the list itself; given that there are individuals the government does not want on airplanes, this might imply that flying is a risky endeavor.

**Tangible Benefit: Preventing a Costly Attack?**

Having identified many of the potential intangible benefits of the no-fly list that are difficult to assess financial value to (such as the ability to track suspected individuals and deter potential attacks) it is worth considering what tangible benefit the list might serve if it is effective. There are a number of reasons to question whether or not the no-fly list is able to deliver on the intangible benefits, as outlined above, but assuming that it can, what tangible savings might the country realize?

One way to assess the tangible benefits of preventing an attack is to estimate what it would cost the country if the no-fly list was not in place and terrorists were able to easily board an aircraft and bring it down. While this represents a scenario that is less likely to occur since September 11, 2001, as airline security has increased, it is nevertheless worth investigating as a middle-range possibility in terms of cost. The RAND Corporation, in a 2005 paper investigating the cost and benefits of aircraft missile defense systems, estimated that the direct costs of an airliner being attacked in flight would approach $1 billion. The indirect costs, which are more difficult to estimate because predicting state response to the attack is difficult (such as whether or not air travel would be shut down for a significant period of time as it was after 9/11), are estimated at close to $15 billion when all potential long-term effects are accounted for. This number would, of course, increase substantially if more than one aircraft was involved in an attack. While the tangible cost of a potential airliner attack is useful in its own right in providing a sense of what type of benefit the no-fly list might provide, it can only be evaluated fully by assigning a probability to the attack, computing the probable tangible cost of the attack, and comparing that figure to the cost of maintaining the list. It is to that final task that the article now turns.

**BRINGING COSTS AND BENEFITS TOGETHER: CONCLUDING THOUGHTS**

Assessing whether or not the no-fly list is valuable or “worth” the money being spent is a difficult endeavor because ultimately it is a subjective one without a clear and objective answer. By way of conclusion, however, the article will end with a question in hopes that it will spur additional research and discussion on the topic. Comparing the intangible benefits to costs is difficult because a quantitative approach is not sufficient; assigning a financial figure to intangibles is difficult, and any qualitative approach would necessarily be muddied by subjective arguments about the relative merits of the intangibles. For instance, some might find high value in the government’s ability to monitor and track individuals, while others see this as an ancillary, or indeed (if it infringes on the civil liberties and rights of those being monitored) negative “benefit.” Tangible benefits are seemingly easier to compare to costs because we can attach a financial figure to each benefit, but the probability of realizing those benefits is quite subjective. To answer any question regarding the worthiness of the no-fly list the first
question that must be answered is: how likely is it that there will be an attack attempt? The answer to this question is inherently subjective depending on one’s own sense of security, how one perceives world events, and how closely one pays attention to world politics. Recent polls demonstrate this subjectivity by illustrating the diversity of opinion as to whether or not Americans are likely to witness another terrorist attack in the near future.\textsuperscript{71}

Nevertheless, with tangible benefits we at least can compare the realized return to the costs of implementation across a range of probabilities. A common methodology for assessing cost effectiveness is to multiply the costs of an event by the probability that event will happen and then compare that to the costs of a system in place to prevent the attack from occurring. For instance, if one perceives a 1 percent chance of individuals boarding a plane and bringing it down each year, with the costs of such an attack reaching $15 billion, per the RAND study cited above, then one theoretically could argue that $150 million (0.01 * $15,000,000,000) should be spent, each year, in attempting to prevent such an attack. Similarly, if one considers the probability of an attack to be 0.1 percent, then one could argue that the no-fly list is “worth” $15 million in prevention of such an attack. Given the costs identified in this article, a first-cut reasonable estimate of the probability of an attack needed to justify the cost of the no-fly system is somewhere between \textasciitilde 0.3\% and 1.1\%. It is important to note, however, that this analysis is true only if the no-fly list alone could stop the attack.

More likely, the no-fly list reduces the likelihood of an attack by adding another layer of security to air travel. How much value it provides in reducing the likelihood of attack is a subjective measure that relies on the probabilities assessed by the analyst. Clearly assessing the probability of attack is difficult. From there assessing what role the no-fly list would play in a “non-event” is even more so. Precisely because the no-fly list serves as a deterrent, success is defined not by what happens but what does not happen. This makes analysis of whether the no-fly list is “worth it” a subjective call. Making that call, however, requires data of the type presented in this article.

On the other hand, there have been recent attempts to quantitatively value human life and compare the costs of saving those lives to the cost of losing them.\textsuperscript{72} Mark Stewart and John Mueller, in looking at the cost and benefits of hardening cockpit doors and the air marshal program in Australia, use a quantitative approach on both the cost and benefit end. They note that if human life is calculated to be between $1 and $10 million, based on Australian government guidelines, then the cost of the cockpit door hardening is less than the expected benefit in terms of historical fatality numbers and the risk associated with terrorists entering cockpits. Using the same calculation, the air marshal program fails. They note that even if their estimates are in error by 100 percent, it would not change the conclusions with respect to the program. Similar calculations, using the data provided in this article, could be used in answering the “is it worth it” question.

Such attempts at quantitatively assessing the value of human life will likely cause some to pause. Should we be placing monetary value on human life or if security measures have the potential of saving even one life, should we pursue them? These are not easy philosophical questions to answer. However, conducting analyses of the costs and benefits of security measures do allow us to understand where resources are going and what they might be preventing. We can then compare these expenditures to the
potential of using the resources elsewhere, perhaps in vaccinations, health programs, road safety, etc., which can also be used productively to save lives. The goal of this article is not to make this assessment but rather to provide some tools and data such that a conversation can begin with respect to where our security dollars should be spent. It is hoped that the investigation this article has taken, of the costs and benefits of the no-fly list, will spur additional work in attempting to elucidate educated relative probabilities of various no-fly list-related scenarios. It is only then that the cost-effectiveness, and the financial worth of the list, can be thoroughly assessed.

Marcus Holmes is a PhD candidate in political science at Ohio State University. His research interests are in international relations and political psychology with particular emphasis on social neuroscientific insights into politics. Mr. Holmes can be contacted at holmes.504@osu.edu.

The author would like to thank John Mueller, Dale D. Murphy, Mark Stewart, Nathan Stickney, a large number of sources in the private sector, and three anonymous reviewers. All mistakes remain mine.

NOTICE OF CORRECTION: This article was corrected and republished on February 13, 2009 to reflect the following changes: (1) addition of section entitled “Psychological Benefits of Security,” (2) new text in the Conclusion, and (3) author’s acknowledgment. These changes were made to correct an editorial oversight on the part of Homeland Security Affairs.
## Appendix A – Consolidated Table of No-Fly List Costs

<table>
<thead>
<tr>
<th>Players/Costs</th>
<th>Low Estimate</th>
<th>Medium Estimate</th>
<th>High Estimate</th>
</tr>
</thead>
<tbody>
<tr>
<td>DHS, TSA, NCIC, NSA, DARPA, FBI, CIFA, Private Firms, etc. Burn Rate</td>
<td>$7.5 million/year</td>
<td>$20 million/year</td>
<td>$43+ million/year</td>
</tr>
<tr>
<td>Government Technology Products</td>
<td>$25 million/year</td>
<td>$33 million/year</td>
<td>$42+ million/year</td>
</tr>
<tr>
<td>Airline Technology Products</td>
<td>$8.3 million/year</td>
<td>$17 million/year</td>
<td>$42+ million/year</td>
</tr>
<tr>
<td>Law Enforcement Involvement (Airport Security)</td>
<td>$5.5 million/year</td>
<td>$5.5 million/year</td>
<td>$5.5+ million/year</td>
</tr>
<tr>
<td>Passenger False Positive Airport Time</td>
<td>$2 million/year</td>
<td>$7.5 million/year</td>
<td>$15+ million/year</td>
</tr>
<tr>
<td>Passenger Removal From List Costs</td>
<td>$1.5 million/year</td>
<td>$3.75 million/year</td>
<td>$7.5+ million/year</td>
</tr>
<tr>
<td>Airline Diversion Costs (Airlines and Passenger Delay Costs)</td>
<td>$0.4 million/year</td>
<td>$0.66 million/year</td>
<td>$1+ million/year</td>
</tr>
<tr>
<td>Lawsuits Against US Government</td>
<td>$1 million/year</td>
<td>$2 million/year</td>
<td>$5+ million/year</td>
</tr>
<tr>
<td><strong>Total Yearly Cost</strong></td>
<td>~$51 million</td>
<td>~$89 million</td>
<td>~$161 million</td>
</tr>
<tr>
<td><strong>Total Since 9/11/01</strong></td>
<td>~$300 million</td>
<td>~$536 million</td>
<td>~$966 million</td>
</tr>
</tbody>
</table>


For a frame of reference, the Transportation Security Administration’s budget in 2007 was $4.7 billion (Public Law 109-295).

It is possible that a financial analysis of the no-fly list has been conducted by government officials, but such an analysis is not available to the public. If this is the case, it is unclear as to why it should not be available. While clearly operational information, such as on what servers the list resides on, for instance, might constitute sensitive information, the costs of such operation should not be sensitive. There is no a priori reason why the costs of such a program should be classified.


This is not to say that there are not substantial intangible costs as well. These have been dealt with elsewhere. The focus of this article is on strictly tangible costs.

The Arrow et al argument is made with respect to environmental, health and safety regulation in particular. Kenneth Arrow and others, “Is There a Role for Benefit-Cost Analysis in Environmental, Health and Safety Regulation?” Science 272, no. 5259 (1996).


CBS News, “Unlikely Terrorists on No Fly List.”


Ibid.

Ibid.

Florence, “Making the No Fly List.”

An aggregated table of costs is provided in Appendix A.

See, for example, a sample Request for Proposal (RFP) to contractors as issued by the Internal Revenue Service (IRS): http://www.irs.gov/pub/irs-procure/tirn007r00013rfp.doc.


See for example GAO, Aviation Security, and GAO, Terrorist Watch List Screening.


26 These calculations can be represented in the following equations, based on the burn rates calculated above.

Low = 250 full time * $100,000 + 500 partial time * $100,000 * 0.25.

Medium = 500 full time * $100,000 + 1000 partial time * $100,000 * 0.50.

High = 1000 full time * $100,000 + 1500 partial time * $100,000 * 0.75.

27 I am including overhead such as benefits for the government employees since such information is readily available by agencies such as the Bureau of Labor Statistics. I am not including overhead for private sector employees as that data is not publicly available and would vary considerably depending on the firm.

28 GAO, Aviation Security.

29 Ibid.

30 Ibid.


36 Susan Trenton and Joseph Trenton, Unsafe at Any Altitude (Hanover, NH: Steerforth Press, 2006).


40 This figure likely increases over time with inflation, but for the purposes of this article, it will suffice. Philip Lederer and Ramakrishnan Nambimadom, “Airline Network Design,” Operations Research 36, no. 6 (November/December 1998): 785-804.

41 Complaint at paragraphs 21-26, Green v. Transportation Security Administration, 351 F. Supp. 2d. 1119 (W.D.Wash. 2005)(No. CV 04-0763)

42 Complaint at Green v. Transportation Security Administration, 351 F. Supp. 2d. 1119 (W.D.Wash. 2005)(No. CV 04-0763)


44 These calculations can be represented in the following equations, based on the value of passenger time described above ($50/hour).
Low = 30,000(0.10) * (50)(10)
Medium = 30,000(0.25) * (50)(10)
High = 30,000(0.50) * (50)(10)

46 Joseph Sirven and others, “Is there a Neurologist on This Flight?” Neurology 58, no. 12 (2002): 1739-44.
48 One study noted that in the state of Florida, 336 frivolous lawsuits filed between 2004 and 2005 cost taxpayers roughly $16 million. “Frivolous Lawsuits Cost Taxpayers Millions,” WESH Orlando, February 20, 2006. This translates into approximately $50,000 per case. Given that frivolous lawsuits likely result in significantly less governmental resource time than lawsuits over the no-fly list, it is reasonable to estimate that the government spends millions in responding to no-fly list related lawsuits.
49 Schneier, “Conversation with Kip Hawley.”
50 GAO, Aviation Security.
55 Ibid.
60 Schneier, “Conversation with Kip Hawley.”
61 The US Attorney for the Eastern District of California, McGregor W. Scott makes this point as well with respect to the Hamid and Umer Hayat plot (PBS, 2006).
An upper range estimate might include a scenario with multiple planes being compromised or a plane being used a missile similar to September 11, 2001. A lower range estimate might include a scenario where a plane is not brought down, but rather individuals on the plane murder passengers or hijack it to another location for ransom purposes.


Competing with Intelligence: New Directions in China’s Quest for Intangible Property and Implications for Homeland Security

Robert Slate

INTRODUCTION

Some enterprises do not hesitate to use illegal means to collect intelligence from their competitors, making trade secret protection increasingly challenging and urgent.

—China Business Training Course on Competitive Intelligence Practices
Shanghai, Oct. 17-18, 2008

Chinese executives’ intense desire to succeed globally, combined with the Chinese government’s encouragement and support, has driven some companies to develop corporate competitive intelligence (CI) programs that increasingly rely on illegal human and technical intelligence collection methods to acquire intangible property from U.S. companies and government agencies. The plethora of industrial espionage cases involving Chinese companies in recent years reveals extensive Chinese government involvement in such activity and the role of CI in facilitating the transfer of U.S. proprietary technology from civilian to military uses. Against this backdrop, the United States faces a rising national security threat from Chinese corporations that employ robust CI programs to enhance illegal company- or government-directed espionage and intellectual property (IP) theft and infringement. The complicated and global character of this phenomenon requires that the U.S. government rethink the traditional intelligence community (IC) approach to collection and analysis of intelligence on China and the implications for homeland security.

This article draws upon a body of Chinese literature on CI to explore the role of CI in helping China to conduct industrial espionage and acquire U.S. IP and illustrate how the study of Chinese CI can help the U.S. government and business make sense of future trends in Chinese industrial espionage. Chinese CI theory and practice is pushing Chinese intelligence in new directions; however, this trend has gone relatively unnoticed in the U.S. intelligence and academic communities, probably because CI is largely viewed as the domain of private sector and professional organizations in the United States. Despite Chinese corporations’ growing reliance on CI, and the significant role it has played in corporate successes, many U.S. companies remain relatively unfamiliar with the state of Chinese corporate intelligence and the evolving risks for U.S. corporations.

INTANGIBLE THREAT

The 17th Century French missionary Louis Le Comte wrote in his memoirs that trade and commerce “is the soul of the (Chinese) people” and “the primum mobile of all their actions.” China’s trade and commercial genius has certainly played a major role in the
spectacular rise of China’s economy and its integration with the U.S. economy over the last several decades. Some observers view China’s growing stake in America’s economic system as an extremely positive development for the United States, while others see Beijing as a military, economic, and technological threat. Most would probably agree, however, that China’s growing economic power and massive annual trade surplus with the United States – $250 billion and growing – puts China in a position to affect the United States economy in ways considered improbable in the past.

Chinese firms’ increasing involvement in corporate spying and IP theft in America raises the stakes of the trade deficit problem with China and is the source of a great deal of concern for U.S. homeland security. Chinese corporations that use IP theft and infringement as components of their overall business model, and effectively employ corporate intelligence programs to that end, are damaging the foundations of the American corporate world: intangible property.

Most of the value in corporations, particularly in America, remains in intangible property. The term “intangible property” is generally used to refer to the following non-physical assets, such as intellectual property (e.g., patents, copyrights, trademarks, and trade secrets), legal rights (e.g., leases, contracts, and licenses), relationships (e.g., supply and custom distribution chains) and brands. According to a 2006 Brand Finance report in 2006, 62 percent of the value of corporations around the globe is based on intangibles ($19.5 trillion of global market value). U.S. corporations have 75 percent of their value tied up in intangibles. Not surprisingly, intangible property accounts for 98 percent of the U.S. technology sector.

Intellectual property receives a lot of attention because its misappropriation can devastate companies, especially those in IP industries, and can have a disproportionate impact on countries like the United States, where IP factors so prominently in the overall economy. U.S. IP industries, for example, have been responsible for approximately 40 percent of the total growth of the U.S. economy. The International Intellectual Property Alliance (IIPA) released an economic study in 2007 that assessed U.S. copyright industries (e.g., entertainment software, motion picture, business software, and recording) as contributing more job growth, gross domestic product (GDP), and foreign exports and sales to the U.S. economy than any other industry; they contributed about $1.38 trillion to U.S. GDP, employed 11.3 million workers, and accounted for approximately $110.8 billion in foreign sales and exports in 2005.

OVER 300 HUNDRED YEARS OF COUNTERFEITING EXCELLENCE

Le Comte extolled Chinese merchants for their commercial genius, but suggested they focus much of their “labor and natural industry” on dishonest business practices and counterfeit “almost everything they vend.” He writes: “(Chinese merchants) counterfeit Gammons of Bacon so artificially, that many times a Man is mistaken in them; ... It is certain a Stranger will be always cheated, if he buy alone, let him take what care he will.”

Remarkably, Le Comte’s observations from over 300 years ago remain valid today, and manifest themselves in the intractable problem U.S. companies encounter doing business with China: how to take advantage of China’s vast trade and commercial
potential without losing much of the intangible value of their corporations to counterfeiting and other forms of infringement.

Chinese counterfeiting and piracy levels are extremely high. According to the IIPA’s 2008 Special 301 Report, Chinese copyright piracy cost U.S. copyright industries almost $3 billion in 2007; piracy levels reached 90 percent of published records and music, 80 percent of business software and 95 percent of entertainment software. According to the U.S. trade representative’s report to Congress on China’s World Trade Organization compliance in 2004, the value of Chinese counterfeit products brought into the U.S. market reached $134 million. Chinese counterfeiting also limits demand for legitimate U.S. IP products globally, which damages company revenues and, by extension, the U.S. economy. The U.S. Department of Commerce, for example, reported that Chinese counterfeiting cost the U.S. economy about $20-24 billion in 2004.

Counterfeiting is not limited to Chinese street merchants. Chinese multinational corporations (MNC) are significant contributors to the overall counterfeiting of high-tech products. Cisco Systems filed an IP infringement claim in 2003 against Huawei Technologies (a powerful Chinese MNC that produces telecommunications and networking equipment) for copying patented Cisco technologies, user manuals, and the source code used for Huawei’s counterfeit routers. In a 2005 interview with PriceWaterhouseCoopers, Warren Heit, a partner at White & Case, states that display cases at some of Huawei’s offices contained ‘perfect’ knock-offs of Cisco telecom and Polycom equipment.20

Some Chinese MNCs view both legal IP development and illegal IP theft and infringement as extremely important components of their business models and key to their long-term profitability and survival. Huawei’s business model, for example, is partly based on selling counterfeit products in developing countries with poor IP protection. As Heit suggests: “Huawei is saying to itself... ‘I am going to knock (Cisco) products off and to the extent the IP law allows me to practice in these areas, I’m going to go there...Cisco, maybe you can have the U.S., but I’ll take you everywhere you haven’t gone.’”21

Chinese corporations’ counterfeiting of high-tech equipment and IP theft raises concerns beyond economic loss. Counterfeit computer components from China, for example, could be used to compromise U.S. corporate and government computer networks and cause military systems to fail.22 The U.S. government in early 2008 seized $76 million worth of counterfeit Cisco routers, switches, WAN interface cards, and gigabit interface converters, which were purchased by the U.S. Naval Academy, U.S. Naval Air Warfare Center, General Services Administration, U.S. Naval Undersea Warfare Center, and defense contractor Raytheon, among others.23 Melissa Hathaway, director of the Director of National Intelligence’s (DNI) cyber security office, commented on the government’s seizure of over 400 counterfeit routers: “Counterfeit products have been linked to the crash of mission-critical networks, and may also contain hidden ‘back doors’ enabling network security to [be] bypassed and sensitive data accessed [by hackers, thieves, and spies].”24
COUNTERFEITER, HACKER, SOLDIER, SPY

Chinese espionage directed against U.S. government and corporate targets is well-documented in the recent literature. U.S. Immigration and Customs Enforcement officials have investigated over 540 instances of illegal technology exports to China, which often involve Chinese corporations. The Washington Post published an article in April 2008 describing twelve cases of Chinese espionage that have occurred since March 2007. The charges range from illegal export of warship technology and source codes for simulation software for the precision training of fighter pilots, to theft of trade secrets from two companies on behalf of a Chinese military program. Joel Brenner, the head of the counterintelligence office of the DNI, states: “Espionage used to be a problem for the FBI, CIA and military, but now it’s a problem for corporations...It’s no longer a cloak-and-dagger thing. It’s about computer architecture and the soundness of electronic systems.”

The U.S. Defense Department and IC claim that China is America’s most serious cyber security threat. The Office of the DNI, in response to a Business Week inquiry, stated that computer intrusions have been successful against a wide range of government and corporate networks across the critical infrastructure and defense industrial base. A recent Business Week special report revealed Chinese hackers may have recently sent an e-mail attachment containing the malicious computer code to an executive at Booz Allen Hamilton, a $4 billion U.S. corporation, in an attempt to infect the company’s computer network and acquire sensitive information. According to the report, hackers have launched numerous similar attacks on U.S. companies and government agencies for the last several years; the Departments of Defense, State, Energy, Commerce, Health and Human Services and Treasury, and corporations Boeing, Lockheed Martin, General Electric, Raytheon and General Dynamics, are some of the known victims. The U.S. government reported the occurrence of 12,986 cyber intrusions and other cyber security events on government and defense contractor networks; U.S. military networks experienced a 55 percent increase in attacks. O. Sami Saydjari, a former National Security Agency (NSA) official, suggests the scale of organized Chinese hacking activities – much of which involves the Chinese military – is having a devastating impact on U.S. government and corporate computer networks.

A number of Chinese companies aggressively employ intelligence collection methods that cross the line of propriety and legality, and some of them are also IP infringers. According to the U.S. Department of Justice, U.S. auto-parts manufacturer Metaldyne, one of only two corporations in the world capable of transforming powdered metal into high-performance engine components, was seriously damaged when one of its former engineers gave proprietary information to potential Chinese competitors. A Huawei employee illegally took photos of Fujitsu circuit boards at Supercomm in 2003; Business Week speculated that the employee may have also collected proprietary information from AT&T, Cisco, Lucent, Nortel, and Tellabs. The U.S. software maker 3DGeo Development Inc. caught several trainees of the Chinese state-owned oil company Petro China Co. trying to access 3DGeo’s secure computer systems; one was sentenced to two years in prison in 2004. As a result of the increased incidents, the FBI decided in 2007 to identify the ten highest-value U.S. corporations (including General Electric,
DuPont and Corning) in the respective areas of the FBI’s fifty-six field offices throughout America and brief those corporations on the threat.\textsuperscript{33}

Chinese government research institutes are also actively involved in trade secret theft. The FBI and other U.S. government agencies recently identified about 150 individuals and businesses involved in illegally transferring aerospace and weapons technology to China and Iran; the espionage may have benefited Chinese government’s space program.\textsuperscript{34} Most notably, the FBI arrested physicist Shu Quan-sheng, the president of a National Air and Space Agency (NASA) subcontractor, for allegedly exporting restricted U.S. technology to China to assist the development of China’s Long March V heavy booster. According to the federal claim, Shu allegedly transferred sensitive data on the components of a specialized cryogenic hydrogen tank to the People’s Liberation Army’s General Armaments Department and its 101\textsuperscript{st} Research Institute. In a separate case, the U.S. Department of Justice (DOJ) reported in June 2008 that China’s Naval Research Center acquired Quantum3D Inc.’s Mantis 1.5.5 and viXsen trade secrets – software programs used to simulate real world motion and train military fighter pilots – from Xiaodeng Sheldon Meng, a Chinese software engineer and former employee of Quantum3D Inc.\textsuperscript{35}

**STRATEGIC ROAD AHEAD: CHINESE CORPORATIONS MUST LEAD THE WAY**

The late Professor Zheng Chengsi, father of IP in China and former director of the Intellectual Property Office of the Chinese Academy of Sciences (CAS), declared China’s economic growth in the 21\textsuperscript{st} Century will largely depend on its ability to manage intangible property and produce enterprises capable of successfully engaging in global IP competition.\textsuperscript{36} Zheng’s work at CAS persuaded the State Council to develop China’s first National Intellectual Property Strategy – promulgated in June 2008 – and his intellectual imprint is reflected in the Strategy’s emphasis on transforming the way companies create and acquire IP overseas.\textsuperscript{37} Section 2 (12) of the Strategy emphasizes the importance of making the corporation “the principal entity in the creation and utilization of intellectual property.” The Strategy also bears the mark of China’s national security experts in that it calls upon government agencies and enterprises to make more effective use of IP for national defense and encourages the development and use of civilian IP for military purposes.\textsuperscript{38}

The Strategy highlights the importance of improving China’s capacity to create IP and Chinese-developed standards,\textsuperscript{39} in which increased research and development (R&D) plays an integral role.\textsuperscript{40} On this front, Beijing has been very successful in inducing most large U.S. high technology firms to invest heavily in R&D in China – largely in the form of high-technology R&D programs and centers in exchange for market access and financial incentives – which is gradually helping China close the gap between basic research and bringing inventions to market. In addition, U.S. R&D activities in China not only help Chinese subsidiaries improve their own R&D programs,\textsuperscript{41} but could also indirectly help China’s defense-modernization efforts.\textsuperscript{42}

[Local Chinese employees working at foreign R&D centers may gain an in-depth understanding of how foreign technologies are developed and function. In some instances, R&D activity has included integrating foreign technology with local...]
systems or making foreign technology compatible with Chinese technical standards. This latter form of knowledge transfer (systems and standards integration capabilities), in particular, could be of potential use to China’s defense modernization goals, especially in developing asymmetric capabilities. For this and other reasons...extensive knowledge transfers through R&D in China could pose risks for long-term US security as well as economic interests.  

China spends heavily on R&D to improve China’s capacity to rapidly absorb and adopt foreign technologies that can advance civilian and defense technology and IP development. According to the 2007 OECD report, China has become one of the most R&D intensive countries in the world, second only to the United States; China’s R&D spending in 2007 surpassed Japan’s for the first time. China’s R&D spending could increase 24 percent in 2008 to $216.8 billion, which is roughly 18 percent of R&D spending worldwide. China’s total R&D spending in 2007 reached approximately $175 billion (an increase of nearly $155 billion in R&D spending since 2003). U.S. and Japanese spending during that same period totaled about $353 billion and $143.5 billion, respectively. The European Commission recently assessed that, if China continues to increase its R&D spending at the current pace, China could match the EU in R&D expenditure as a percentage of GDP by 2009. It is important to note, however, that government-sponsored R&D focuses primarily on applied research and technology development (the government used less than 6 percent of total R&D funding for basic research in 2002 and 2003).

Chinese corporations are becoming the most important contributors to the R&D spending in China. According to the Research Institute of Industrial Economics and Orebro University in Sweden, Chinese companies conducted about 68 percent of China’s total R&D in terms of spending in 2005, which highlights the dramatic shift from a government-centered to a corporate-dominated innovation system. Comparisons of China’s R&D expenditures with developed countries do not account for the large disparities between China and the West in the quality and cost of research staff. As Dr. Xu Zhijun, chief marketing officer of the Chinese multinational telecommunications giant Huawei argues, because of China’s low labor costs and access to high-quality researchers, Huawei may have spent only $1.1 billion in R&D last fiscal year, but that is equivalent to about $4 to $5 billion spent by western rivals such as Cisco.

As suggested later in this article, the global economic downturn has important implications for Chinese corporate R&D programs. Chinese companies will have to make hard choices about R&D funding, and many of them will probably choose to focus exclusively on combining in-house R&D with imported technology to avoid the high costs and risks associated with basic and more innovative research. (This R&D strategy has been heavily used by legitimate companies and counterfeiters in the past for reverse engineering purposes).

THE STRATEGIC VALUE OF COMPETITIVE INTELLIGENCE

Beijing’s push to make IP the strategic imperative of government agencies and corporations, as manifested in the Strategy, has had a significant impact on Chinese companies. Many Chinese executives, seeking to fulfill the government’s desire that
their enterprises become the driving force behind China’s technological innovation and IP creation, have established new competitive intelligence (CI) units or expanded their existing programs.\textsuperscript{52} Chinese companies have reportedly intensified efforts to hire qualified Chinese CI personnel to fill a growing number of CI collection and analysis positions.\textsuperscript{53}

Zhong Tianwei, the Guangzhou branch manager of Beijing TRS Information Technology Company,\textsuperscript{54} notes that many domestic enterprises can attribute their successes to CI.\textsuperscript{55} Competitive intelligence can help companies determine competitors’ R&D capabilities, keep informed of competitors’ product developments, assess competitors’ product performance, design new technologies and products, assess a competitor’s management strategies and decision-making capabilities, plan and manage R&D activities, create advanced S&T-based strategies, identify competitors interested in strategic alliances, and improve a company’s capability to protect its intellectual property from illegal human and technical collection.\textsuperscript{56}

\textbf{The Mandarins’ Perspective on Competitive Intelligence}

Chinese government officials, scholars, and business strategists have written extensively about CI and recognize how it can help China (as it did Japan) achieve its IP goals and eventually become an economic superpower.\textsuperscript{57} China’s vigorous promotion of CI, and its subset competitive technical intelligence (CTI), have helped make these important topics of concern in China.\textsuperscript{58} The Chinese Ministry of Ordnance Industry’s Intelligence Research Institute, National Defense Science and Industry Scientific and Technical Intelligence Bureau, and the State Science and Technology Commission initiated a study comparing domestic and foreign intelligence research and held a series of seminars on strategic intelligence research and development from 1991 to 1994, resulting in a change in the direction of Chinese intelligence research work: competitive intelligence became its new focal point.\textsuperscript{59}

Since the mid-1990s, a growing number of Chinese PhD dissertations have focused on CI and the use of intelligence to advance China’s national interests.\textsuperscript{60} Many of these students have gone on to become influential in business, government, and academia, and have helped push the theoretical development of corporate intelligence in China. Dr. Chen Feng, for example, who received his PhD from Beijing University and wrote his dissertation on CI in China with the assistance of his advisor Liang Zhanping, director of China’s Institute of Information Science and Technology, is now a CAS associate researcher and senior consultant to Ding Lu Management Consultants, Ltd. and has advised Chinese high-technology firms how to set up CI programs.\textsuperscript{61}

U.S. and Chinese scholars have provided a myriad of definitions of CI and CTI. Corporate CI can generally be defined as activity related to the collection, processing, exploitation, analysis, and dissemination of information and finished intelligence on corporate competitors and pertinent industries that could impact a firm’s competitive situation. How narrowly or broadly a corporation defines the term depends on the company’s mission and the goals of its intelligence programs; generally, more resources and funding are required to meet intelligence goals that are broader in scope. W. Bradford Ashton of Pacific Northwest National Laboratory and Richard Klavans of the Center for Research Planning define CTI as “business sensitive information on external
scientific or technological threats, opportunities, or developments that have the potential to affect a company’s competitive situation.62

Chinese scholars have generally accepted the above definitions, but have added caveats of their own. Chinese and U.S. scholars also agree that corporate intelligence does not and should not include unethical or illegal forms of intelligence collection, such as unauthorized monitoring of phone and internet communications, trade secret theft, etc. However, some Chinese scholars concede that a gray area exists in CI, where reverse engineering and IP transfer may take place without necessarily breaking the law and the benefit to public interest may override the ethical considerations.63

Chinese academics point out that company intelligence efforts are necessarily proprietary and need to be protected. The company’s sources and methods of collecting, processing, and analyzing information, and the intelligence derived from such activities, is confidential and usually well-guarded because unauthorized disclosure could negatively impact the company’s competitive position. This is primarily why Chinese companies are so interested in “anti-competitive intelligence” (also referred to as counterintelligence) programs: to help protect against IP loss in the “gray area.” This is discussed with some frequency in the Chinese literature.64 (As will be suggested later in this article, U.S. companies could also benefit from increased emphasis on counterintelligence programs.)

**Chinese Competitive Intelligence in Practice**

Chinese corporate intelligence in practice can differ substantially from how it is described in scholarly works. Although Chinese scholars stress that corporate intelligence programs must employ ethical and legal intelligence techniques and methods to produce intelligence, mounting evidence suggests Chinese firms are increasingly using their intelligence units to enhance the effectiveness of their illegal activities. Chinese espionage cases involving IP theft from U.S. companies since 2007 indicate the emphasis China places on illegal corporate intelligence, the great risks China is willing to take to acquire U.S. IP, and the disregard it has for the global IP system (note that the Chinese government denies any illegal conduct).

As discussed, Chinese executives and managers hope to transform their companies into global competitors (86 percent of Chinese executives interviewed for a McKinsey survey in 2008 indicated they had global ambitions). They view the development of corporate intelligence programs as a means to improve strategic management and help identify struggling U.S. firms to purchase. This ambition can drive them to turn otherwise ethical CI programs into illegal collection platforms. ‘The Chinese are out to develop a modern economy and society in one generation,’ notes Joel Brenner. ‘There is much about their determination that is admirable. But they’re also willing to steal a lot of proprietary information to do it, and that’s not admirable.65

The most robust Chinese corporate intelligence units are likely located in R&D centers overseas (often called “listening posts”), where the company can most effectively collect intelligence from its competitors and leverage the deep expertise of its many high-quality and relatively low-cost scientists and engineers to analyze and evaluate the technology and IP the company purchases or steals.66 The Chinese literature suggests the intelligence units’ internal processes are generally similar to those described in some of the most prominent works on corporate intelligence in the west.67 The organization of
some of the units may differ somewhat from those in the West, but they likely combine personnel with formal intelligence training and those who are experts in their given technical or scientific fields to conduct intelligence collection, processing and exploitation, analysis, production, and dissemination.68 Personnel assigned to listening posts can use their legal collection and analysis of patents, standards, business and market data, and information to inform illegal collection activities and vice-versa. They can also rely on scientific and technical assistance from their company headquarters, some of which are located in high-technology science parks in China and so have direct access to world-class government research institutes and universities (many of which employ scientists, engineers and academicians who have undoubtedly developed a corpus of useful knowledge and techniques related to obtaining proprietary and classified information from U.S. corporate and government laboratories).69,70

These listening posts – some of which may receive Chinese government intelligence and military financial support and collection guidance71 – may also employ illegal technical collection techniques (such as hacking) in the United States to obtain proprietary information from key U.S. competitors. Brenner claims Chinese hackers, on behalf of a Chinese corporation, hacked into “a large American company” to obtain sensitive company information prior to an impending business negotiation between the U.S. and Chinese companies. In a National Journal article, Brenner recounted the following incident: “The [U.S. business] delegation gets to China and realizes, ‘These guys on the other side of the table know every bottom line on every significant negotiating point.’ They had to have got this by hacking into [the company’s] systems.”72

Chinese illegal technical collection threatens U.S. corporate facilities worldwide and puts U.S. R&D centers operating in China at risk. In late 2007, Jonathan Evans, the director general of Britain’s domestic intelligence agency MI5, warned 300 firms operating in the UK of growing evidence that state-sponsored Chinese hackers were attacking corporate networks and stealing proprietary information.73 Although U.S. technology firms likely have physical and operational security procedures in place in their facilities inside China, they are probably no match for China’s corporate and government intelligence services – among the most effective in human and technical intelligence collection in the world.74 Microsoft Corporation, which intends to invest one billion dollars in China R&D over the next three years, will undoubtedly be a target for domestic Chinese competitors.

RETHINKING THE INTELLIGENCE PARADIGM

Roger George, senior analyst at the CIA’s Global Futures Partnership, argues the traditional intelligence paradigm, which was relatively successful in dealing with state-centric problems, is less effective at collecting and analyzing global and transnational phenomena. These emerging challenges are ‘blind spots’ that are difficult for analysts operating under traditional organizational and functional constraints to identify and understand.75 The global character of Chinese corporate espionage challenges the effectiveness of traditional U.S. intelligence and law enforcement efforts.76 An analysis of recent studies and press reports also suggests the U.S. IC and law enforcement communities still lack sufficient resources and expertise to effectively collect and
analyze data and information on Chinese espionage activities directed against U.S. companies worldwide.

Although the Cox Report was written a decade ago, many of its findings are relevant today. The report acknowledges the U.S. government cannot “completely monitor PRC activities in the United States” because of the scope of China’s “decentralized collection efforts.” According to the report, the CIA, Department of Commerce, FBI, and DoD never considered Chinese technology acquisition an intelligence priority. They failed to establish collection requirements to obtain information on Chinese government or commercial efforts to acquire U.S. technology companies, identify and obtain advances in U.S. technology, or establish business relationships with U.S. high-technology companies. Nor did U.S. agencies establish requirements to examine commercial affiliations between Chinese foreign nationals and U.S. companies. The Select Committee of the U.S. House of Representatives determined U.S. government agencies only conducted “narrow” or “reactive” monitoring of Chinese business activities rather than taking more proactive measures. “There is little or no coordination,” states the report, “within the U.S. Government of counterintelligence that is conducted against the PRC-directed efforts to acquire sensitive U.S. technology.”

The IC’s scientific and technical (S&T) intelligence framework – an outgrowth of the Cold War which largely collects and analyzes key S&T data and information within a classified system to understand foreign weapons platforms and identify emerging S&T threats, remains ill-suited to adequately handle evolving Chinese corporate espionage focused on IP theft and infringement. Under this S&T paradigm, Chinese CI would not likely be considered relevant for S&T collection and analysis (the IC would probably view it as a business or management issue) and IP would be treated primarily as an economic, legal, and trade-related matter. Chinese academics, government, and industry, however, encourage greater collaboration between government and industry intelligence programs and largely view S&T and IP as inseparable, whether from an intelligence or economic perspective.

Dr. Rob Johnston, in his 2005 study on analytic culture in the IC, suggests there is a separation of the domains of S&T and economic intelligence and expertise within the analytic community. To the extent that situation now exists and is not mitigated through collaboration, some S&T and economic analysts, who are looking at data and information from the perspective of their areas of focus and expertise, may overlook critical IP and R&D data and information that directly impacts analytic judgments on S&T developments in China. An economic analyst who has spent a career learning the tenets of economic analysis may not understand how unique IP and R&D data and information could inform S&T intelligence analysis, or consider how Chinese corporate intelligence impacts trade and innovation. If such issues are not overlooked, they would probably fall under the purview of analysts working on transnational matters; those analysts may or may not have extensive scientific, technical, or economic expertise, or even speak Chinese (RAND suggests the IC’s expertise and focus on S&T analysis and the assessment of foreign R&D programs has decreased).

The lines between Chinese intelligence, military, and commercial activities are not truly ‘blurred.’ The blurring of the lines cited in the Cox Report demonstrates how the IC has tried to apply a Western construct to understanding Chinese business and intelligence practices. As suggested from the evidence in previous sections of this article,
there are no strict legal lines separating Chinese intelligence activities from the corporate world as exist in the United States. Chinese corporations are always subject to extensive government influence and control, and many companies prefer having close links to the government for protection and access to resources and information that can give them a competitive advantage.

The barrier the IC has created between S&T and IP could create an imbalance in the allocation of resources and funding for collection and analysis of the issues. This could influence which U.S. agencies handle certain requirements and how IC offices are organized and staffed to deal with particular analytic problem sets; it could hinder collaboration and increase analytic error.90

The IC lists its intelligence collection priorities in the National Intelligence Priorities Requirements Framework (NIPF), which emphasizes about twelve priority intelligence targets, countries, or issues out of 150, according to a 2008 study by the RAND Corporation.91 The NIPF ranking of the relative importance of these priorities affects government resource allocations and those of the most critical importance to the country receive more funding for collection and analysis.92 The RAND study characterizes priorities such as terrorism, WMD proliferation (an S&T intelligence issue) and China as NIPF “crosscutting problems or theme-areas.”93 The study points out the “NIPF has great value for many uses, but it also provides an incentive to reduce spending resources on all but the hottest current priorities, often at the expense of deeper assessments of longer-term challenges.”94

Many U.S. policymakers tend to look to organizations such as the Department of State, DOJ, and the U.S. Patent and Trademark office for expertise on IP and other IP-related issues. Trade secret theft – one area of IP most often discussed in the intelligence context – is largely seen as the purview of agencies dealing with domestic counterintelligence matters, such as the FBI.95 Because of this, some other IC agencies, which are in the position to assist the FBI, might not be doing so because of cultural or institutional barriers.

It is also difficult for the U.S. government to impress upon companies the seriousness of the threat and persuade them to respond appropriately. Some U.S. corporations might be unwilling to assist the FBI or Department of Homeland Security (DHS) – for example, by revealing the fact a Chinese corporation has stolen proprietary information through human or technical intelligence collection methods – to avoid potentially negative repercussions for their business interests in China or damage to shareholder confidence.96

There are also indications that U.S. companies are still not taking the Chinese seriously. A recent McKinsey survey suggests that while U.S. executives view Chinese corporations as a significant threat, few (28% of respondents) have taken sufficient steps to counter the threat because of a perception that Chinese firms are relatively weak in product quality, marketing, and brand development. The report observes: “This lackluster reaction to the global ambitions of Chinese companies raises the question of whether business executives elsewhere are setting themselves up for some unhappy competitive surprises.”97
THE COMING STORM

Chinese leaders have made it clear that they want to reinvent China’s role in the world economy and move from dependence on foreign technology and direct investment to a country that rivals the United States in terms of industrial and technological power. They recognize that this requires promoting and rewarding scientific discovery and true innovation, increasing IP ownership, developing new technology standards, and making it possible for Chinese corporations to play an even greater role in foreign technology acquisition and IP transfer. China has made considerable advances in developing favorable national and local S&T, IP, and business policies, and has increased its emphasis on education and R&D.

Chinese companies have shown they can effectively absorb and adopt U.S. technology and IP to push innovation. According to Curtis Carlson and William Wilmot of SRI International, the company that pioneered innovations such as the computer mouse and robotic surgery, China is working with preeminent partners around the globe to create the future technologies, attaining parity with the United States in some areas such as nanotechnology. Along these lines, Frans van Houten, CEO of the European semiconductor company NXP, states China is now home to about 400 semiconductor firms that design chips and some of these companies will rapidly become top-notch innovators. Motorcycle suppliers, designers, and manufacturers, in Chongqing, China, have collaborated to develop a unique entrepreneurial network and business model called ‘localized modularization’, which allows manufacturers to request parts from suppliers without specifying details; i.e., makers note the size and weight of the parts in their orders and suppliers decide what parts to provide. This push to innovate is contributing to the rapid expansion of China’s patent system: Chinese domestic patent applications grew from 165,773 in 2001 to 470,342 in 2006.

Some observers are very optimistic about China’s largely untapped capacity to innovate. The National Science Foundation estimates China could graduate about four-times more engineering PhDs than America in the next several years. Based on their observations of the work of Chinese scientists, engineers, and researchers, Carlson and Wilmot believe the Chinese are just as creative as their Western counterparts; there is ample evidence of creativity and entrepreneurial ambition in Chinese firms. Many Chinese engineers and scientists who received their PhDs in the United States, some of whom played important roles in successful innovations in U.S. high-tech firms, are now returning to China.

At the same time, Chinese industrial espionage and IP misappropriation, often done with the support or knowledge of the government, shows China is also willing to disregard the traditional rules of the game when convenient and take great risks to acquire U.S. government secrets and corporate proprietary information to the detriment of U.S. national security. As demonstrated earlier, a number of the most well-known and powerful Chinese corporations actively engage in IP misappropriation, theft, and reverse engineering and solicit IP transfer from their foreign competitors’ former employees. To date, intense U.S. corporate and government pressure on the Chinese government to improve the enforcement of IP rights has had limited results. Clearly, the blowback for Chinese espionage has not been severe enough for some Chinese companies to stop their illegal activities.
Against this backdrop, one wonders how long U.S. technology firms – despite their current comparative advantage in S&T and IP – will be able to withstand Chinese competition. Many U.S. scholars and business leaders might argue that most U.S. firms will not succumb to Chinese competitive pressure until China improves its capability to innovate and strengthen its IP base vis-à-vis the United States. This could take several decades at a minimum. However, some of these same U.S. observers (perhaps due to bias, mirror imaging, apathy or hubris) fail to take seriously a question that weighs heavily on the minds of many Chinese executives with global aspirations and government leaders who want to turn China into a superpower: “How can we further improve the effectiveness of our CI programs, whether it be through legal or illegal means, to continue to close the IP gap with U.S. companies?”

**ECONOMIC DOWNTURN CREATES OPPORTUNITIES**

The global economic crisis is having a major impact on Chinese companies and trade. Chinese President Hu Jintao recently told members of the Communist Party that the global economic downturn is hurting China’s competitive advantage in trade and threatens Party legitimacy and ability to rule. Chinese leaders are growing increasingly concerned that the economic crisis, which has significantly reduced demand for Chinese exports and played a major role in the collapse of over 68,000 small Chinese companies, will leave millions of workers unemployed and lead to widespread domestic unrest. As the situation worsens, the pressure for Huawei and other MNCs to gain a competitive edge over U.S. and European competitors grows. Huawei’s CEO called on his employees in July to prepare “psychologically” for the impending downturn; employees must work in “crisis mode” to ensure growth and innovation. The pressure of working for Huawei is well-known in China, and employee depression and suicides have been on the rise this year, according to Chinese press reports. A Huawei employee, speaking on condition of anonymity, said that overtime is part of employee evaluations and the corporate culture encourages overtime to shorten product cycles and remain competitive vis-à-vis international giants.

Huawei and some other large Chinese companies view the crisis as an opportunity to invest in the United States and acquire Western IP at an excellent value. Recent press reports, for example, suggest Huawei will continue to expand in the U.S. market in 2009. China Mobile Ltd. also intends to set up its first R&D center outside of China (in California’s Silicon Valley in 2009) to assist its work on Internet and telecommunications integration. Donald Straszheim, an economist and vice chair of Roth Capital Partners, which has handled the financing of Chinese companies, states: “In the global recession, Chinese companies are looking around the world to acquire knowledge.” Chinese employees of Frog Design, a consulting firm that develops innovative products for Fortune 500 companies, take the following view of the crisis:

In China, the rule of the game is always "Stay One Step Ahead of Your Competitors"...[W]hen Chinese businesses run out of initiatives in which to invest their capital or when their investments stop...they make a concerted effort to...invest in research and development. In fact, senior executives in some companies have said publicly that in the near future they would either invest in...
their own health and personal happiness, or they would increase R&D budgets in their businesses to invest in better products to prepare for a new run when the downturn ends...This puts a premium on vision and strategic planning instead of short-term financial risk taking.\textsuperscript{110}

Some companies, which lack funds for R&D because of the credit crunch, may simply decide to engage in IP theft to maintain an edge over competitors. Michael Kump, a lawyer specializing in IP law, contends:

As economic conditions tighten and people start looking for ways to cut corners and gain an advantage, some will cross the line...in an illegal manner. One of the classic shortcuts is to steal competitors’ intellectual property. It can be quicker to target key employees at a successful competitor and try to get those employees to come over to your side than to invest in process and grow your business the right way.\textsuperscript{111}

PriceWaterhouseCoopers notes that established Chinese companies can greatly benefit from employee IP transfer; former U.S. technical specialists can receive financial support to establish start-up companies that rely on the proprietary knowledge obtained from their U.S. employers.\textsuperscript{112}

As the global economy continues to weaken, Chinese corporations will likely seek to expand their CI and R&D activities in the United States to increase productivity and improve their competitive positions. This growth will include acquiring struggling U.S. technology firms or their R&D centers, which could result in windfall IP transfers to Chinese firms. Jin Chen, a professor at Zhejiang University, asserts that Holly, a Chinese conglomerate, used its wholly-owned subsidiary in the U.S. to identify and acquire the Code-Division Multiple Access R&D unit from Phillips Electronics, which gave Holly rights to all IP at the facilities and many experienced engineers. The acquisition allowed Holly to improve its mobile telephone chip designs and position in the Chinese telecommunications market.\textsuperscript{113} Other notable examples include Lenovo’s purchase of IBM’s personal-computer business, the Shanghai Automotive Industry Corporation acquisition of Rover technology to create the Roewe brand,\textsuperscript{114} and Huawei’s purchase of Marconi to tap European markets and relationships with local carriers.\textsuperscript{115}

The list of high technology companies that are reducing their technical staff is growing. Sun Microsystems Inc. announced in early November 2008 that it would lay off about 6,000 employees. Teradyne Inc., the leading maker of microchip test equipment, stated it would release about 185 workers worldwide. National Semiconductor Corp., which makes chips, decided to lay off 330 employees and Applied Materials Inc., a manufacturer of chip equipment, announced it would cut 1,800 positions.\textsuperscript{116} Some Chinese companies may increase efforts to hire recently laid-off employees of U.S. high technology firms, which could be a growing source of IP transfer.\textsuperscript{117}

**RECOMMENDATIONS**

The following recommendations are provided for the consideration of the U.S. government:
Take Steps to Encourage the Chinese Government and Industry to Stop Illegal Industrial Espionage and Large-Scale Intellectual Property Theft

Thus far, complaints from the U.S. government and industry to stop this illegal behavior have either been met with Chinese government denials, abject disregard, or half-hearted enforcement efforts. Although U.S.-China trade agreements have had some success in curbing IP infringement, U.S. IP industries claim Chinese IP infringement is still occurring at unacceptable levels. It would be neither fair nor accurate to attribute all industrial espionage and IP misappropriation to the Chinese government, or state that all Chinese firms are engaged in this sort of behavior. However, the mounting evidence of Chinese illegal activities is creating a dark cloud of mistrust regarding Chinese business practices that fuels the more pessimistic views of Beijing’s plans and intentions.

U.S. government representatives should impress upon their Chinese counterparts that this behavior could have a long-term negative impact on U.S. public perception of China. In addition, given the level of Chinese industrial espionage, the U.S. government should consider enacting laws that would impose more severe sanctions on Chinese companies whose employees are caught stealing U.S. technology and IP.

Closely Review Proposals of Chinese Companies to Purchase R&D Centers of U.S. High-Technology Companies

Huawei proposed to purchase its U.S. competitor 3Com last year, which would have given it access to technology supplied to the Pentagon. Although this was clearly a case in which national security interests were at stake, a closer examination of future high-technology purchase proposals may reveal security implications that are not quite so obvious.

Make CI a New Strategic Theme in the IC

The IC should consider designating CI as a new ‘strategic research theme’ to help identify and monitor new trends in foreign intelligence that could impact homeland security. China has made CI the center of its intelligence studies and, as mentioned, this is having an impact on Chinese government intelligence research. CI exerts an important influence on the evolution of intelligence programs in other countries as well. In France, for example, CI “involves all levels of government, numerous support organizations from the private and public sectors as well as public private partnerships and quasi-governmental organizations, like the Chamber of Commerce and Industry...or the Agency for the Diffusion of Information and Technology.”

Develop Programs on IP and CI at U.S. Government Civilian and Military Colleges and Universities

The extensive Chinese literature on CI has provided a window into a side of China that one is otherwise hard-pressed to find: a detailed discussion of Chinese government intelligence and counterintelligence operations. CI gave the Chinese a vehicle through which they could once again openly discuss intelligence and operations within the politically safe context of international business. At the same time, U.S. literature and understanding on the subject is relatively inadequate, with few books having been written on the subject of Chinese intelligence operations. Against this backdrop, the U.S. government should develop courses and sub-discipline programs at government civilian
and military colleges and universities to train and educate students and professionals in IP and CI matters.

**Devote More Funding to Collection and Analysis**

As part of this effort, the IC should devote more resources and funding to collection and analysis of the Chinese S&T and IP collection issues. As S&T intelligence requirements are part of the NIPF (National Intelligence Priorities Requirements Framework), according to the RAND report IP requirements should be combined with S&T requirements and ranked among the ‘hottest priorities.’ The IC should also require Chinese S&T analysts to obtain a deeper understanding IP issues and the development of Chinese language skills. S&T analysts who do not have S&T backgrounds should be required to obtain formal training and education in critical S&T areas.

The IC also needs more intelligence officers to devote to the problem. Despite the rapid increase in cyber security incidents and illegal technology transfer activities in America, the number of officers available to handle these cases remains limited. For example, the number of FBI agents assigned to handle Chinese spying activities in the United States has only risen from 150 in 2001 to 350 in 2007.121

**Develop a Cadre of Analysts, Scientists, and Technical Personnel with Chinese Language Proficiency**

The IC also requires more S&T analysts fluent in Chinese. As suggested in some of the declassified National Intelligence Estimates (NIE) on China (from 1949 to 1976), the IC had difficulty assessing the strategic objectives, military, and scientific and technical capabilities of China because the IC lacked collection in some areas and was forced to rely on Chinese press reporting.122 Given China’s intense secrecy today, IC China analysts are perhaps forced to rely on Chinese open source material more than analysts focusing on other foreign countries.123

Unfortunately, only a limited number of IC analysts can read Chinese; translating scientific and technical Chinese documents requires specialized skill. More China analysts must develop the capability to read and understand scientific and technical Chinese. Developing this skill is especially crucial for today’s S&T analysts because of the great strides China is making in S&T and R&D (many key Chinese S&T documents and books have only been published in Chinese).

The following recommendations are provided for the consideration of U.S. corporations:

**Establish or Strengthen Competitive Intelligence Programs**

U.S. corporate executives and managers also need to develop or strengthen intelligence and counterintelligence programs in their companies. Some Chinese companies are outperforming their U.S. competitors in this area, and their successes can provide useful lessons for U.S. companies doing business with China. The consensus in the Chinese literature on CI is that training and education is essential for a successful CI program.124 Although U.S. companies also understand this is important, they lag far behind some Chinese companies in CI training and education. For example, while DuPont employees are required to complete online training regarding insider risks,125 employees in some Chinese companies are obtaining their doctorates in CI.126
Consider Sending Employees to Outside Competitive Intelligence Training Courses

Company employees could learn a great deal about CI matters by attending outside CI training courses in China and the United States. Chinese companies send employees to CI courses held in various cities in China. The Chinese Business Training Network (CBTN) offers CI courses in China almost monthly. The course syllabus covers the following selected topics: goals of intelligence and competitive intelligence collection; using intelligence analysis and production methods; preventing disclosure of proprietary information during company visits; developing insiders in competitors’ companies; creation of social networks to find and recruit key IT personnel; creating CI units within the company; establishing clear lines of communication and support with other departments; protecting trade secrets; identifying and neutralizing intelligence threats; and case studies on real espionage cases and lessons learned (including case studies based on traditional CIA espionage operations and Chinese corporate counterintelligence investigations).\textsuperscript{127}

Increase Collaboration with Government Agencies and Heed Government Warnings

Although the FBI and DHS have set up official groups within which U.S. companies can confidentially reveal their computer network vulnerabilities to the government,\textsuperscript{128} some companies remain loath to do so, for reasons mentioned previously. The National Journal’s recent article on Chinese hacking also suggests that some U.S. companies view government warnings as alarmist hyperbole.\textsuperscript{129}

Strengthen Protection of Sensitive Data and Consider the Long-term Risks Associated with Lay-Offs of Employees with Knowledge of Critical Proprietary Information

As high-technology corporations increase employee lay-offs, they must take steps to ensure their sensitive data is well protected. Current information storage technologies, such as USB drives and other devices, have facilitated the ability of employees to take vast amounts of proprietary information to a company’s competitors.\textsuperscript{130} Cadence Design Systems, a software company, developed standard operating procedures – consisting of strict access and document controls, enterprise rights management and compartmentalization – to control the unauthorized release of such proprietary information. Cadence also employs modular software development procedures to compartmentalize information when conducting R&D in developing countries.\textsuperscript{131} However, the potential problem with such a method is that all of the money and effort put into its design can be lost if only one trusted employee with access to the right proprietary data departs the company and works for a competitor. Many U.S. high-technology corporations, with the sole aim of cutting costs, often release employees without even assessing how they could damage compartmentalization efforts and long-term market position.
CONCLUSION

The U.S.-China Economic Security and Review Commission warns in its 2007 annual report that, as U.S. companies continue to develop new technologies in hundreds of high-tech factories and joint R&D facilities in China, Chinese espionage poses the most significant threat to U.S. technology. If the U.S. government and industry cannot adequately control Chinese espionage in America, they certainly cannot expect to stop massive IP infringement and theft from U.S. R&D centers and other facilities located in China. Although U.S. IP industries can continue to push for stronger legislation (in both America and China) that would increase the penalties for Chinese companies and individuals involved in espionage, they must take steps to protect their intangible property to maintain their competitive positions worldwide.

China’s large-scale infringement and theft of IP hurts the U.S. economy and, at the same time, helps advance Chinese science and technology, improve new weapons systems, and develop new products and processes. If America cannot do better at curbing these activities, then it becomes imperative for the IC to develop more robust methods of following Chinese S&T developments and informing policymakers of their potential ramifications. As U.S. preeminence in S&T and IP begins to wane, the importance of tracking and understanding emerging trends – such as CI in China – grows. Left unchecked, Chinese illegal forms of intelligence collection will enhance China’s corporate intelligence programs and competitive advantage to the detriment of U.S. corporations and the U.S. economy.

China must strengthen efforts to cooperate with the United States on stopping such illegal activities, which greatly damage China’s image and could push American public opinion toward protectionism or economic retaliation during an extended economic downturn.132 As the cases of contaminated Chinese food products and toys demonstrate, the short term economic benefits of unscrupulous and illegal behavior is not worth the long-term damage to the image of Chinese corporations and their business practices in the United States. The majority of ethical Chinese businessmen and laborers have worked too hard over the last several decades to watch their many successes become tarnished by the refusal of the Chinese government and unscrupulous corporations to admit and stop such wrongdoing.

Robert Slate is a lead systems engineer at the MITRE Corporation. He formerly served as a captain in the U.S. Army and faculty member at the National Defense Intelligence College, Post-Graduate Intelligence Program-Reserves. Prior to obtaining his Juris Doctorate, he received his master’s degree from the Fletcher School of Law and Diplomacy and bachelor’s from Oberlin College. Slate is currently pursuing his PhD in environmental science. He has previously published articles on U.S. intelligence and Chinese military, strategy, and legal issues. Mr. Slate may be contacted at rbslate@gmail.edu.

† The views express in this manuscript are the author’s and do not reflect the official position of the MITRE Corporation or imply endorsement by the Office of the Director of National Intelligence or any other U.S. government agency. The author’s affiliation with MITRE is provided for identification only. It does not convey or imply MITRE’s concurrence with, or support for, his positions, opinions, or viewpoints.

2 “Competition from China: Two McKinsey Surveys,” *The McKinsey Quarterly* (2008): 8. [Hereafter cited as “Two McKinsey Surveys”]; The National Counterintelligence Executive’s 2005 report holds: “Foreign governments and intelligence organizations have created quasi-official organizations to enable them to capitalize on the private-sector technology theft that is underway. Indeed, the CI Community believes that foreign governments are major beneficiaries of the private-sector technology flow...To elicit sensitive information from those attending these quasi-official organizations, government officials may appeal to the professional egos of the private sector contacts, to their patriotism, or to their commercial sensibilities, by offering domestic business deals to accomplish technology transfer. Coercion is also an option in countries like Russia and China, where security services still hold considerable sway over the private sector.” National Counterintelligence Executive, *Annual Report to Congress on Foreign Economic Collection and Industrial Espionage (2005)*, (Washington, DC: National Counterintelligence Executive, 2006), 6. [Hereafter cited as *Collection and Industrial Espionage*.]

3 The Office of the Director of National Intelligence (DNI) states human intelligence collection “is performed by overt collectors such as diplomats and military attaches... [and] includes clandestine acquisition of photography, documents, and other material; overt collection by personnel in diplomatic and consular posts; debriefing of foreign nationals and U.S. citizens who travel abroad; and official contacts with foreign governments.” See Official Website, Office of the Director of National Intelligence, http://www.dni.gov/what_collection.htm.

4 Wesley Wark suggests some methods of technical collection, such as “line-tapping, bugging, outputs from remote sensors, computer hacking (and) perhaps ‘deep mining’ of the Internet” can be difficult to neatly place in any single-intelligence agency category. Wesley Wark, *Twenty-First Century Intelligence* (Oxford, UK: Routledge, 2005), 53. Technical collection generally refers to signals intelligence (SIGINT), imagery intelligence (IMINT), measurement and signature intelligence (MASINT) and geospatial intelligence (GEOINT). According to the DNI, SIGINT “is derived from signal intercepts comprising – however transmitted – either individually or in combination: all communications intelligence (COMINT); electronic intelligence (ELINT); (and) foreign instrumentation (FISINT). Ibid. For the purposes of this paper, “illegal” technical collection primarily refers to illegal SIGINT and computer hacking.


6 See, for example, Wang Qi, “Business Competition and Competitive Intelligence,” [*Qiye Jingzheng yu Jingzheng Qingbao*] *Military Dual-Use Technology and Products* (2002); “A Chinese Website advertising a technology exhibit in April 2006 in Chongqing, China, highlights the emphasis Beijing places on facilitating the transfer of technology from civil to military uses. According to the Website, the exhibit has three objectives: breaking down the barriers to sharing technology among industries, bureaucratic entities, and state and private sectors; facilitating coordinated development between the civilian hi-tech sector and the military; serving as a technology-exchange platform for civilian and military technologies.” *Collection and Industrial Espionage*, supra note 2, 5.

7 Christopher Bellavita, in his article “Changing Homeland Security: Shape Patterns, Not Programs,” *Homeland Security Affairs* II, No.3 (October 2006), notes the majority of homeland security policy matters are overly “undefined...broad...(and) complex.” [Hereafter cited as *Shape Patterns*.]

8 Li Yingzhou et al., *A Summary of Nearly a Decade of Competitive Intelligence Research in China* [*Jin Shi Nian Wo Guo Jingzheng Qingbao Yanjiu Zengshu*] (Jan. 1, 2007) http://www.zoomchina.cn/content/view/45/97/1_0.html. [Hereafter cited as *Decade of CI*.]

9 Jamie Smith and Leila Kossou, “The Emergence and Uniqueness of Competitive Intelligence in France,” *Journal of Competitive Intelligence and Management*, No. 4.3 (2008): 65. [Hereafter cited as *CI in France*.]

---

*Homeland Security Affairs, Volume V, No. 1 (January 2009) www.hsaj.org*
Over the past sixteen years, foreign direct investment in China has reached almost a half-trillion dollars; China’s annual economic growth rate has routinely topped upwards of 8 percent, and some years it has approached 10 percent. David Lei, “Outsourcing and China’s Rising Economic Power,” *Orbis: A Journal of World Affairs* 51, No. 1 (2007).


18 See *Memoirs*, supra note 10, 238-239.

19 Ibid., 238.


21 Ibid.


23 Ibid.

24 *Dangerous Fakes*, supra note 22, p. 035.

25 *Decades*, supra note 5.


27 Ibid., 035.

28 Ibid., p. 033.

29 According to the *National Journal*, the Chinese government and military employs computer hackers to steal government secrets and corporate proprietary information. Shane Harris, “China’s Cyber-Militia:

30 E-spionage, supra note 26, 040.
31 Case of China, supra note 20.
32 Implications, supra note 16, 43-48.
35 Ibid. See also, Department of Justice, Chinese National Sentenced for Economic Espionage (2008), http://hongkong.us consulate.gov/uscn_ others_2008061802.html.
38 “The administration of intellectual property needs to cover all links in national defense, including research, production, operation, equipment procurement and guarantee, and project management, and control of major intellectual property related to national defense should be strengthened. A guideline to key technologies needs to be published. Create a number of the self-relied intellectual property in areas such as key technologies for weapons and military equipment and high technologies for both military and civilian purposes. An early warning mechanism for intellectual property related to national defense needs to be established, and special examinations of IPRs related to national defense should be carried out in military technology cooperation and arms trade...Make more effective use of intellectual property related to national defense. The rules for keeping secrecy and declassification of intellectual property related to national defense need to be further improved. Promote the use of intellectual property related to the national defense for civilian purposes with the condition that national security and the interests of national defense are not compromised. Encourage the use intellectual property for civilian purposes in the area of national defense.” Ibid., §IV (7) (38, 39).
39 China’s push to create standards for third-generation (3G) mobile telephony, based on the TD-SCDMA (Time Division-Synchronous Code Division Multiple Access) standard, and the Internet (IPV6), is motivated by a desire to avoid licensing fees and ground the standards for these technologies in Chinese IP. James Popkin and Partha Iyengar suggest China is generally developing standards to protect domestic firms from foreign competition and, in the case of security standards for wireless communications,


41 Chien-Hsun Chen et al., High-tech Industries in China (Cheltenham, UK: Edward Elgar Publishing, 2005), xv. “In the vast majority of cases, multinationals are willing to provide their China subsidiaries with advanced technology; this was true of 86.6 percent of the multinationals included in the sample. 65.3 percent of the multinationals in the survey were providing technology that had not previously been available in China. Technology obtained from foreign-invested enterprises accounts for over 50 percent of all foreign technology introduced into China; in more than 60 percent of cases multinationals’ Chinese subsidiaries are using technology that is less than three years old.” Ibid.


43 Ibid.


47 See Case of China, supra note 20, 3-4.

48 Ibid., 2.


50 Some Chinese counterfeiting operations are so advanced that they include well-funded and elaborate underground R&D programs. Xu Chao, “Black Phone Innovations [Hei Shouji Chuangxin],” World Communications Weekly (June 10, 2008) http://www.cww.net.cn/mobile/html/2008/6/10/20086101826494773.htm; See also Case of China, supra note 20, 3-4.

51 China’s IP Strategy is intended to transform China’s IP activities from being primarily a legal and trade-related issue, to becoming a strategic imperative that is the domain of Chinese corporations and government agencies. Numerous policymakers and officials from the State Council, SIPO, COSTIND (State Commission on Science, Technology and Industry for National Defense), the Ministry of Science & Technology (MOST), CAS, Supreme People’s Court (SPC), Ministry of Public Security (MPS) and representatives from top universities in China, such as Beijing and Qinghua Universities, have been involved in developing, collaborating and coordinating on various aspects of the Strategy. Coinciding with the development of the IP Strategy, statements on the importance of IP and the IP Strategy for improving the development of the national economy, innovation and military weaponry began to appear in national S&T development plans, China’s National Defense White Papers (NDWP) (2006), and COSTIND publications—a relatively recent phenomenon in China. The NDWP, for example, emphasizes that the military should improve innovation to build better weapons and equipment and that increased R&D in the military has resulted in the development of new S&T inventions and IP. Implications, supra note 16, 29.


54 TRS conducts R&D on information retrieval and content management systems for the Chinese government and industry and provides information technology support to corporate and government CI systems. TRS Website [(in Chinese), Company Profile, http://www.trs.com.cn/company/compintro/lhz.


57 Justin L. Bloom, “Japan as a Model for a National Approach to Business Intelligence,” 49.


59 Decade of CI, supra note 8.


63 Decade of CI, supra note 8.

64 Ibid.

65 Cyber-Militia, supra note 29.

66 Chinese R&D and CI labor costs are significantly lower than in America. According to Huawei, at one-fifth of that in the West, Chinese multinational giants can compete in the R&D arena with less than a quarter of the R&D budget of large Western firms. Prowess, supra note 49.

67 Technical Intelligence, supra note 56.

68 See Decade of CI, supra note 8.

69 Chinese companies that are located in high-tech science parks in China not only benefit from preferential tax, financial and foreign exchange treatment, but are also able to collaborate with first-class research institutes and universities. Beijing’s Zhongguancun Science Park, for example, contains over 12,000 firms and is located in the Haidian district, which contains 232 scientific research institutes, 73 universities (including the Harvard and MIT of China, Beijing University and Qinghua University, respectively). Company R&D and innovation costs are tax deductible, and imported technology and IP receive tariff exemptions. According to official Chinese data, the park’s gross industrial output reached about $25 billion in 2003. Quanlin Gu et al., “Firm Dynamics in Economic Transition: Evidence from a

70 Notra Trulock, the former director of intelligence at the U.S. Department of Energy, writes: “[T]he Chinese approached spying differently from the Russians... Chinese techniques were “nontraditional” in that they concentrated more on eliciting information from visiting scientists and other officials and less on Soviet-style spycraft...[T]he Chinese would employ scientists, academicians and students to collect information of interest...Intelligence taskings would come from scientists or academic institutions engaged in research for the People’s Liberation Army or from other government customers... The Chinese painstakingly collected lab and Energy Department unclassified technical reports, and visitors to Chinese facilities were struck by the thoroughness of their collections. In their own writings, the Chinese assessed these reports as ‘provid[ing] intelligence of great value.’ The Chinese knew all about the labs’ penchant for sloppy handling and “inadvertent” releases of classified documents...” Notra Trulock, Code Name Kindred Spirit: Inside the Chinese Nuclear Espionage Scandal (San Francisco, CA: Encounter Books, 2003), 106-07; Chinese companies located in the park also have access to government-supported research in scientific and technical areas. Strategic Intent, supra note 49, 5.


72 Cyber-Militia, supra note 29.

73 E-spionage, supra note 26, 040.

74 Cox Report, supra note 72.


76 Ibid.

77 Cox Report, supra note 72, p. 87.

78 Ibid., 87-88.

79 Ibid., 88.

80 Ibid.

81 Ibid.


83 CI & Strategic Management, supra note 60.

84 Rob Johnston, Analytic Culture in the US Intelligence Community: An Ethnographic Study (Washington, DC: Center for the Study of Intelligence, 2005), 66-70. [Hereafter cited as Analytic Culture.]

85 Ibid.

86 Ibid., 67.

87 Gregory F. Treverton and C. Bryan Gabbard, Assessing the Tradecraft of Intelligence Analysis (Santa Monica, CA: RAND Corporation, 2008), 4. [Hereafter cited as RAND report.]
88 Intelligence Analysis, supra note 82, 294.
89 Cox Report, supra note 72, 50.
90 Analytic Culture, supra note 84, 66-70.
91 RAND report, supra note 87, 1.
92 Ibid.
93 Ibid., 48.
94 Ibid., 7.
95 Decades, supra note 5, A1.
96 Cyber-Militia, supra note 29.
97 Two McKinsey Surveys, supra note 2, 6.
100 Implications, supra note 16, 46.
101 Innovation, supra note 98, 268-269.
110 Ibid.
112 The company’s 2005 study on Chinese IP points out: “In China, a large number of technical specialists who have retired after enjoying a full career in the United States or Europe discover a very supportive
environment for a second career in China...funds are available for such start-ups from domestic and foreign sources, and venture capital money increasingly is attracted to ones with major potential and apparent political support.” *Case of China*, supra note 20, 5.


115 *Strategic Intent*, supra note 49, 9.


117 *Case of China*, supra note 20, 5.

118 *Implications*, supra note 16, 43.

119 Christopher Bellavita suggests using a “pattern-based approach” to help make sense of such evolving homeland security issues “to sift through the elements of strategic disorder...and determine whether an issue can be ordered—and thus subject to a rich set of knowledge and methodologies...” See *Shape Patterns*, supra note 7.

118 CI in France, supra note 9, 6.

112 FBI Offensive, supra note 33.


113 Ibid.

114 *Decade of CI*, supra note 8.

115 FBI Offensive, supra note 33.

116 *Decade of CI*, supra note 8.

117 See *Trade Secret Protection*, supra note 1.

118 *Cyber-Militia*, supra note 29.

119 Ibid.


121 ‘You just don’t give the developers access to the code tree the way we would in an equivalent position here...We’re just opening up Russia as an example. We have 100 people there; we’ll have 200 people there a year from now. They’re superb engineers. They are the best of the best out of the Russian Academy of Sciences and their engineering schools, and they’re astonishing mathematicians. So we’re giving them big math problems, big algorithm problems to help drive the heart of these software packages that we produce. It doesn’t connect to anything for them—it’s just a big matrix to solve, and they’re doing a marvelous job of it.” *Case of China*, supra note 20, 58-60.

122 Thomas P.M. Barnett, "Ten Reasons Why China Matters To You," *Good 10* (2008), 63. Although Professor David Lampton, Director of China Studies at John’s Hopkins University’s School of Advanced International Studies, does not support a “confrontationalist” policy toward China, he concedes that China must cooperate with the United States on the matter of intellectual property protection: "China
simply is too big to be allowed to violate foreign intellectual property the way earlier, smaller modernizing economies did. Beijing has to assume responsibility for the local officials who have become addicted to the revenues and employment their localities generate through the theft of intellectual property." David M. Lampton, "Paradigm Lost: The Demise of "Weak China," The National Interest, No. 81 (2005), 79-80.
Community Health Centers: The Untapped Resource for Public Health and Medical Preparedness

Karen M. Wood

The last few years of our political history have witnessed the emergence of a national preparedness architecture boasting numerous plans, strategies, directives, legislation, and even more novel programs to address those issues identified therein. One of the more recent entrants to this collection includes Homeland Security Presidential Directive-21 (HSPD-21) also known as the Public Health and Medical Preparedness Strategy. On October 18, 2007 HSPD-21 was released to the public calling for a transformation in the national approach to public health and medical preparedness in the United States.

Like most everything else in this body of work, HSPD-21 adheres to the paradigm of the National Incident Management System (NIMS) and the National Response Framework (NRF), and elaborates on a preparedness vision conceptualized in previous strategies. The latest deliberations, as prioritized by this strategy, are to bolster the nation’s ability to manage a public health crisis by stimulating improvements in the areas of biosurveillance, countermeasure distribution, mass casualty care, and community resilience; the objective being to create a much more tightly integrated systems-approach toward public health and medical preparedness. Interestingly, a huge potential component of this proposed system is already relatively well developed and continues to grow, but has been unable to garner significant preparedness support in the government’s frenzy to develop wholly new entities and indoctrinate skeptical hospitals.

As providers of critical medical and human services to vulnerable populations in medically underserved areas, community health centers (CHCs) – the untapped resource – are often recognized as indispensable and respected authority figures within their communities. As federally qualified health centers (FQHCs), regulated by the Bureau of Primary Health Care (BPHC) in the Health Resources and Services Administration (HRSA) of the U.S. Department of Health and Human Services (HHS), the administrative infrastructure and accountability mechanisms are already in place to groom CHCs for an active and measurable role in public health and medical preparedness.

This article discusses the background of the Health Center Program and the potential roles of CHCs in relation to the Public Health and Medical Preparedness Strategy. Specifically, it argues that CHCs by philosophic orientation, geographic location, and as publicly funded entities, are well-positioned to provide medical services, education, and other human services to prevent, prepare for, mitigate, respond to, and recover from the public health impact of a bioterrorist event or other biological disease outbreak. Ultimately, this paper contends that aggressive investment in CHCs and their emergency management programs is a dual-purpose investment that will (1) support many of the objectives identified in the Public Health and Medical Preparedness Strategy, and (2) create greater social equity by reducing health disparities and make public health emergency management more accessible to special needs populations.
Finally, it discusses the current state of preparedness in CHCs, identifies barriers to implementation, and presents essential recommendations to get our nation on the path to public health and medical preparedness.

THE HEALTH CENTER PROGRAM

A community health center (CHC) is a non-profit primary-care practice governed with federal support via Section 330 of the Public Health Services Act\(^2\) and is strategically located in a federally-designated medically-underserved area to provide high-quality primary and preventive health care to anyone seeking care, regardless of their ability to pay. The emphasis on the underserved includes the uninsured, underinsured, Medicaid and Medicare recipients, and those without a medical home or who otherwise lack access due to travel distance, hours of operation, and cultural and linguistic barriers. The majority of patients served would fall in the classification of indigent care including migrant health and healthcare for the homeless, but CHCs also provide primary care in rural areas where services simply do not exist. Beyond the many required services that health center programs must provide and/or coordinate, most CHCs (dependent on their resources, capabilities, and the needs of their target population) directly provide pharmaceutical services, translation services, substance abuse and mental health services, and oral health services.\(^3\)

According to the National Association of Community Health Centers (NACHC), there are around 1,200 community health centers with more than 6,600 delivery sites (see Figure 1) spread across all fifty states and U.S. territories providing primary care to more than 18 million patients annually.\(^4\) Fortunately, the Bush Administration has been fairly supportive of the Health Center Program in recent years through the President’s Health Center Initiative. Between 2002 and 2007, the goal of CHC expansion into 1,200 additional communities was reached by doubling annual investments from $1 billion in 2000 to nearly $2 billion today.\(^5\) Even with these successes, the numbers of the medically underserved in our nation is staggering. The number of uninsured Americans is projected to reach 60 million by 2010 and another 56 million Americans lack access to primary care simply due to a shortage of physicians in their communities.\(^6\)

STRATEGY IMPLEMENTATION: THE ROLE OF THE COMMUNITY HEALTH CENTERS

HSPD-21 or the Public Health and Medical Preparedness Strategy asserts that the most critical components of public health and medical preparedness include biosurveillance, countermeasure distribution, mass casualty care, and community resilience. Within each of these defined critical areas, CHCs have the potential to make significant contributions to our nation’s emergency preparedness and response efforts.

This section discusses the variety of ways in which CHCs can support their emergency management networks including: biosurveillance in hard-to-reach populations, supporting local health departments by providing staff and/or facilities for dispensing countermeasures, supporting mass casualty care efforts by mitigating surge on area hospitals and health systems, and promoting community resilience by supporting the spectrum of emergency management activities.
Biosurveillance

Overwhelming evidence exists suggesting that vulnerable populations suffer the greatest during natural disasters and epidemics. According to the U.S. Commission on Civil Rights:

A crisis exists that has left a vast number of Americans, primarily the poor, women, and language, racial, and ethnic minorities, unprotected and uncared for by our nation’s medical system. The current and very real threat of a biological attack has brought this crisis to the forefront of public issues necessitating immediate action.7

Patterns in susceptibility to illness and disease are unevenly stratified across socioeconomic status, racial, and/or ethnic groups. For example, Philip Blumenshine and others suggest that pandemic influenza will permeate these vulnerable populations with greater ease and speed because of financial and social constraints like limited telecommuting opportunities, financial pressures to go to work, and reliance on daycare services for childcare.9 Ultimately these pressures create a tendency to congregate which

Figure 1
Data Source: Health Resources and Services Administration, 2005
is clearly dangerous for disease containment and will result in greater affliction for these groups.

Consistent with the overarching objective of CHCs to provide primary and preventive care to underserved populations, service delivery sites are logically nestled within these vulnerable populations and could be strategically utilized to enhance our nation’s biosurveillance capabilities in the very populations that may be the first to signal a public health problem. Most CHCs occupy freestanding, permanent facilities while others are based in public schools, in or near hospitals and tribal communities, and still others operate seasonal programs and mobile clinics bringing their services directly to the patient. CHC services and the expertise of their clinical staff, however, often extend even beyond the immediate facility. Many CHCs partner with or are contracted by nursing homes, correctional facilities, and various shelters to provide services, as well. With this reach in their respective communities, CHCs could be leveraged as the eyes and ears of the public health community in these hard to reach populations.

The BPHC issued Program Assistance Letter (PAL) 2002-02 advising health centers to “utilize the CDC and other appropriate clinical information resources on bioterrorism to enhance the health center’s ability to recognize the signs and symptoms of diseases and toxic agents that may be used in a bioterrorist attack.” Yet for agencies that are dedicated to expanding patient services, at times operating very close to the margin, this undertaking is generally not managed in any methodical way. In 2006, Art Clawson and others surveyed Florida-based CHCs and revealed that of those respondents having an emergency operations plan, only 41 percent had written policies that addressed bioterrorism preparedness and only 56 percent discussed reporting suspicious symptoms to the county health department. Moreover, when prompted with the question of what the center would need to respond, 80 percent of respondents reported a high-priority need for training personnel.

C. Robert Kline, Jr. describes the ruinous impact of a biological attack and highlights the urgency of preparation when he states:

The stresses placed on responding to disasters, of whatever source but especially bioweapon release, strain even the best systems, and they do so for a long time with both volatile perturbations and a rapidity that is often hard to grasp. Preplanning reduces some of the stresses. Prevention is cheaper than cure.

It has already been established that the public health infrastructure is overtaxed. Michael A. Stoto and others warn that even the threat of a localized outbreak will compel a surge in surveillance in surrounding jurisdictions. A surge, coupled with a slower turnaround in investigation and diagnosis for uncommon pathogens, could be an invitation for a costly recovery as opposed to the presumably cheaper alternatives of prevention and mitigation. Preparing CHCs to support biosurveillance activities and surveillance systems could be an inexpensive and effective means for bolstering the public health infrastructure during an otherwise crippling incident. All that is required to implement this valuable asset is training practitioners to recognize the clinical features of the various biological weapons agents and providing adequate and robust reporting channels to facilitate a rapid response.
Countermeasure Distribution

When practicable, Points of Dispensing (PODs) for countermeasure distribution even for one community, much less a region, should be designated in a way that provides comprehensive coverage for an area and ensures accessibility for residents all the while ensuring sufficient space between sites and within operational areas to minimize the challenges associated with crowd control. Steven Harrison, the assistant director of emergency operations, planning and logistics for the Virginia Department of Health, further contributes that non-traditional dispensing modalities such as drive-through dispensing and institutional delivery can be used in conjunction with PODs to help reduce the number of citizens reporting to individual sites.17

In the event of a biological disease outbreak, adequate space for triage, dispensing, patient care, and counseling should be provided when possible.18 Within the POD, maintaining order through validated procedures would be necessary to ensure efficiency and prevent secondary infections where applicable. Personnel working in the PODs must be provided for in terms of their own health and safety through the provisioning of PPE and security as needed.

A discussion of CHCs as points of dispensing for countermeasures and mass prophylaxis is not a new idea and several centers have already instituted agreements with officials to serve in this capacity.19 Again, CHCs are placed in a location that deliberately and thoroughly considers the level of accessibility to the target population. Many are in urban areas, are public transit accessible (where available), are proximate to their target populations, and most offer transportation services to fill the gap.

According to Dr. Joseph V. Saitta, the emergency services coordinator for the Rappahannock Area Health District in Virginia, using the BERM model to calculate PODs and the number of people needed to staff them, would demonstrate that in many communities the typical health department could not do it alone. The health department would commit both its own staff and all available volunteers that it could muster from the Medical Reserve Corps, the regional Volunteer Organizations Active in Disaster (VOAD), and the area’s Community Emergency Response Teams (CERT) to the incident. Depending on the nature, magnitude, and location of an outbreak, it is conceivable that a CHC might run a POD by itself, though the health department would make every attempt to provide staff or volunteers to help whenever possible.20

The commitment to act as a POD, however, is not a matter to be taken lightly and should be preceded with a discussion of responsibilities and expectations. To be successful, a POD must be well integrated in relevant incident command systems as they will be reliant on these structures for resources and other types of support. If the CHC anticipates providing their own staff for such purposes, they should ensure that personnel are knowledgeable of the need for such measures, the threats that could surface, and the safety considerations that have been planned for on their behalf. It will require a trained staff that can appropriately communicate with patients to provide necessary information and manage patient flow. It will require an exercised triaging system that is merely a “good idea” at this early stage of development for many CHCs moving towards emergency preparedness. While just-in-time training may be provided, preparing staff in advance for this response role may convey the importance of their efforts and help to alleviate the concerns that researchers have shown as contributing to a worker’s unwillingness to respond.21 At a minimum, CHCs serving as PODs should
engage in continuous incident command training for new staff, refresher training for existing staff, and exercises when possible to assess the site’s capabilities and improve coordination in the community. Beyond these basics, personnel policies may need to be revised to encourage sick employees to stay home, well employees to report for duty, and all employees to feel secure during an incident. Clearly, sustained relationships and coordination with local health departments are the initial step for moving in this direction. Beyond these obvious partnerships, first responders as a whole would need to be educated on the role of the CHC-POD to appropriately direct citizens and provide support when needed.

Mass Casualty Care

The mass casualty care aspect of the *Public Health and Medical Preparedness Strategy* is an ambitious undertaking of the federal government and is envisioned to offer an “operational concept for the medical response to catastrophic health events that is substantively distinct from and broader than that which guides day-to-day operations.”

The main components of this enterprise, to date, include the Modular Emergency Medical System (MEMS), the National Disaster Medical System (NDMS), and the Medical Reserve Corps (MRC).

The MEMS concept is based on the rapid organization of expandable patient care modules, and provides the structure and space to process up to 1,000 patients per day for each unit, ultimately expanding capacity and directing those in need to the appropriate care. The MEMS is intended for setup near local hospitals to manage the flow of patients in a systematic way to alleviate surge on area hospitals. The MEMS requires a staff of 500 persons per twelve-hour shift representing a variety of medical disciplines to operate at full capacity. It should also be noted that the MEMS has an important limitation of being “one practical approach to managing a major non-communicable incident.”

The NDMS on the other hand is a volunteer program implemented with the purpose of augmenting the nation’s medical response capability by assisting state and local authorities in dealing with the medical impacts of major peacetime disasters. Once activated, NDMS response personnel are federalized and are protected by the Federal Tort Claims Act (FTCA) for medical malpractice claims and have recognized credentials in any state.

Finally, the MRC is a community-based network of volunteers (similar to the NDMS) that is organized to “improve the health and safety of communities across the country by organizing and utilizing public health, medical, and other volunteers.” MRC units are largely composed of active medical personnel from area hospitals and healthcare systems and retired medical personnel who maintain their licenses and credentialing, among other professions. MRC units have been identified at the local and state levels as possible resources for meeting part of the staffing demands to operate the MEMS until, and if, federal resources can be deployed.

While these programs may be a practical response to a number of incidents these entities could in and of themselves cause a range of unintended consequences during a pandemic illness. For the most part these programs rely on volunteers, which could present a number of challenges. For example, John B. Delaney argues that the NDMS will be proven futile during a pandemic disease outbreak and urges the federal
government, knowing of the systems limitations, to stop propagating them as a resource. Specifically, he points out that long deployments away from family and intense patient contact coupled with responders’ fear for personal safety and their family’s well-being will be a major deterrent for these volunteers to volunteer.28 This argument should not be limited solely to NDMS. As a community resource, the MRC may be able to garner more support, but inevitably will see their resources drastically cut as well. Moreover, the counts for many of our emergency response assets may be inflated.29 The NDMS and MRC depend on volunteers to function, many of whom are being double-counted because they belong to more than one volunteer emergency support program like Community Emergency Response Programs or the Red Cross.30 The resource count for these systems could be further diminished during an emergency because of either an unwillingness to respond or an inability due to professional obligations in their own communities.

Pandemic by definition indicates that the response partners we would ordinarily expect to assist will be grappling with the same issues in their own communities.31 Activating personnel through NDMS or the MRC would be of limited use under the pandemic scenario without creating undue hardship in the practitioners’ originating community and/or facility; this, of course, assumes that there even is interest from the teams. These teams may be viable under many of the national planning scenarios, but would still struggle to quickly meet the staffing demands of the MEMS.32

By enabling CHC penetration, nurturing their emergency preparedness and response capabilities, and priming personnel for personal preparedness, CHCs can effectively and systematically help to alleviate surge pressures by acting as “alternate care sites” and tending to the needs of the “worried well” and/or “walking wounded.” In some instances, CHC medical practitioners could be prepared to rapidly fill a number of the positions that the MEMS would need to function without compromising any other locales, a concept more generally referred to as “community-based surge capacity.”33

In 2007, the Office of the Press Secretary announced that it is the policy of the United States to ensure a “rapid public health and medical response that marshals all available national capabilities and capacities in a rapid and coordinated manner.”34 CHCs, as federally-funded entities, may be obligated to support response efforts by federal mandate. CHCs located within those jurisdictions having reformed their statutes per the Model State Emergency Health Powers Act (MSEHPA)35 may be obligated to support response efforts by state mandate.36 As providers of primary care services, CHCs may have a regulatory obligation, at the very least, to treat their rolls of existing patients.37 Finally, those CHCs holding recognition as the sole medical provider in their respective communities may confront an overwhelming ethical obligation to provide care. Dr. D. Bradley Drawbaugh, executive director of Highland Medical Center in Virginia, further contributes that the healthcare system has been entrusted by the public to be prepared; when you betray that trust, it takes a long time to earn it back. “I’ve seen firsthand – the jobs lost and careers ruined when emergency preparedness is an afterthought. Crisis management is never good management when it commences during a crisis.”38

In the end, the will to respond is a personal decision – volunteer or otherwise. However, by actively engaging in emergency management planning as a function of the workplace, thoroughly considering the needs of employees to execute response plans, and demonstrating appropriate provisions through incident command system
integration, a CHC may be able to provide the assurance needed to compel their practitioners to respond.

**Community Resilience**

Perhaps the most significant contribution CHCs can offer during a catastrophic health event would be promoting community resilience in the sphere of public health and medical preparedness. By providing citizen education, coordinated risk communications, community outreach, and basic medical services, CHCs as an organized force spanning the nation could assure the worried well, tend to the walking wounded, and support the special needs populations.

The worried well can unknowingly increase infection rates by inadvertently exposing themselves and others by seeking unnecessary treatment. CHCs could serve as triage centers or alternate care sites for the walking wounded, consequently helping to manage the demand for services on area hospitals. Finally, CHCs could continue to provide the medical home their vulnerable populations have come to know and trust. Without adequate attention, each of these groups could needlessly overwhelm the lifesaving capacities that only the more advanced treatment facilities may be able to offer.

A recent survey administered in Kentucky revealed that a doctor’s office was the most frequently mentioned resource individuals would turn to for health information. While a CHC is unlikely to play a direct role in the development of needed educational and informational materials, it is prudent to embrace them as critical partners for the dissemination of such information. Dr. Karen Remley, the state health commissioner for the Virginia Department of Health, established that citizens trust their primary care physicians as the primary source of information. She continued, “We [the state] want primary care physicians to trust us as the primary source of information,” but as of yet the appropriate communication channel is obscure. Since the public-private divide permeates healthcare as it does most of the nation’s critical infrastructure, resolution of this issue may continue to be elusive. In the meantime, however, it is a reasonable starting point to connect with the CHCs. State and federal agencies may utilize any number of information networks to keep citizens informed; in the end, however, the public will want this information confirmed by their medical providers.

Ultimately, CHCs may prove to be the crutch of the community by supporting the whole spectrum of emergency management activities to minimize the economic impacts and the loss of life due to a biological disease outbreak or other public health emergency.

**THE CASE FOR IMPLEMENTATION**

Strategically enlarging the Health Center Program and its preparedness capabilities is a dual-purpose investment: enhancing emergency preparedness by supporting the objectives identified in HSPD-21 and creating greater social equity. This section discusses the Health Center Program through a values lens and specifically considers the principles of health, justice, transparency, and accountability.

Deborah Stone offers the goals of equity, efficiency, security, and liberty as crucial objectives of policy analysis. She warns us however, that “these values are ‘motherhood issues’: everyone is for them when they are stated abstractly, but the fight begins as soon as we ask what people mean by them.” For example, ensuring security often comes at
the price of liberty; protecting liberty can equate to diminished security; and promoting equality and security through redistributive policies may, from perspectives, occur at the expense of efficiencies.

This strategy is an opportunity to move toward enhanced security while keeping infringements on liberty as minimal as possible and moving down the path already envisioned and authorized in HSPD-21 and the Public Health Security and Bioterrorism Preparedness and Response Act of 2002, respectively. It is the opportunity to promote equality while relying on the existing administrative infrastructure that has made proven contributions to enhancing social equity and has been documented as possibly more efficient than some of the alternatives. Finally, the benefits, especially during a pandemic, would be more evenly distributed among the population as compared to many of the existing initiatives. According to George J. Annas and others:

Both history and current events demonstrate the need for a new, positive paradigm for pandemic preparedness, one that harnesses the talents of all Americans to take effective action to protect the health of all, instead of punishing those who fall ill. This new paradigm should be based on four fundamental principles: Health, Justice, Transparency, and Accountability.

The Health Center Program by creation and mission already exudes these principles. The contributions that they make to our nation’s healthcare and the manner by which they are organized and regulated lend themselves to being in near perfect harmony with this paradigm.

Health and Justice

Public discourse and academic research has established that the United States is in the midst of a healthcare crisis with the number of persons presenting without medical insurance reaching dangerously high levels and impacting service delivery and the accessibility of basic healthcare. This has created comparatively greater hardship for racial and ethnic minorities in this country, as was substantiated by an Institute of Medicine report documenting inequities in medical treatment among these groups. Even when these individuals have the same health insurance and similar access to a health care provider as non-minorities, research indicates that minorities tend to receive a lower quality of healthcare (e.g. not receiving the needed services, receiving less desirable services) than whites. Much of the argument points to the need to socialize healthcare in some form or another to reduce healthcare costs, minimize or eliminate health disparities, and provide universal access to residents of the United States. While some individuals may not view the public financing of healthcare as desirable, the social and economic costs of inequities in health are a cost shared by all. For example, the Centers for Disease Control and Prevention indicates that costs associated with chronic diseases – the most common and the most costly – account for more than 70 percent of the $1 trillion in U.S. healthcare expenditures each year. Chronic diseases are largely preventable diseases. Therefore, reductions in the prevalence of disease, in any population, should in turn accrue healthcare cost savings and other benefits for all. As it happens, health disparities research demonstrates vulnerable populations suffer a disproportionate share of the chronic disease burden.

As a federal program, the CHCs have made significant contributions in this domain. “Health centers are a principle strategy for anchoring accessible, high quality primary
health care in pervasively poor and uninsured communities that, without such investment, could not hope to independently attract and support sufficient private medical care practices."

The same factors of quality health care accessibility that have contributed to health disparities in racial and ethnic minorities will similarly surface during a public health crisis but could potentially result in higher consequences for these vulnerable populations and the medical infrastructure as a whole. The need to systematically and concretely conduct emergency planning to meet the needs of the socially disadvantaged has been advocated by numerous researchers and emergency management professionals and is captured in a distinct course offered through FEMA’s Emergency Management Institute. Fortunately, a niche profession of special-needs emergency planners has surfaced to provide leadership in this domain. Special-needs populations can be defined as “groups whose needs may not be fully addressed by traditional service providers or who feel they may not comfortably or safely access and use the standard resources offered in disaster preparedness, response, relief, and recovery.” Planning for special-needs or vulnerable populations has received significant attention recently as evidenced by its inclusion in the Congressional Research Service Report, Public Health Medical Preparedness and Response: Issues in the 110th Congress and the Homeland Security Programs Grant (HSPG) guidance where it receives mention as an “area of paramount concern.”

A large portion of these special-needs populations comprise CHCs’ target populations and vice versa. Through expansion of the Health Center Program and dedicated funding to create robust emergency management programs within CHCs, the administration can make substantial improvements in healthcare accessibility and cost, reduce health disparities, and positively improve the nation’s public health and medical preparedness. With dedicated support, CHCs could be well positioned to be fundamental agents for these groups during a public health crisis and other emergencies.

During non-emergency operations the provision of primary and preventive healthcare to underserved populations saves the system money in both the short and long term. CHCs already save the national health care system between $9.9 billion and $17.6 billion a year by helping patients avoid emergency room visits through better use of preventive services, but an additional $18 billion still aggregates each year from emergency room visits that could have and should have been managed through health center providers. The expectation during emergency operations is that care would be more widely available to not only the special-needs populations, but to the greater population as a whole through the systematic management of the afflicted and the concerned, ultimately ensuring that those in need of specialized care will have an improved chance of access by preventing and mitigating infection and subsequent surge up front. Even without significant CHC expansion, improved coordination and integration could augment medical preparedness and response capabilities.

While risk-based programs for emergency management funding like the Urban Areas Security Initiative (UASI) or the Metropolitan Medical Response System (MMRS) are clearly warranted on some level, emergency management competencies should be established and maintained in a manner that provides a basic level of security for all.
Transparency and Accountability

As federally qualified health centers (FQHC), regulated by the Bureau of Primary Health Care (BPHC) in the Health Resources and Services Administration (HRSA) of the U.S. Department of Health and Human Services (HHS), the administrative infrastructure and accountability mechanisms are already in place to groom CHCs for an active and measurable role in public health and medical preparedness. “The medical care services furnished by health centers are subject to extensive federal requirements, and the quality of care is carefully monitored in accordance with federal clinical care standards.”

Every three to five years, FQHCs must reapply for funding through “Service Area Competitions” managed and administered by HRSA. Within HRSA, a number of offices impact the overall administration of community health centers, but the greatest concentration of oversight and program guidance is directed through BPHC. Meanwhile, the Healthcare System Bureau, within HRSA, is dedicated to “the facilitation of the development of state, territorial, and municipal preparedness programs to enhance the capacity of the nation’s hospitals and other healthcare entities to respond to mass casualty incidents caused by terrorism and other public health emergencies,” and is further coordinated at a higher level through the Office of the Assistant Secretary for Preparedness and Response (ASPR) located within HHS. In their article, Emergency Management Planning as Collaborative Community Work, Wendy A. Shafer and others warn that strictly top-down reforms “could fail to effectively leverage (or perhaps take notice at all of) locally based resources that could play useful, and perhaps critical roles in given emergency operations.” Perhaps the viability of CHCs as an integral component of public health and medical preparedness was somehow lost on this large, complex bureaucracy. Nonetheless, this bureaucracy is precisely the regulatory structure that is needed to assure transparency and accountability for any country-wide preparedness initiative.

Another useful component of the Health Center Program’s administrative infrastructure is the Primary Care Association (PCA). Each state has a PCA at the service of member centers to provide training and technical assistance. HHS may be able to coordinate preparedness initiatives through the PCA to streamline the funding process, ensure consistency across programs, and actually measure progress in a meaningful way and on a scale that would support strategic planning.

BARRIERS TO IMPLEMENTATION

At this time, the BPHC has imposed a relatively ambiguous framework for emergency management programs in health centers. They mandate all-hazards preparedness yet hamper such efforts by maintaining barriers that essentially bar CHCs from progressive integration with the system. These barriers largely include inadequate funding, a restrictive regulatory environment, and ground-level integration challenges.

Policy Information Notice (PIN) 2007-15: Emergency Preparedness and the Potential Role of Health Centers in Community Response, acknowledges the health centers’ ability to support homeland security efforts and encourages them to understand and institutionalize NIMS and understand the National Response Framework (NRF) while recommending typical emergency management concepts, e.g., interagency
coordination, interoperability, proactive planning, risk communications, etc.\textsuperscript{64} Unfortunately, \textit{PIN 2007-15} stands to serve a much more symbolic, rather than operational, framework because funding for such preparedness activities is nominal, if existent at all. According to a recent study conducted by the National Association of Community Health Centers (NACHC), of the $1.54 billion awarded for public health and healthcare emergency management programs nationwide in 2006, only 0.7 percent or $11.1 million was awarded to PCAs and/or CHCs.\textsuperscript{65} A few CHCs have been successful obtaining funding and support through the risk-based programs mentioned earlier, the CDC’s Public Health Emergency Preparedness (PHEP) Cooperative Agreement, and the Hospital Preparedness Program (HPP) which specifically prompts inclusion of CHCs in planning efforts. In Virginia, at the time of writing, CHCs have only just been formally approached regarding participation in the HPP. Before funding becomes a discussion topic, however, Virginia’s twenty-three CHCs, representing 129 service delivery sites,\textsuperscript{66} will need to engage in extensive fact-finding accompanied by a presumably lengthy induction with one or more of the state’s six Regional Healthcare Emergency Planning Committees. With $3.5 million of the $11.1 million in funds (described above) being concentrated in California,\textsuperscript{67} it is safe to assume the discretionary distribution of these funds by each state has left more than a few CHCs planning in a vacuum.

To complicate matters, the subsequent PIN issued by the BPHC, \textit{Policy Information Notice 2007-16: Federal Tort Claims Act (FTCA) Coverage for Health Center Program Grantees Responding to Emergencies}, advises that FTCA coverage for health center employees and certain contractors providing services during emergencies on behalf of the health center, is limited to adjacent jurisdictions and those areas described within the center’s approved section 330-grant “scope of project” which specifies very specific sites, services, providers, target population, and service areas, but may be amended on a case-by-case basis.\textsuperscript{68} In essence, this means a CHC is restricted from mobilizing to respond to an incident. This policy gives little assurance to the health center attempting to integrate into this greater emergency management network, which relies on the use of mutual aid agreements (the sharing of \textit{staff} and other resources) and commends them as a best practice.

On the other hand, \textit{Program Information Notice 05-19: Federal Tort Claims Act Coverage for Deemed Consolidated Health Center Program Grantees Responding to Hurricane Katrina}, established the precedent of FTCA coverage flexibility during a catastrophic incident by permitting some health centers to provide services at temporary locations with looser restrictions during Hurricane Katrina.\textsuperscript{69} While this PIN may provide a hint as to how things might unfold during an emergency, it is no more than a hint. This uncertainty is detrimental to a rigorous emergency management program that in theory stresses \textit{all-hazards preparedness} and is evaluated by conducting \textit{realistic} exercises.

The Homeland Security Exercise and Evaluation Program (HSEEP) was conceptualized in response to the directive established in HSPD-8 to establish a comprehensive training program to meet the national preparedness goal that also includes training for the nation’s first responders, officials, and others with major event emergency management roles\textsuperscript{70} and provides a robust model for creating and sustaining a progressive capabilities-based training and exercise program utilizing the Target Capabilities List (TLC).\textsuperscript{71} Yet the investment to appropriately embrace this methodology,
under the described circumstances, is difficult to justify. CHCs could support a variety of capabilities identified in the TLC. Some of the more obvious capabilities include responder safety and health, mass care, emergency triage and pre-hospital treatment, medical surge, medical supplies management and distribution, and mass prophylaxis, but could extend to fatality management as well. However, the amount of time and money that would be needed just to navigate these complex partnerships and interactions is daunting in and of itself; this of course does not even begin to encompass the commitment to properly train and exercise staff in these capabilities utilizing the HSEEP framework. Most CHCs do not receive any direct federal funding for emergency management activities and, in 2006, only an estimated twenty states had planned to fund emergency preparedness and response programs in CHCs.72

According to Robert Housman and Ed Bethune, post 9/11 preparedness mandates are smoking guns: “vulnerability assessments that offer long lists of potential risks, large numbers of documented security flaws, and large price tags to close these gaps.”73 Tort claims are being litigated right now clarifying the “duty to prepare” and the “duty to respond.”74 Steven Gravely, J.D., M.H.A., of the Joint Subcommittee Studying the Feasibility of Offering Liability Protections to Health Care Providers Rendering Aid During a State or Local Emergency in Virginia, warns of multiple suits in Canada against health care providers and the government stemming from the failure to use infection control measures during the SARS outbreak and similar suits against providers in Louisiana alleging the failure to evacuate in a timely manner in response to Hurricane Katrina.75 Other claims arising from these incidents include the failure to prepare, the failure to have emergency power, the failure to utilize realistic planning assumptions, and the failure to anticipate flooding and relocate generators accordingly.76 In light of these allegations, it could be argued that the BPHC mandates have left a paper trail for tort claims in those CHCs that fail to comply with the emergency management expectations outlined in the various PINS and by other relevant regulatory agencies. Ultimately, finger pointing could make its way back to the federal government in these cases because (1) the PINs arguably contradict the emergency management fundamentals of resource support through mutual aid agreements and consequently hinder the full exploration of CHCs as potential resources for incident management; and (2) funding for the implementation of comprehensive emergency management programs in CHCs often appear to be unavailable, insufficient, or amassed by other entities whom in turn may be either unaware of or unconcerned with the role of CHCs. After all, the Health Center Program is a federal initiative.

Challenges in the CHC

Beyond the larger policy issues, CHCs may have to overcome challenges in their localities as well. For a CHC to be successful in the emergency preparedness and response realm, it must be integrated in the local emergency management network. Yet achieving this needed state of integration is not always an easy feat.

Currently, the main push for emergency preparedness and response in CHCs revolves around the drafting of the EOP. While it is clear that EOPs and the process of developing the plan is the foundation of emergency management programs, it is also becoming clear that this activity in and of itself may not provide the results intended. Sang O. Choi and Ralph S. Brower conducted a study under the assumption that appropriate persons
tasked with emergency management responsibilities were knowledgeable of their relevant EOPS, only to discover that this assumption was far from the truth. “Surprisingly, the majority (60.0%) of all organizations appear to understand the plan only a little.”77 Louise Comfort and Naim Kapucu add additional concern when they assert that “most public agencies have emergency plans, but they are not always current” (311).78 Moreover they've found integration inconsistencies with the plans themselves.

Although some private companies and nonprofit organizations such as hospitals and schools have emergency plans, they often are not integrated with those of the public agencies to provide a comprehensive plan for a community, much less multiple communities in an affected region.79

Without the flexibility to truly integrate, CHCs may easily become stuck in the planning mode and never delve any deeper into the areas where they can make the greatest impact: personal preparedness initiatives and training to ensure an adequate and “ready” workforce capable of supporting biosurveillance efforts, countermeasure distribution, mass casualty care, and the provisioning of community education and risk communications to strive for the best outcome in their communities under the worst-case scenarios.

FEMA offers a long list of recommended activities for NIMS implementation in hospitals and healthcare systems including, but not limited to:

- The adoption of NIMS, continuous efforts to provide NIMS/ICS training, and the utilization of exercises to determine corrective actions;
- Promoting and supporting mutual aid agreements, the maintenance of inventoried response assets, and the use of integrated Multi-Agency Coordination Systems (MACs);
- The implementation of public information systems and all-hazards exercise programs.80

Without dedicated personnel and funding, these activities will be extremely difficult for a CHC to implement and as it stands now, every dollar spent on preparedness is a dollar taken away from clinical programs.

It should not be assumed that a Local Emergency Management Committee (LEMC) has the means and foresight to include CHCs in preparedness activities and further the structure and incentive to maintain and report such progress. Many jurisdictions are overwhelmed by the challenge of achieving even basic NIMS compliance in their agencies. A study by the Colorado Community Health Network (the Colorado PCA) found that of those CHCs surveyed, those not involved in community planning had actually been rejected by the community with one respondent reportedly being told ‘We’ll call you if we need you’.81 In contrast to this interaction, Steve Harrison asserts that close collaboration and mutual understanding of response roles is not simply needed, but required, to effectively resolve many of the issues necessitating consideration prior to and during a public health incident.82

Creating an emergency management program that is responsive to the needs and particular nuances of the individual CHC is a tall order. The resources and capabilities of each one can be quite varied. Some of the rural health programs, for example, may not have the staff to attend long trainings without completely shutting down their
operations. Meanwhile, as the sole healthcare provider within a particular area, their facility may be the one that could benefit the most from these interactions. With cuts in Medicaid expenditures, resulting in a higher number of uninsured people seeking services, more centers struggle with their day-to-day finances, which ultimately constrains their ability to effectively undertake emergency management planning and all that a quality program entails. The case of the Eastern Shore Rural Health System (ESRHS), the most progressive CHC in terms of emergency management in Virginia, demonstrates these tensions.

In Virginia, the Eastern Shore Rural Health System (ESRHS) operates five community health centers along the eighty-mile stretch of land between the Chesapeake Bay and the Atlantic Ocean. With more than 50,000 residents, only one area hospital with 180 beds, and at least half of the population relying on ESRHS for their care, ESRHS partnered with their local health department as early as 2002 to begin emergency planning. They developed relationships with the local hospital and area emergency management personnel and eventually formalized these partnerships through the creation of the Eastern Shore Disaster Preparedness Coalition. ESRHS has been very active with the coalition and initially attempted to support community exercises with each of their health centers every year, but it soon became apparent that the time commitment to plan and coordinate these events was too much and that ESRHS could generally only permit one center to participate per year. Since ESRHS is very well integrated with their local emergency management network and is fairly confident in their response roles through their local ICS, the abated exercise schedule is less of a concern than the possibility of losing contact during an incident.

The ESRHS is probably the most capable CHC in the state (at this point) for supporting incident response and they are actually located quite close to the Norfolk UASI jurisdictions. In fact, roughly 41 percent or 2,882 CHC service delivery sites are located within candidate urban areas queried by the Department of Homeland Security as part of their overall risk methodology (see Appendix for CHC counts by state and relevant Metropolitan Statistical Area). Yet FTCA guidelines would prevent them from quickly responding to an incident in most of the state’s UASI areas due to the coverage guidelines discussed previously.

RECOMMENDATIONS

In Biodefense for the 21st Century, the United States declared that it “will continue to use all means necessary to prevent, protect against, and mitigate biological weapons attacks perpetrated against our homeland and our global interests” [emphasis added]. The preceding discussion points to a means that is clearly necessary. Supporting the Public Health and Medical Preparedness Strategy to the greatest extent possible, however, hinges on a few critical recommendations:

Remove Regulatory Barriers

The National Strategy for Homeland Security states that the nation must develop “interconnected and complementary homeland security systems that are reinforcing rather than duplicative and that ensure essential requirements are met.” In 2005 DHS announced the national priorities, in the Interim National Preparedness Goal, one of
which includes the goal of strengthening “medical surge and mass prophylaxis capabilities by establishing emergency-ready public health and healthcare entities” and another calling for “expanded regional collaboration through mutual aid agreements and assistance compacts.” These goals point to the development of specific capabilities and specify the means for getting there. Meanwhile, CHC participation is limited because the current guidelines for granting medical malpractice insurance through the Federal Tort Claims Act (FTCA) have all but ensured their paralysis.

First and foremost, FTCA coverage must be determined in a way that supports rather than contradicts emergency management programs. In emergency management, mutual aid agreements and memorandums of understanding provide the framework for requesting resources during an incident response. In light of these regulations, CHCs may provide supplies and equipment but are quite restricted in the use of personnel. This equates to an underutilized asset of more than 36,900 medical care providers, more than 2,700 mental health providers, and nearly 105,000 personnel in total across the U.S., providing patient services. Despite this barrier, health centers treated more than 19,000 evacuees in Louisiana and nearly 18,000 in Mississippi after Hurricane Katrina – nearly 80 percent of whom did not have health insurance.

At a minimum, FTCA coverage should be designated in a way that permits staff-sharing between centers and their temporary sites or provides specific assurance that coverage will be extended under certain circumstances. For example, the guidelines could state that coverage will be provided during a state declared disaster for intrastate practitioners responding to a Type-2 Incident or coverage will be extended if WHO Pandemic Phase 5 is signaled. This will facilitate preparedness at the local and state levels by instantly boosting medical response capabilities and will enhance preparedness at the national level by creating the flexibility and assurance for CHCs to begin integrated training and exercise programs with other stakeholders. Those CHCs formerly rejected by their LEMC, or those residing in inactive jurisdictions, could pursue alternative partners from a broader jurisdictional perspective and ultimately pursue NIMS compliance where formerly their success would have been predicated on their immediate community’s interest in and ability to integrate them. CHCs and their respective PCAs could then begin to link into Emergency Operations Centers (EOCs) and other multiagency coordination systems and vice versa with greater efficiency. Ideally, the NDMS model of FTCA coverage and recognized credentialing across state lines should be extended to CHC personnel to promote all-hazards preparedness. To reiterate, FTCA coverage for providers will only be extended when services provided are consistent with those identified in the CHCs’ “scope of project,” including sites, services, service areas, and target populations (target populations generally meaning medically underserved and/or vulnerable populations). Ironically, the threat of pandemic influenza and the looming medical response shortage raises the probability that every citizen will be medically underserved. During a pandemic event, CHC personnel (after stabilizing their own communities) perhaps could provide temporary assistance through partner CHCs in those jurisdictions still struggling with the incident.

Enable CHC Growth to Ensure an Evenly Distributed Public Health Response
The Institute of Medicine praised health centers for providing care that is “at least as good as, and in many cases superior to, the overall health system in terms of better quality and lower costs.”93 Moreover, Jack Hadley and Peter Cunningham suggest that CHC expansion reduces the reliance on more expensive hospital resources, ultimately improving delivery system efficiency and offsetting the costs of expanding CHC capacity.94 Aaron Katz and others describe CHCs as well situated in some communities to be the first line of response during public health emergencies and warned that reductions in public health infrastructure investments could erode newfound capacity in community preparedness.95 The list of various reports and research supporting CHCs goes on and on.96 Denise Santiago and Anke Richter, however, caution against the reliance on “dual-use functionality” for public health preparedness pointing to the obvious assumption that the concept assumes that there were sufficient resources for “single use.”97 The demand for services during a public health emergency will certainly overwhelm existing capabilities. Even future infrastructure development will falter during a WMD attack or biological disease outbreak. Yet until health care accessibility provides for a more equitable distribution there should be little reservation in moving forward on capacity building. “Congress and the agencies must address the fact that many critical systems on which the nation will rely during future emergencies are already overstrained. This applies in particular to health care and public health sectors.”98

Use the Administrative Infrastructure to Promote Health, Justice, Transparency, and Accountability

PCAs, the state-level associations for CHCs, receive funding authorized under the Public Health Service Act to provide “assistance to Statewide organizations in the development and delivery of comprehensive primary health care service in areas that lack adequate numbers of health professionals or have populations lacking access to primary care services” and “technical and non-financial assistance to community-based providers of comprehensive primary and preventive care for underserved and vulnerable populations.”99

Training and technical assistance for emergency management is quickly being added to the list of services provided through the PCA, but the breadth and quality of those programs, if implemented, will largely be dependent on their level of funding. Costly consultants can easily be brought in for a quick presentation on risk communications or personal preparedness. The challenge though is connecting those needs to the CHC and the CHC to the emergency management network and the resources to the CHC so that those needs result in implementation actions. None of this can be accomplished in a significant way if done in isolation.

The Association of State and Territorial Health Officials (ASTHO) described the following roles that PCAs could use to facilitate emergency preparedness and response:

- Represent CHCs at state emergency planning tables;
- Provide training and technical assistance to CHCs as they develop their emergency operations plan;
- Serve as the communication link between CHCs and government resources.100
A more recent report by ASTHO describes partnerships forged between some state health agencies, PCAs, and CHCs to improve emergency preparedness. Some of these efforts include, but are not limited to: defining emergency response roles in California; enhancing surge capacity in Massachusetts, resource integration in Arkansas, emergency preparedness training for health centers in Maine, and infectious disease control in New York; and building health care coalitions in the state of Washington. These successes should certainly serve as models for improving coordination and integration at the state and local levels.

Working through the PCA could be a means to facilitate the coordination and execution of many public health and medical preparedness activities through a more manageable program design. It would create another layer of accountability and positions the CHC and the PCA to take advantage of pull and push strategies for creating awareness and improving integration at the local, regional, and state levels.

CONCLUSION

If CHCs are to be contributing partners in public health and medical preparedness, funding must be made available that supports a minimum level of preparedness for all centers. With more than 36,900 medical professionals across the nation to prepare for emergency preparedness, the funding is needed and has the potential to engage a previously untapped resource.

As potential PODs for countermeasures and mass prophylaxis, certain personnel will need to take the full spectrum of NIMS and ICS training and engage in community and/or state exercises. To effectively contribute to biosurveillance or mass casualty care, certain personnel will need bioterrorism training and the opportunity to participate in relevant drills. Finally, to be a key player in community resilience, CHCs need the recognition and support from the emergency management network across agencies and all levels of government.

Even though coordination, collaboration, and communication are the mantras of emergency management, this networked vision has yet to be achieved on a large scale. Public health has only recently joined the ranks of the first responders and the titling of whom meets this classification is still gray for many even within the emergency management and homeland security professions. Including CHC representation on the occasional advisory committee without soliciting feedback, without appropriating funding to them, and without publicly acknowledging their role will do little to move the relationship forward. “Our entire response framework is predicated on a coordinated response that spreads across jurisdictions and up jurisdictional channels as resources are exhausted.” Outside of local EMS resources, public health is not well organized to contribute to this model and certainly not in the capacity envisioned by the Public Health and Medical Preparedness Strategy.

Expanding the Health Center Program and embracing these entities as critical partners in the Public Health and Medical Preparedness Strategy is a viable strategy by first striking a reasonable balance between many of our contending values, and second by staying within our comfort zone in terms of incremental policy change by relying on existing administrative infrastructure and expanding capabilities rather than creating new entities to achieve them.
The entities we do have (i.e., NDMS, MRC) cannot be held accountable to meet FEMA’s training and exercise standards nor the actual response needs outlined in the nation’s preparedness architecture. Hospitals are already running at or beyond capacity. According to a recent real-time congressional survey of Level I Trauma Centers, conducted by the Committee on Oversight and Government Reform, none of the hospitals surveyed had enough critical care capacity or inpatient beds available to absorb a sudden influx from a mass casualty event (the “less severely injured” were included in the counts). It is quite possible that improved performance could have been realized had those “less severely injured” individuals been considered for treatment at nearby CHCs. Health departments have missions and responsibilities that delve into a wide array of programs, some preparedness related and many others not. Since these agencies are generally understaffed themselves, consideration must be given to other resources that are well-positioned to assist them in their preparedness and response efforts. Private physicians, medical centers, clinics, and every other healthcare system in existence should be incorporating emergency management programs into their operations to address those areas identified in HSPD-21. Unfortunately many of those entities do not generally have the bureaucratic structure in place to ensure transparency and accountability. When they do, their distribution does not generally reflect a system that promotes health and justice; if it did, CHCs would not exist.

According to HRSA’s Elizabeth Duke “health centers have been identified by the OMB as one of the federal government’s most successful programs.” Through a thoughtful revisioning that broadens the program’s scope to include strategic emergency planning, CHCs – with support – can build on what they already do well to augment our nation’s public health and medical preparedness capabilities.

This article is not intended to minimize the progress made over the past few years or to imply that CHCs have gone completely unnoticed – some are very well integrated and funded in their particular communities. Further, it is not intended to acclaim the Health Center Program as the sole solution to the Public Health and Medical Preparedness Strategy. The goal is to highlight the untapped resources that, through the proper attention to funding and development, can enhance the nation’s public health and medical preparedness. CHCs can provide biosurveillance in the populations that may be the first to signal a public health emergency, by serving as PODs in those areas that that are closest to special needs populations, by supporting mass casualty care efforts by mitigating surge at the onset and providing a supply of competent professionals dedicated to the public interest, and ultimately ensuring community resilience by leveraging their existing capabilities and relationships to ease their communities through a public health catastrophe. “It is the policy of the United States to plan and enable provision for the public health and medical needs of the American people in the case of a catastrophic health event through continual and timely flow of information during such an event and rapid public health and medical response that marshals all available national capabilities and capacities in a rapid and coordinated manner.” CHCs can be, should be, and may be front line public health responders whether they are prepared or not.

Is your Community Health Center Prepared?
Karen M. Wood serves as the emergency preparedness and response coordinator for the Virginia Community Healthcare Association in Richmond, Virginia. Previously, she worked on special projects for the Center for Homeland Defense and Security as a research associate/intern through the Homeland Security and Defense Education Consortium. Wood holds a bachelor of science from Virginia Commonwealth University and a master’s in public administration from Virginia Tech. She may be reached at karen1wood@hotmail.com.

Any opinions, findings, and conclusions or recommendations expressed in this publication are those of the author and do not necessarily reflect the views of the Virginia Community Healthcare Association.

NOTICE OF CORRECTION: Page 12 (the second paragraph under the heading Barriers to Implementation) has been modified to remove information appearing in the original publication of this article. The author’s personal communications with professionals from the New Jersey, Missouri, and Michigan Primary Care Associations were cited incorrectly.
### APPENDIX

#### CHC Prevalence in Candidate Urban Areas under the FY 2008 UASI Program

<table>
<thead>
<tr>
<th>State</th>
<th>Candidate Urban Area by Metropolitan Statistical Area</th>
<th>Counties and Cities Selected for Query</th>
<th>CHC Counts</th>
</tr>
</thead>
<tbody>
<tr>
<td>CA</td>
<td>Los Angeles-Long Beach-Santa Ana Area</td>
<td>Alameda County</td>
<td>134</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Contra Costa County</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Marin County</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>San Benito County</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>San Francisco County</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>San Mateo County</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Santa Clara County</td>
<td></td>
</tr>
<tr>
<td></td>
<td>San Francisco-San Jose-Bay Area</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>DC</td>
<td>Washington-Arlington-Alexandria, DC-VA-MD-WV Area</td>
<td>All Jurisdictions</td>
<td>45</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>IL</td>
<td>Chicago-Naperville-Joliet Area, IL-IN-WI</td>
<td>Cook County</td>
<td>320</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Dekalb County</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>DuPage County</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Grundy County</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Kane County</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Kendall County</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Lake County</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>McHenry County</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Will County</td>
<td></td>
</tr>
<tr>
<td>IN</td>
<td>Chicago-Naperville-Joliet Area, IL-IN-WI</td>
<td>Jasper County</td>
<td>8</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Lake County</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Newton County</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Porter County</td>
<td></td>
</tr>
<tr>
<td>MD</td>
<td>Washington-Arlington-Alexandria, DC-VA-MD-WV Area</td>
<td>Calvert County</td>
<td>15</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Charles County</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Frederick County</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Montgomery County</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Prince George's County</td>
<td></td>
</tr>
<tr>
<td>NJ</td>
<td>Newark Area</td>
<td>Bergen County</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Essex County</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Hudson County</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Hunterdon County</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Middlesex County</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Monmouth County</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Morris County</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Ocean County</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Passaic County</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Somerset County</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Sussex County</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Union County</td>
<td>62</td>
</tr>
<tr>
<td>NY</td>
<td>New York-Long Island Area</td>
<td>Bronx County</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Kings County</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Nassau County</td>
<td></td>
</tr>
</tbody>
</table>
### CHC Prevalence in Candidate Urban Areas under the FY 2008 UASI Program

<table>
<thead>
<tr>
<th>Tier 1 Urban Areas</th>
<th>Counties and Cities Selected for Query</th>
<th>CHC Count</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>State</strong></td>
<td><strong>Candidate Urban Area by Metropolitan Statistical Area</strong></td>
<td><strong>NY</strong> New York-Long Island Area (continued)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Kings County</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Nassau County</td>
</tr>
<tr>
<td></td>
<td></td>
<td>New York County</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Putnam County</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Queens County</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Richmond County</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Rockland County</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Suffolk County</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Westchester County 283</td>
</tr>
<tr>
<td><strong>PA</strong></td>
<td>Newark Area</td>
<td>Pike County 0</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Austin County</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Brazoria County</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Chambers County</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Fort Bend County</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Galveston County</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Harris County</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Liberty County</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Montgomery County</td>
</tr>
<tr>
<td></td>
<td></td>
<td>San Jacinto County</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Waller County</td>
</tr>
<tr>
<td><strong>TX</strong></td>
<td>Houston Area</td>
<td>Alexandria City 20</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Arlington County</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Clarke County</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Fairfax City</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Fairfax County</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Falls Church City</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Fauquier County</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Fredericksburg City</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Loudoun County</td>
</tr>
<tr>
<td></td>
<td>Washington-Arlington-Alexandria, DC-VA-MD-WV Area</td>
<td>Manassas City</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Manassas Park City</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Prince William County</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Spotsylvania County</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Stafford County</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Warren County 7</td>
</tr>
<tr>
<td><strong>VA</strong></td>
<td>Washington-Arlington-Alexandria, DC-VA-MD-WV Area</td>
<td>Kenosha County 1</td>
</tr>
<tr>
<td><strong>WI</strong></td>
<td>Chicago-Naperville-Joliet Area, IL-IN-WI</td>
<td>Jefferson County 1</td>
</tr>
<tr>
<td><strong>WV</strong></td>
<td>Washington-Arlington-Alexandria, DC-VA-MD-WV Area</td>
<td>Jefferson County</td>
</tr>
</tbody>
</table>

**Tier 1 Total** 1,092
<table>
<thead>
<tr>
<th>Tier 2 Urban Areas</th>
<th>Counties and Cities Selected for Query</th>
<th>CHC Count</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>AR</strong></td>
<td>Memphis Area, TN-MS-AR</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Crittenden County</td>
<td>2</td>
</tr>
<tr>
<td><strong>AZ</strong></td>
<td>Phoenix-Mesa-Scottsdale Area</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Maricopa County</td>
<td>26</td>
</tr>
<tr>
<td></td>
<td>Pinal County</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Tucson Area</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Tucson County</td>
<td>54</td>
</tr>
<tr>
<td></td>
<td>Pima County</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Santa Ana-Anaheim-Irvine Area</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Orange County</td>
<td>9</td>
</tr>
<tr>
<td><strong>CA</strong></td>
<td>Sacramento-Arden-Arcade-Roseville Area</td>
<td></td>
</tr>
<tr>
<td></td>
<td>El Dorado County</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Placer County</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Sacramento County</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Yolo County</td>
<td>17</td>
</tr>
<tr>
<td></td>
<td>San Diego-Carlsbad-San Marcos Area</td>
<td></td>
</tr>
<tr>
<td></td>
<td>San Diego County</td>
<td>101</td>
</tr>
<tr>
<td></td>
<td>Riverside County</td>
<td></td>
</tr>
<tr>
<td></td>
<td>San Bernardino County</td>
<td>19</td>
</tr>
<tr>
<td><strong>CO</strong></td>
<td>Denver-Aurora Area</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Adams County</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Arapahoe County</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Broomfield County</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Clear Creek County</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Denver County</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Douglas County</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Elbert County</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Gilpin County</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Jefferson County</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Park County</td>
<td>45</td>
</tr>
<tr>
<td><strong>CT</strong></td>
<td>Hartford-West Hartford-East Hartford Area</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Hartford County</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Middlesex County</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Tolland County</td>
<td>42</td>
</tr>
<tr>
<td></td>
<td>Bridgeport-Stamford-Norwalk Area</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Fairfield County</td>
<td>31</td>
</tr>
<tr>
<td><strong>DE</strong></td>
<td>Philadelphia-Camden-Wilmington Area, PA-NJ-DE-MD</td>
<td></td>
</tr>
<tr>
<td></td>
<td>New Castle County</td>
<td>5</td>
</tr>
<tr>
<td><strong>FL</strong></td>
<td>Fort Lauderdale-Pompano Beach Area</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Broward County</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Palm Beach County</td>
<td>9</td>
</tr>
<tr>
<td></td>
<td>Jacksonville Area</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Baker County</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Clay County</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Duval County</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Nassau County</td>
<td></td>
</tr>
<tr>
<td></td>
<td>St. Johns County</td>
<td>7</td>
</tr>
<tr>
<td></td>
<td>Miami Area</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Miami-Dade County</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Monroe County</td>
<td>98</td>
</tr>
<tr>
<td></td>
<td>Orlando-Kissimmee Area</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Lake County</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Orange County</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Osceola County</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Seminole County</td>
<td>5</td>
</tr>
<tr>
<td>State</td>
<td>Candidate Urban Area by Metropolitan Statistical Area</td>
<td>Counties and Cities Selected for Query</td>
</tr>
<tr>
<td>-------</td>
<td>-----------------------------------------------------</td>
<td>---------------------------------------</td>
</tr>
<tr>
<td>FL</td>
<td>Tampa-St. Petersburg-Clearwater Area</td>
<td>Hernando County&lt;br&gt;Hillsborough County&lt;br&gt;Pasco County&lt;br&gt;Pinellas County</td>
</tr>
<tr>
<td>GA</td>
<td>Atlanta-Sandy Springs-Marietta Area</td>
<td>Barrow County&lt;br&gt;Bartown County&lt;br&gt;Butts County&lt;br&gt;Carroll County&lt;br&gt; Cherokee County&lt;br&gt;Clayton County&lt;br&gt;Cobb County&lt;br&gt;Coweta County&lt;br&gt;Dawson County&lt;br&gt;DeKalb County&lt;br&gt;Douglas County&lt;br&gt;Fayette County&lt;br&gt;Forsyth County&lt;br&gt;Fulton County&lt;br&gt;Gwinnett County&lt;br&gt;Haralson County&lt;br&gt;Heard County&lt;br&gt;Henry County&lt;br&gt;Jasper County&lt;br&gt;Lamar County&lt;br&gt;Meriwether County&lt;br&gt;Newton County&lt;br&gt;Paulding County&lt;br&gt;Pickens County&lt;br&gt;Pike County&lt;br&gt;Rockdale County&lt;br&gt;Spalding County&lt;br&gt;Walton County</td>
</tr>
<tr>
<td>HI</td>
<td>Honolulu Area</td>
<td>Honolulu County</td>
</tr>
<tr>
<td>IN</td>
<td>Cincinnati-Middletown Area, OH-KY-IN</td>
<td>Dearborn County&lt;br&gt;Franklin County&lt;br&gt;Ohio County</td>
</tr>
<tr>
<td></td>
<td>Indianapolis-Carmel Area</td>
<td>Boone County&lt;br&gt;Brown County&lt;br&gt;Hamilton County&lt;br&gt;Hancock County&lt;br&gt;Hendricks County&lt;br&gt;Johnson County</td>
</tr>
<tr>
<td>State</td>
<td>Candidate Urban Area by Metropolitan Statistical Area</td>
<td>Counties and Cities Selected for Query</td>
</tr>
<tr>
<td>-------</td>
<td>--------------------------------------------------------</td>
<td>---------------------------------------</td>
</tr>
<tr>
<td>IN</td>
<td>Indianapolis-Carmel Area (continued)</td>
<td>Marion County</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Morgan County</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Putnam County</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Shelby County</td>
</tr>
<tr>
<td></td>
<td>Louisville/Jefferson County Area, KY-IN</td>
<td>Clark County</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Floyd County</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Harrison County</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Washington County</td>
</tr>
<tr>
<td>IL</td>
<td>St. Louis, MO-IL Area</td>
<td>Bond County</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Calhoun County</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Jersey County</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Macoupin County</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Madison County</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Monroe County</td>
</tr>
<tr>
<td></td>
<td></td>
<td>St. Clair County</td>
</tr>
<tr>
<td>KS</td>
<td>Kansas City Area, MO-KS</td>
<td>Franklin County</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Johnson County</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Leavenworth County</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Linn County</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Miami County</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Wyandotte County</td>
</tr>
<tr>
<td>KY</td>
<td>Louisville/Jefferson County Area, KY-IN</td>
<td>Bullitt County</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Henry County</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Jefferson County</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Meade County</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Nelson County</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Oldham County</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Shelby County</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Spencer County</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Trimble County</td>
</tr>
<tr>
<td>LA</td>
<td>Baton Rouge Area</td>
<td>Boone County</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Bracken County</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Campbell County</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Gallatin County</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Grant County</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Kenton County</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Pendleton County</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Ascension Parish</td>
</tr>
<tr>
<td></td>
<td></td>
<td>East Baton Rouge Parish</td>
</tr>
<tr>
<td></td>
<td></td>
<td>East Feliciana Parish</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Iberville Parish</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Livingston Parish</td>
</tr>
</tbody>
</table>

CHC Prevalence in Candidate Urban Areas under the FY 2008 UASI Program

<table>
<thead>
<tr>
<th>State</th>
<th>Candidate Urban Area by Metropolitan Statistical Area</th>
<th>Counties and Cities Selected for Query</th>
<th>CHC Count</th>
</tr>
</thead>
<tbody>
<tr>
<td>LA</td>
<td>Baton Rouge Area (continued)</td>
<td>Pointe Coupee Parish</td>
<td>21</td>
</tr>
<tr>
<td></td>
<td></td>
<td>St. Helena Parish</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>West Baton Rouge Parish</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>West Feliciana Parish</td>
<td></td>
</tr>
<tr>
<td></td>
<td>New Orleans-Metairie-Kennar Area</td>
<td>Jefferson Parish</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Orleans Parish</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Plaquemines Parish</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>St. Bernard Parish</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>St. Charles Parish</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>St. John the Baptist Parish</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>St. Tammany Parish</td>
<td></td>
</tr>
<tr>
<td>MA</td>
<td>Boston-Cambridge-Quincy Area, MA-NH</td>
<td>Essex County</td>
<td>114</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Middlesex County</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Norfolk County</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Plymouth County</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Suffolk County</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Providence-New Bedford-Fall River Area, RI-MA</td>
<td>Bristol County</td>
<td>5</td>
</tr>
<tr>
<td>MD</td>
<td>Baltimore-Towson Area</td>
<td>Anne Arundel County</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Baltimore County</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Baltimore City</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Carroll County</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Harford County</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Howard County</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Queen Anne's County</td>
<td>55</td>
</tr>
<tr>
<td></td>
<td>Philadelphia-Camden-Wilmington Area, PA-NJ-DE-MD</td>
<td>Cecil County</td>
<td>1</td>
</tr>
<tr>
<td>MI</td>
<td>Detroit-Warren-Livonia Area</td>
<td>Lapeer County</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Livingston County</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Macomb County</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Oakland County</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>St. Clair County</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Wayne County</td>
<td>20</td>
</tr>
<tr>
<td>MN</td>
<td>Minneapolis-St. Paul-Bloomington Area, MN-WI</td>
<td>Anoka County</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Carver County</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Chisago County</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Dakota County</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Hennepin County</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Isanti County</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Ramsey County</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Scott County</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Sherburne County</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Washington County</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Wright County</td>
<td>49</td>
</tr>
<tr>
<td>State</td>
<td>Candidate Urban Area by Metropolitan Statistical Area</td>
<td>Counties and Cities Selected for Query</td>
<td>CHC Count</td>
</tr>
<tr>
<td>-------</td>
<td>------------------------------------------------------</td>
<td>---------------------------------------</td>
<td>------------</td>
</tr>
<tr>
<td>MO</td>
<td>Kansas City Area, MO-KS</td>
<td>Bates County</td>
<td>14</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Caldwell County</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Cass County</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Clay County</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Clinton County</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Jackson County</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Lafayette County</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Platte County</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Ray County</td>
<td></td>
</tr>
<tr>
<td>MO</td>
<td>St. Louis, MO-IL Area</td>
<td>Crawford County</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Franklin County</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Jefferson County</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Lincoln County</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>St. Charles County</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>St. Louis City</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>St. Louis County</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Warren County</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Washington County</td>
<td>56</td>
</tr>
<tr>
<td>MS</td>
<td>Memphis Area, TN-MS-AR</td>
<td>DeSoto County</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Marshall County</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Tate County</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Tunica County</td>
<td>4</td>
</tr>
<tr>
<td>NC</td>
<td>Charlotte-Gastonia-Concord Area, NC-SC</td>
<td>Anson County</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Cabarrus County</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Gaston County</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Mecklenburg County</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Union County</td>
<td>12</td>
</tr>
<tr>
<td>NH</td>
<td>Norfolk-Virginia Beach, Newport News Area, VA-NC</td>
<td>Currituck County</td>
<td>0</td>
</tr>
<tr>
<td>NY</td>
<td>Albany-Schenectady-Troy Area</td>
<td>Albany County</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Rensselaer County</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Saratoga County</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Schenectady County</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Scholharie County</td>
<td>9</td>
</tr>
<tr>
<td>NY</td>
<td>Buffalo-Niagara Falls Area</td>
<td>Erie County</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Niagara County</td>
<td>4</td>
</tr>
<tr>
<td>NY</td>
<td>Buffalo-Niagara Falls Area</td>
<td>Erie County</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Niagara County</td>
<td></td>
</tr>
</tbody>
</table>
## CHC Prevalence in Candidate Urban Areas under the FY 2008 UASI Program

<table>
<thead>
<tr>
<th>State</th>
<th>Candidate Urban Area by Metropolitan Statistical Area</th>
<th>Counties and Cities Selected for Query</th>
<th>CHC Count</th>
</tr>
</thead>
<tbody>
<tr>
<td>NY</td>
<td>Rochester Area</td>
<td>Livingston County, Monroe County, Ontario County, Orleans County, Wayne County</td>
<td>31</td>
</tr>
<tr>
<td></td>
<td>Syracuse Area</td>
<td>Madison County, Onondaga County, Oswego County</td>
<td>22</td>
</tr>
<tr>
<td></td>
<td>Cincinnati-Middletown Area, OH-KY-IN</td>
<td>Brown County, Butler County, Clermont County, Hamilton County, Warren County</td>
<td>49</td>
</tr>
<tr>
<td>OH</td>
<td>Cleveland-Elyria-Mentor Area</td>
<td>Cuyahoga County, Geauga County, Lake County, Lorain County, Medina County</td>
<td>11</td>
</tr>
<tr>
<td></td>
<td>Columbus Area</td>
<td>Delaware County, Fairfield County, Franklin County, Licking County, Madison County, Morrow County, Pickaway County, Union County</td>
<td>12</td>
</tr>
<tr>
<td></td>
<td>Toledo Area</td>
<td>Fulton County, Lucas County, Ottawa County, Wood County</td>
<td>9</td>
</tr>
<tr>
<td>OK</td>
<td>Oklahoma City Area</td>
<td>Canadian County, Cleveland County, Grady County, Lincoln County, Logan County, McClain County, Oklahoma County</td>
<td>13</td>
</tr>
<tr>
<td>OR</td>
<td>Portland-Vancouver-Beaverton Area, OR-WA</td>
<td>Clackamas County, Columbia County, Multnomah County, Washington County, Yamhill County</td>
<td>76</td>
</tr>
<tr>
<td>State</td>
<td>Candidate Urban Area by Metropolitan Statistical Area</td>
<td>Counties and Cities Selected for Query</td>
<td>CHC Count</td>
</tr>
<tr>
<td>-------</td>
<td>-------------------------------------------------------</td>
<td>---------------------------------------</td>
<td>-----------</td>
</tr>
<tr>
<td>PA</td>
<td>Philadelphia-Camden-Wilmington Area, PA-NJ-DE-MD</td>
<td>Bucks County</td>
<td>37</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Chester County</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Delaware County</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Montgomery County</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Philadelphia County</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Pittsburg Area</td>
<td>Allegheny County</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Armstrong County</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Beaver County</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Butler County</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Fayette County</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Washington County</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Westmoreland County</td>
<td>58</td>
</tr>
<tr>
<td>PR</td>
<td>San Juan-Caguas-Guaynabo Area</td>
<td>Aguas Buenas Municipio</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Aibonito Municipio</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Arecibo Municipio</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Barceloneta Municipio</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Barranquitas Municipio</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Bayamon Municipio</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Caguas Municipio</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Camuy Municipio</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Canovanas Municipio</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Carolina Municipio</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Catano Municipio</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Cayey Municipio</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Ciales Municipio</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Cidra Municipio</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Comerio Municipio</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Corozal Municipio</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Dorado Municipio</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Florida Municipio</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Guaynabo Municipio</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Gurabo Municipio</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Hatillo Municipio</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Humacao Municipio</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Juncos Municipio</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Las Piedras Municipio</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Loiza Municipio</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Manati Municipio</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Maunabo Municipio</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Morovis Municipio</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Naguabo Municipio</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Naranjito Municipio</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Orocovis Municipio</td>
<td></td>
</tr>
<tr>
<td>State</td>
<td>Candidate Urban Area by Metropolitan Statistical Area</td>
<td>Counties and Cities Selected for Query</td>
<td>CHC Count</td>
</tr>
<tr>
<td>-------</td>
<td>-------------------------------------------------------</td>
<td>----------------------------------------</td>
<td>-----------</td>
</tr>
<tr>
<td>PR</td>
<td>San Juan-Caguas-Guaynabo Area (continued)</td>
<td>Quebradillas Municipio</td>
<td>32</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Rio Grande Municipio</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>San Juan Municipio</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>San Lorenzo Municipio</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Toa Alta Municipio</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Toa Baja Municipio</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Trujillo Alto Municipio</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Vega Alta Municipio</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Vega Baja Municipio</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Yabucoa Municipio</td>
<td></td>
</tr>
<tr>
<td>RI</td>
<td>Providence-New Bedford-Fall River Area, RI-MA</td>
<td>Bristol County</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Kent County</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Newport County</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Providence County</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Washington County</td>
<td>44</td>
</tr>
<tr>
<td>SC</td>
<td>Charlotte-Gastonia-Concord Area, NC-SC</td>
<td>York County</td>
<td>5</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Memphis Area, TN-MS-AR</td>
<td>Fayette County</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Shelby County</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Tipton County</td>
<td></td>
</tr>
<tr>
<td>TN</td>
<td>Nashville-Davidson, Murfreesboro, Franklin Area</td>
<td>Cannon County</td>
<td>25</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Cheatham County</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Davidson County</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Dickson County</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Hickman County</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Macon County</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Robertson County</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Rutherford County</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Smith County</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Sumner County</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Trousdale County</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Williamson County</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Wilson County</td>
<td></td>
</tr>
<tr>
<td>TX</td>
<td>Austin-Round Rock Area</td>
<td>Bastrop County</td>
<td>36</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Caldwell County</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Hays County</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Travis County</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Williamson County</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Dallas-Forth Worth-Arlington Area</td>
<td>Collin County</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Dallas County</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Delta County</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Denton County</td>
<td></td>
</tr>
<tr>
<td>State</td>
<td>Candidate Urban Area by Metropolitan Statistical Area</td>
<td>Counties and Cities Selected for Query</td>
<td>CHC Count</td>
</tr>
<tr>
<td>-------</td>
<td>-----------------------------------------------------</td>
<td>--------------------------------------</td>
<td>-----------</td>
</tr>
<tr>
<td>TX</td>
<td>Dallas-Forth Worth-Arlington Area (continued)</td>
<td>Ellis County</td>
<td>16</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Hunt County</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Kaufman County</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Rockwall County</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Johnson County</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Parker County</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Tarrant County</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Wise County</td>
<td></td>
</tr>
<tr>
<td></td>
<td>El Paso Area</td>
<td>El Paso County</td>
<td>17</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Atascosa County</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Bandera County</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Bexar County</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Comal County</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Guadalupe County</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Kendall County</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Medina County</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Wilson County</td>
<td></td>
</tr>
<tr>
<td>UT</td>
<td>Salt Lake City Area</td>
<td>Salt Lake County</td>
<td>28</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Summit County</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Tooele County</td>
<td></td>
</tr>
<tr>
<td>VA</td>
<td>Richmond Area</td>
<td>Amelia County</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Caroline County</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Charles City County</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Chesterfield County</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Colonial Heights City</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Cumberland County</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Dinwiddie County</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Goochland County</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Hanover County</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Henrico County</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Hopewell City</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>King and Queen County</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>King William County</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Louisa County</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>New Kent County</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Petersburg City</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Powhatan County</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Prince George County</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Richmond City</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Sussex County</td>
<td>16</td>
</tr>
<tr>
<td></td>
<td>Norfolk-Virginia Beach, Newport News Area, VA-NC</td>
<td>Chesapeake City</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Franklin City</td>
<td></td>
</tr>
<tr>
<td>State</td>
<td>Candidate Urban Area by Metropolitan Statistical Area</td>
<td>Counties and Cities Selected for Query</td>
<td>CHC Count</td>
</tr>
<tr>
<td>-------</td>
<td>-----------------------------------------------------</td>
<td>--------------------------------------</td>
<td>-----------</td>
</tr>
<tr>
<td>VA</td>
<td>Norfolk-Virginia Beach, Newport News Area, VA-NC</td>
<td>Gloucester County</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Hampton City</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Isle of Wight County</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>James City County</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Mathews County</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Newport News City</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Norfolk City</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Poquoson City</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Portsmouth City</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Southampton</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Suffolk</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Suffolk City</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Surry County</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Virginia Beach City</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Williamsburg City</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>York County</td>
<td>15</td>
</tr>
<tr>
<td>WA</td>
<td>Seattle-Tacoma-Bellevue Area</td>
<td>King County</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Snohomish County</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Pierce County</td>
<td>81</td>
</tr>
<tr>
<td></td>
<td>Portland-Vancouver-Beaverton Area, OR-WA</td>
<td>Clark County</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Skamania County</td>
<td>3</td>
</tr>
<tr>
<td>WI</td>
<td>Milwaukee-Waukesha-West Allis Area</td>
<td>Milwaukee County</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Ozaukee County</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Washington County</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Waukesha County</td>
<td>18</td>
</tr>
<tr>
<td></td>
<td>Minneapolis-St. Paul-Bloomington Area, MN-WI</td>
<td>Pierce County</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>St. Croix County</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td><strong>Tier 2 Total</strong></td>
<td></td>
<td><strong>1,790</strong></td>
</tr>
</tbody>
</table>
Community Health Centers generally receive funding from a variety of sources including private donors, foundations, and fundraising, as well as state funds. The majority of those distributions from governmental agencies come from federal sources, though some community health centers have been recipients of local- and state-level funding for special projects and services.


Map created with permission, August 17, 2008, using the Rural Assistance Center’s RAC Mapping Service.


Ibid.


17 October 2008, personal communication with Steven Harrison, assistant director of emergency operations, planning, and logistics, Virginia Department of Health.


20 August 2008, personal communication with Dr. Joseph V. Saitta, emergency services coordinator, Rappahannock Area Health District, Virginia Department of Health.


24 Ibid., 19-23.

25 Ibid., 4.


27 Office of the Civilian Volunteer, Medical Reserve Corps, “About the Medical Reserve Corps” (March 5, 2008), para. 1, http://www.medicalreservecorps.gov/About.


29 April 2008, personal communication with Dr. Joseph Saitta, emergency services coordinator, Rappahannock Area Health District, Virginia Department of Health.


37 Ibid., 21.

38 October 20, 2008, personal communication with Dr. D. Bradley Drawbaugh, executive director of Highland Medical Center in Virginia.


40 ASHTO and others, Collaborating with Community Health Centers for Preparedness, 7.


52 Ibid.


60 National Association of Community Health Centers, “The Challenges.”


65 As cited in National Association of Community Health Centers, Community Health Centers & Emergency Management Fact Sheet, (June 2008).


67 As cited in National Association of Community Health Centers, Community Health Centers & Emergency Management Fact Sheet (June 2008).


76 Gravely, “Legal & Ethical Implications.”


79 Ibid., 311.


81 Colorado Community Health Network, Colorado Community Health Center (CHC) Emergency Preparedness Survey Results (January 2007), 5.


84 Ibid.

85 June 2008, personal communication with Anne Crabbe, chief operations officer, Eastern Shore Rural Health System.


93 Institute of Medicine, Fostering Rapid Advances in Health Care: Learning from System Demonstrations (Washington, DC, National Academy of Sciences Press, November 2002), 43-46.


95 Aaron Katz, Andea B. Staiti, and Kelly L. McKenzi, “Preparing for the Unknown, Responding to the Known: Communities and Public Health Preparedness,” Health Affairs 25, no. 4 (July/August 2006): 954-957.


99 Bureau of Primary Health Care, Program Assistance Letter 02-02, 2.


101 ASTHO and others, Collaborating with Community Health Centers for Preparedness.

102 Wood and Supinski, “Pandemic Influenza Tabletop Exercises,” 8.


104 Shin and others, Reducing Racial and Ethnic Health Disparities, 5.


106 The use of Metropolitan Statistical Areas and the associated cities and counties in the overall risk methodology does not necessarily identify a particular jurisdiction as a UASI jurisdiction. See Government Accountability Office, DHS Risk-Based Grant Methodology, 54-64.

107 Ibid.

108 Data for this table was obtained using HRSA’s Geospatial Data Warehouse, Healthcare Service Delivery Sites which consolidates several Section 330 programs into one data set containing information.
about both grantees and about their associated sites. The report was filtered by community health center, by state, then by relevant county or city. When compared to the Federally Qualified Health Center data through the Geospatial Data Warehouse, the Healthcare Service Delivery Sites data provides a more accurate representation of CHC resources and access points. For example, dental programs, migrant health programs (seasonal and permanent), and other service sites (e.g. nursing homes, correctional facilities) that contract CHCs for primary care services are important to biosurveillance but are not generally listed in the Federally Qualified Health Center data (see also “Dentistry’s Role in Responding to Bioterrorism and Other Catastrophic Events” at: http://www.ada.org/prof/resources/topics/topics_bioterrorism_conf.pdf.

Likewise, mobile medical units and dental clinics, could be similarly valuable response assets, but similarly are not generally noted. On the other hand, CHCs may maintain hospital privileges, notably among those providing OB-GYN services, and include these establishments as service delivery sites which ultimately skew the counts. Additionally, FQHC Look-A-Likes are subject to the same BPHC expectations, PIN 2007-15 included, as FQHCs but do not receive Section 330 funding and are thus exempt from grantee reporting requirements and are not documented in the Healthcare Service Delivery Sites. NACHC suggests that FQHC Look-A-Likes could increase CHC counts by approximately 10 percent. Each state’s PCA may be a good source for the most accurate profile of CHCs in UASI jurisdictions and the most appropriate site for administrative contact information.