HOMELAND

SECURITY

EXECUTIVE SUMMARY

Since September 11, 2001, the nation has been struggling with the problem of responding to an ill-defined but potentially very large and complex terrorist threat. Initial homeland security efforts have sought to address obvious deficiencies in airline security, border controls, defense against weapons of mass destruction and the capabilities of first responders. Billions of dollars have been budgeted to provide additional personnel, equipment and training in these areas. A new cabinet department, the Department of Homeland Security, has been created. A special Terrorist Threat Intelligence Center is being created.

Despite these efforts, most experts give the administration only passing marks for their homeland security efforts. Much of the current literature on homeland security tends to focus on the magnitude of the problem. They criticize the administration's slow progress in addressing these many potential threats.

These judgments are not entirely fair. Threats appear almost endless and overwhelming. Absent adequate threat assessments it is difficult for the new Department to establish sensible priorities for addressing possible vulnerabilities. Without a good set of metrics, it is also impossible to know whether the American people are safer today than they were on September 10, 2001. Thus, it appears to some as if the only way of enhancing homeland security is to spend and do more in every area and against all possible threats.

These four essays present refreshingly different perspectives on what has been accomplished in homeland security to date and what more needs to be done. Dr. Loren Thompson provides a cogent case for the importance of public education and communications, an oft-overlooked area of homeland security. His essay emphasizes the role of strong leadership in providing the reassurance that the public needs in an era of terrorist threats. Dr. Martin Libicki makes the case that the nation may be much less vulnerable to cyber attack than has been suggested in most public analyses. He suggests that a set of limited measures, largely in the hands of the private sector, could be sufficient to provide robust protection. Mr. Michael Scardaville thoroughly assesses federal critical infrastructure protection efforts employed since September 11. While applauding the early stages of the administration's approach to securing critical infrastructure, he acknowledges that long-term success hinges on both the ability of numerous federal agencies recently transferred to the Department of Homeland Security to quickly consolidate into a focused effort. It will also depend on continued improvements in how intelligence is shared. Dr. Joseph Barbera looks broadly at the problem of managing catastrophic terrorist events. Such events, involving the use of chemical, biological, radiological or nuclear weapons can be expected to result in injury to thousands, even tens of thousands.

The essays are part of a study conducted by the Lexington Institute to assess the state of homeland security more than a year after September 11, 2001. Other analyses examined such topics as border and transportation security, defense against weapons of mass destruction, infrastructure protection and the role of the military in homeland security. Each sought to address the progress made to date in reducing the homeland's vulnerability and to identify steps that still need to be taken. The Lexington Institute plans to publish additional essays over the course of the year.


Lexington
Institute

TABLE OF CONTENTS

How Washington Explains Terrorist Threats to the Public

Loren B. Thompson, Ph.D.

America's domestic counter-terror campaign ended 2002 on an ominous note. On the last day of the year, President George W. Bush disclosed that he personally had approved a nationwide search for a band of terrorists believed to have entered the nation on Christmas Eve. He asked the public for help in finding the terrorists. A criminal accused of smuggling illegal aliens had told Canadian authorities that five Pakistanis with forged documents crossed into the U.S. on December 24. Further inquiries in Pakistan suggested as many as nineteen terrorists might have entered the U.S. -- the same number that carried out the 9-11 attacks.

The story seemed credible given the informant's involvement with smuggling, the fact that he had passed a lie-detector test, and a previous case in which a would-be bomber was detained at the border. The nation was alerted, and an intensive manhunt launched. On January 7, though, the FBI called off the search and announced that the story was a fabrication. No Christmas Eve border-crossing had occurred. Anonymous Justice Department sources told the media they had doubted the story from the beginning. A former Canadian intelligence official defended the handling of the case, telling *The Washington Post*, "If you're interested in precision, go into physics, not intelligence."

Despite this embarrassing episode, exactly one month later the federal government announced another nationwide terrorist alert. The President again signed off on the decision, which resulted in raising the level of the color-coded warning system to orange, or "High Alert." Attorney General John Ashcroft said that diverse intelligence indicated a possible Al Qaeda attack against "soft targets" in the U.S. timed to coincide with the end of the annual Muslim pilgrimage to Mecca. Secretary of Homeland Security Tom Ridge urged the public to be prepared and vigilant, but offered little guidance as to which targets were most at risk. Ridge recommended that the public not make major changes in daily routines.

This time, sources were quick to tell the media that not everyone in the federal government agreed with the decision to raise the alert status. Even before the change was announced, the FBI and CIA were reported to be doubtful about the value of such a move, since warning signs were ambiguous and there was little actionable guidance to give the public. As Massachusetts Public Safety Director Ed Flynn remarked after the alert status was raised, "To be honest, going from yellow to orange for the average citizen means not much, [so] go on with your normal course of business."

That isn't what happened in many places. Anxious shoppers cleared store shelves of bottled water and duct tape for sealing homes. A *New York Times* poll found that four out of five Americans expected a major terrorist attack within U.S. borders in the coming months. Financial analysts reported markets were being weighed down by fear of violence at home and abroad. And then word began to leak out of Washington that some of the information driving this alert too was false, a fabrication of unreliable sources.

It is possible that the security alerts of January and February 2003 discouraged domestic terrorism by bolstering public awareness and law-enforcement efforts. But it is also possible, in fact probable, that such episodes are a reason why the number of citizens who believe America is winning the war on terrorism has declined steadily. In January of 2002, 66% of respondents thought America and its allies were prevailing. A year later, despite the absence of major domestic incidents, the number had declined to 33%. By the time pollsters took the latter reading in January of 2003, one in five Americans thought the terrorists were winning -- a doubling of that sentiment since the days immediately following the 9-11 attacks.

The deterioration in public opinion inevitably raises questions about the Bush Administration's strategy for explaining terrorist threats to the public -- especially given the fact that two nationwide alerts were called in the first quarter of 2003 on the basis of intelligence that turned out to be partly or wholly wrong. The purpose of this essay is to analyze whether the government's current approach to informing the public is working, or whether it needs to be revised. The essay concludes that the current strategy should be improved, but that the unpredictable nature of the threat precludes easy solutions. No matter

what strategy the administration pursues and how deftly it executes that strategy, there will still be problems -- poor preparedness, counterproductive hysteria, uneven awareness, and so on.

The essay begins by briefly explaining the nature of terrorism, and why it is so hard for open societies to counter the unconventional methods embraced by terrorists. It then describes the recommendations of various commissions concerning counter-terror communications, and the role for such communications envisioned in the Bush Administration's homeland-security strategy. Having laid that foundation, the essay identifies the key themes and assumptions that seem to drive administration pronouncements on the threat, and the response they have elicited. The utility of the existing, color-coded alert system is assessed, as is the government's administrative arrangements for issuing alerts. The essay concludes with some tentative lessons that might inform more effective communications efforts in the future -- but also some cautionary observations about the uncertain domestic security environment that Americans now seem to inhabit.

The Political Dynamics of Terrorism

Bush Administration efforts to enhance homeland security are primarily a response to the terrorist attacks of 9-11. While it is easy to imagine worse forms of aggression mounted by nations armed with nuclear weapons or other means of mass murder, the administration views its missile-defense program and other overtly military responses as the main remedy for state-based threats. Terrorist groups such as Al Qaeda, though, represent a uniquely elusive and unpredictable challenge for which military responses are at best a partial solution. The administration considers improved law enforcement and emergency preparedness to be essential features of an effective counter-terror plan.

Simply stated, terrorism is a strategy that seeks to defeat enemies through fear. Like nuclear deterrence, its goal is to influence the perceptions of adversaries so they will behave in ways beneficial to the perpetrators of terrorist acts. Unlike deterrence, though, terrorism relies on repeated, gross acts of violence to accomplish its desired effect. But violence alone is not enough -- the horrific character of the acts must be vividly conveyed to intended audiences if they are to be terrorized. Communication is thus critical to the success of terror campaigns.

Terrorism is not new. Walter Lacqueur describes an extreme Jewish faction called the *sicari* -- root of the modern word “zealot” -- that operated in Roman-occupied Palestine during the early years of the first millennium. A thousand years later, a similarly extreme Muslim sect called the *assassins* terrorized the Middle East. Barbara Tuchman recounts the widespread assassinations and bombings perpetrated by anarchists in her famous study of the *fin-de-siecle* west, *The Proud Tower*. Then as now, the ranks of terrorist organizations were filled by desperate and deluded men. What is new today is the way in which political, economic and technological trends have empowered such men.

In terms of technology, modern terrorists potentially have access to many methods of mass destruction not available in earlier times. These range from chemical, biological and radiological weapons to items available in everyday commerce such as disruptive computer software and volatile ammonium-nitrate fertilizer (used to destroy the Murrah federal building in Oklahoma City). In addition, contemporary terrorists have numerous options for assuring secure communications, including frequency-hopping radios, cellular telephones and anonymous internet accounts employing various encryption techniques. New communications technologies such as cable and direct-broadcast satellite television also enable terrorists to quickly transmit their message of fear to target audiences.

Other factors empowering terrorists include economic globalization -- the removal of barriers to international movement of goods, people, and capital -- and political democratization. As Lacqueur notes, democratic societies are usually more vulnerable to terror campaigns than dictatorships, because security forces are constrained in the tactics they may employ and political authorities have little control over the content of mass media. The rights and opportunities afforded to average citizens in democracies can be readily exploited to aid terrorist causes. Prior to 9-11, these empowering influences were widely viewed in America as enablers of global peace and prosperity. That view wasn't wrong, but it

neglected the implications of placing unprecedented power in the hands of political extremists. After 9-11 the implications became painfully clear, creating a groundswell of support for new domestic-security measures. The absence of follow-on attacks suggests that the measures taken have been fairly effective, but two years of reflection on the larger meaning of 9-11 have convinced many experts that Al Qaeda is the harbinger of permanent changes in the security environment. Some observers describe the emerging danger as "existential," meaning permanent and inescapable.

In a tract circulated after the 9-11 attacks, senior Qaeda operative Ayman al-Zawahiri stressed the importance of using so-called martyrdom operations to inflict maximum casualties on western societies, "for this is the language understood by the West." Zawahiri insisted that "the targets as well as the type and methods of weapons used must be chosen to have an impact on the structure of the enemy and deter it enough to stop its brutality, arrogance and disregard for all taboos and customs." Such thinking is typical of the terrorist mindset, which assumes that indiscriminate violence can alter the beliefs and behavior of whole societies.

The challenge facing the Bush Administration is how to prevent terrorists from carrying out this strategy in a society as porous and diverse as the United States. Communication plays a central role in the administration's plans, just as it does in the strategy of the terrorists. The public must be informed of the danger in a manner that allows it to be prepared and aid counter-terror efforts, and audiences with relevant responsibilities at the state and local levels must be instructed in how to cope with specific types of threats.

But as the two alerts described at the beginning of this essay demonstrate, the wrong kind of public communication potentially can harm counter-terror efforts and aid the terrorist cause. Finding the right tone and content for official communications has proven to be a difficult task in which the subjective judgments of policymakers play a prominent role. The administration is still struggling to reconcile the competing goals of its counter-terror plan in a communications strategy that informs the public without terrorizing it.

Panels and Plans

Advisory bodies charged with assessing U.S. counter-terror preparedness have frequently cited the need for the federal government to develop a coherent public-communications strategy. Perhaps the most persistent has been the federally-chartered "Advisory Panel to Assess Domestic Response Capabilities for Terrorism Involving Weapons of Mass Destruction," usually referred to as the Gilmore Commission. In its first annual report, released in December of 1999, the commission stated: "Considering the serious nature and potential consequences of any terrorist incident, the Panel is convinced that comprehensive public education and information programs must be developed, programs that will provide straight-forward, timely information and advice both prior to any terrorist incident and in the immediate aftermath of any attack."

The commission returned to this theme in its second report a year later, asserting, "The more that American citizens can be educated about what may happen and what will be expected of them, the less likely that an incident will be exacerbated by uninformed public reaction." The commission's third annual report was issued shortly after the 9-11 attacks, and again stressed that "public awareness and communications are important tools in combating terrorism." It continued, "As illustrated by the public affairs and communications activities in the wake of the recent anthrax attacks, pre-event public education and awareness, and post-event public communications require greater attention and better planning."

Similar sentiments have been expressed by other advisory bodies. For example, the Heritage Foundation's Homeland Security Task Force published a report in early 2002 recommending that the federal government develop a "nationwide education and public relations program" for countering terrorism. It argued that "public relations campaigns can be vital to preventing panic, improving civil defense preparedness and responses, and maximizing all efforts to prevent terrorism." One goal of such cam-

paigns, the task force said, should be to improve "cooperation with local media to enhance the dissemination of information to the public."

Even when advisory panels do not explicitly address public-communications strategy, the need for a carefully-constructed communications plan is often implied in their other findings. For instance, a homeland-security task force sponsored by the Council on Foreign Relations warned in late 2002 that "after a year without a new attack, there are already signs that Americans are lapsing back into complacency." The task force decried the "counterterrorism information void" in which local authorities were said to be operating. The obvious implication was that Washington needed to do a better job of educating both specialists and the general public to the severity of the threat.

The Bush Administration undoubtedly understood the importance of effective public communication when it began concentrating on domestic counter-terror plans in the aftermath of 9-11. Senior administration leaders such as Richard Cheney, Colin Powell and Donald Rumsfeld had spent decades in public life, and had seen the consequences of poor communication in past security crises. However, the administration may have underestimated how difficult it would be to get the process and product right.

The first official mention of counter-terror communications came in an October, 2001 executive order creating the Office of Homeland Security within the Executive Office of the President. The order described the mission of the new office as development and implementation of "a comprehensive national strategy to secure the United States from terrorist threats or attacks," and specified a dozen generic functions for the office ranging from detection and preparedness to prevention and recovery. "Public affairs" was the ninth function listed, and was covered in two sentences:

> The Office, subject to the direction of the White House Office of Communications, shall coordinate the strategy of the executive branch for communicating with the public in the event of a terrorist threat or attack within the United States. The Office also shall coordinate the development of programs for educating the public about the nature of terrorist threats and appropriate precautions and responses.

When this language was drafted less than a month after 9-11, the administration had not yet decided to back creation of a cabinet department responsible for homeland security. Senior administration officials opposed creation of a "new bureaucracy," and expected that the head of the White House office, former Pennsylvania Governor Tom Ridge, would serve primarily as an interdepartmental coordinator and confidential advisor to the President. Some even resisted allowing Ridge to testify before Congress.

It soon became apparent that this arrangement would not be adequate. In June of 2002 President Bush proposed creation of a Department of Homeland Security, which came into being at the beginning of 2003. Long before that happened, though, the administration implemented what thus far has proved to be its most important public-communications innovation in the area of homeland-security: a color-coded national alert system. The new system, activated in March of 2002, was designed to standardize official warnings about potential attacks so that all citizens would share a common understanding of threat conditions.

Before assessing how well that system has worked, though, it is worthwhile to briefly examine the high-level messages concerning terrorism articulated in presidential addresses after 9-11. As is typically the case in national emergencies, the public looked to the chief executive for guidance in dealing with the danger, and several presidential speeches were crafted with the goal of broadly defining how citizens should react. These speeches, though few in number, provide a philosophical backdrop for all of the administration's other pronouncements on homeland security.

Presidential Themes

The most important speech President Bush delivered concerning public responses to domestic terrorism came nine days after the 9-11 attacks, when he addressed a joint session of Congress. The nationally-televised remarks were his first formal effort to describe what role the public should play in the nation's counter-terror campaign, and subsequent presidential pronouncements have tended to reiterate the themes of that initial speech. Bush made several general requests of the public:

> Americans are asking: What is expected of us?
> I ask you to live your lives, and hug your children.
> I know many citizens have fears tonight, and I ask you to be calm and resolute, even in the face of a continuing threat.
>
> I ask you to uphold the values of America, and remember why so many have come here. We are in a fight for our principles, and our first responsibility is to live by them. No one should be singled out for unfair treatment or unkind words because of their ethnic background or religious faith.

Reuters

Bush said the public should continue its support of the victims of the 9-11 attacks, both through financial contributions and through prayer. And he made three more requests of the nation:

> The thousands of FBI agents who are now at work in this investigation may need your cooperation, and I ask that you give it.
>
> I ask for your patience, with the delays and inconveniences that may accompany tighter security; and for your patience in what will be a long struggle.
>
> I ask your continued participation in the American economy. Terrorists attacked a symbol of American prosperity. They did not touch its source...

Clearly, the main goal of the President's remarks was to restore public calm and confidence. He asked for unity, tolerance, patience and resolve, but the role of average citizens in counter-terror efforts was described in passive terms. The speech seemed to be aimed primarily at discouraging over-reaction to the attacks and urging citizens to behave as they might have before the attacks occurred. The President was later criticized for asking too little of the public, but in the immediate aftermath of the most traumatic attacks on the American homeland since Pearl Harbor, it isn't hard to see why the White House decided reassuring the public should be its top goal. As noted earlier, fear is the main tool terrorists use to defeat their adversaries.

However, nine months later the President was still asking relatively little of the public beyond patience and calm. In a June 6, 2002 address to the nation reviewing counter-terror efforts and proposing creation of a Department of Homeland Security, Bush advised that “Americans should continue to do what you're doing -- go about your lives, but pay attention to your surroundings.” The President said that citizens should add their “eyes and ears to the protection of our homeland,” but he offered no concrete initiative for enlisting citizen participation such as the civil-defense program of cold-war years. The public's role remained largely passive.

The President's address from Ellis Island on the first anniversary of the attacks was considerably more uplifting, invoking America's destiny and ideals to make the case for a global crusade against terrorism:

"God has placed us together in this moment, to grieve together, to stand together, to serve each other and our country." But once again, the inspirational rhetoric was not matched to any expectation of initiative or involvement on the part of individual citizens. As Thomas Friedman of *The New York Times* commented several months later in assessing the administration's thematic approach to war with Iraq -- a war justified in part by the terrorist threat -- the presidential message seemed to be, "We're at war, let's party."

Friedman's complaint that the White House was not asking the public "to do anything hard" underscores the dilemma that democratic governments face in confronting terrorism. If the government wants to demand sacrifice of the public, it must first acknowledge there is a crisis. That, unfortunately, is precisely the atmosphere that the terrorists wish to provoke. If, on the other hand, the government wants to minimize the apparent power of terrorists, then it must avoid conveying the impression of crisis -- thus undercutting the case for sacrifice. The Bush Administration's solution to this dilemma was to assign the active aspects of the counter-terror campaign to dedicated specialists, while giving the public an undemanding supportive role. One potential drawback of that approach is that it leaves many citizens feeling powerless.

National Alert System

The Bush Administration may not want to ask much of the general public on the counter-terror front, but it has a fair amount it wants to tell the public. In the months immediately following the 9-11 attacks, there was widespread confusion about the nature and degree of danger to the homeland. Despite presidential efforts to reassure the nation, federal agencies issued a continuous stream of unsettling warnings and recommendations. Because the release of such information was only loosely coordinated and often spread beyond intended audiences via the media, it caused unnecessary anxiety.

Six months after the attacks, the administration reorganized its approach to alerting the public about domestic threats by establishing a "Homeland Security Advisory System." In the words of a White House press release, the system was "intended to create a common vocabulary, context and structure for an ongoing national discussion about the nature of the threats that confront the homeland and the appropriate measures that should be taken in response." The press release said that the new system would "inform and facilitate decisions appropriate to different levels of government and to private citizens at home and at work."

The advisory system consisted of five color-coded threat conditions: low (green), guarded (blue), elevated (yellow), high (orange), and severe (red). Each level of danger was associated with a specific series of protective measures. For example, when condition orange was in effect, authorities were expected to take "additional precautions" at public events, including "possibly considering alternative venues or even cancellation." When condition red was in effect, authorities were expected to close public and government facilities. The determination as to which condition was in effect would be made by the Attorney General and the Assistant to the President for Homeland Security (Governor Ridge), based on information received from the intelligence community and domestic law-enforcement agencies.

The new system was an important innovation in explaining threat conditions to the public, but it contained a number of ambiguities. First of all, the presidential directive mandating the system stated that risk of attack would be assessed on the basis of both probability and "potential gravity." Thus, a moderate likelihood of nuclear aggression might be assigned the same threat condition as a high likelihood of truck-bombings. Second, threat conditions might not apply uniformly if intelligence indicated a focused danger; for example, a higher alert level might be assigned to particular regions or industries than to others. Third, the discriminators to be used in differentiating among higher alert levels (yellow, orange and red) proved elusive to both policymakers and the public. Shortly after the public safety director of Massachusetts made his February, 2003 comment that the difference between yellow and orange conditions was unclear to most people, New York's police commissioner asserted, "there are gradations within orange, and New York City is at the high end of orange."

One other problem with the Homeland Security Advisory System became apparent over time, although it originated less in the system itself than in Washington's bureaucratic culture. The presidential directive mandating the system gave the Attorney General and Assistant to the President for Homeland Security responsibility for determining and disclosing threat conditions, but it directed that they should consult closely with other "Homeland Security Principals or their subordinates" such as the Vice President and Secretary of Defense. Consultation was clearly indicated, but a pattern soon emerged in which viewpoints that did not prevail quickly reached the media, undercutting the final decision.

Reuters

Sometimes dissenters complained to reporters before the decision was even announced. For example, a day before the national alert status was raised from yellow to orange on February 8 of this year, *The Washington Post* reported disagreement among policymakers concerning whether such a move was desirable. The White House and Defense Department favored a higher threat condition, *Post* reporter Dan Eggen wrote, but other agencies did not:

> FBI and CIA officials have taken a more cautious position, however, arguing that the threat information -- while clearly troubling -- is vague and contains no specific, credible evidence of an impending attack, sources said... Many of these officials believe that issuing a general terrorism alert would alarm the public without providing any usable information, and would be viewed with undue skepticism because of U.S. preparations for war with Iraq.

Obviously, when insiders leak dissenting views to the media in this manner, they diminish the credibility of the advisory system. A national poll conducted by Fox News last autumn found considerable doubt about the color-coded alerts, with 41% of respondents saying they were "not helpful," 39% saying they were, and 20% saying they were not sure. It appeared that support for the system eroded further in the aftermath of the February 8 alert. Philip Shenon of *The New York Times* echoed much of the media coverage in reporting doubts about the rigor and utility of alerts:

> The administration's critics [argue] that the government's system for analyzing terrorist threats and sharing the information with the public is not making the public any safer. The critics say it is only frightening them... Within the administration, even supporters of what is known as the Homeland Security Advisory System admit that the system is more art than science -- much more -- and that the analysis of often scant intelligence and decisions about whether to alert the public to its contents must often be subject to hunch.

Such doubts are typical of the uncertainty that terrorists seek to sow in societies they are attacking. Information concerning terrorist intentions is usually so fragmentary that subjective judgments about how to react are unavoidable. The possibility that the public will be unduly alarmed must be balanced against the danger that citizens will die unnecessarily for lack of warning. However, in the case of the February 2003 alert, the public's fears may have been worsened by the government's advice concerning how to deal with the elevated threat condition.

Practical Advice

February's orange alert was accompanied by the government's most intensive efforts since 9-11 to provide the public with practical advice about terrorist threats. Instead of simply warning that attacks were more likely, the government recommended measures to individuals and families such as assembling an emergency kit, identifying a safe room, and preparing escape plans. It was these recommendations that provoked panic buying of bottled water and duct tape in some areas (especially on the East Coast, where attacks were said to be more likely).

The government had been planning to provide such advice for some time, but the orange alert prompted Governor (now Secretary) Ridge to accelerate its release. The information on citizen preparedness was first offered in a press conference two days after the threat condition was raised, and then several days later Ridge unveiled a website (www.ready.gov) and an 800-number that the public could use to get more details. An advertising campaign similar to that recommended by the Heritage Foundation and other organizations was also announced to encourage use of the new information sources.

The government's efforts to provide useful advice during the alert were widely ridiculed -- so much so that Ridge had to shift his public message from preparedness to reassurance. A *Washington Post*-ABC News poll conducted nationwide a week after the February 10 press conference found that 44% of respondents thought the advisories had caused "needless fear and alarm," while only 38% felt useful information had been conveyed. However, the same poll revealed that over a third of the nation had actually undertaken some of the steps recommended by Ridge, and in the national capital region -- one of the most likely targets of attack -- six in ten residents had taken precautionary measures.

Those findings represented a significant improvement from the results of a Fox News nationwide poll in November of 2002, when 53% of respondents admitted they were "not at all" prepared for a chemical or biological attack, and 30% said they were "not very" prepared. In that poll, only three percent of citizens claimed to be "very" prepared. Whatever the validity of Ridge's advice may have been, a substantial portion of the public heeded it -- even before the website and 800-number were unveiled.

Although it has become fashionable to deride the administration's public preparedness efforts, few critics have offered concrete alternatives. While some fine-tuning is undoubtedly needed, there is no way of educating citizens about how to protect themselves unless they are first persuaded protection is necessary. The unpredictable timing and character of terrorist acts precludes precise advice as to what steps should be taken. For example, citizens would be well advised to flee some attacks, while staying put in others. When the diversity of dangers is combined with an exceedingly heterogeneous audience and the uncontrollable interpretations of the national media, it isn't hard to see how suggesting any course of action could produce undesirable results.

Furthermore, the psychological dynamics of terrorism are such that some citizens will resent being told what they need to know, and others will consciously or unconsciously avoid assimilating the information. As one reporter who covers homeland security from Washington observed:

> A level of denial is required to live in Washington... I look at this city and say it's a target for the next one thousand years. These terrorists have a millennial memory... The danger is too psychologically painful to focus on.

This reporter has some plans for how to cope with terrorist attacks -- as does his newspaper -- but most of the time he ignores the danger because otherwise he would be unable to do his job. He knows that even working in Washington, he is unlikely to be the direct victim of an attack. He also knows that if he is a victim, he may die promptly or find any preparations he has made irrelevant to the danger at hand.

So he simply chooses not to think about the threat in personal terms most of the time. Millions of Americans probably feel the same way, which means there will always be limits to how effective a public-preparedness campaign can be.

Findings and Recommendations

Less than two years have passed since the atrocities of 9-11. There have been no further attacks in the United States. The Department of Homeland Defense has barely begun operating. Clearly, it would be premature to draw profound conclusions about the merit of the Bush Administration's public-communications strategy for combating terrorism. However, some provisional findings can be offered based on the experience of the last two years and what was already known about the nature of terrorism:

1. Skillful public communication is essential to the success of any counter-terror campaign. Terrorists seek to shape popular psychology through the communication of danger, so those who seek to defeat them must convey counter-messages of reassurance and preparedness. Effective counter-terror communications are more difficult when threats are ill-defined, audiences are diverse and media content is uncontrolled. That is precisely the situation prevailing in the United States today.

2. The Bush Administration understood from the earliest days of its counter-terror efforts that public communication would be important, but it may have underestimated the difficulty of getting the process and product right. Aside from the obvious difficulty of explaining danger without reinforcing fear, the administration's early efforts were impeded by fragmented authority, bureaucratic rivalries, and legitimate differences of opinion among policymakers about the best course of action.

3. The administration has not sought the active participation of most citizens in counter-terror efforts. Instead, it has asked for public support and patience while specialists carry out the various missions associated with securing the homeland. This may reflect a valid assessment of the general public's propensity and ability to participate, but the passive role envisioned for the public could demoralize many who feel powerless to aid the larger effort.

4. The only area where the administration seems inclined to favor individual initiative is self-protection. The government has only recently begun to provide practical advice on self-protection, but early indications are that much of the public is prepared to listen and act. The internet provides a particularly effective method of conveying such advice, because the amount of detail offered can be tailored to the need and interest level of individuals.

5. Despite frequent ridicule, the color-coded threat conditions of the Homeland Security Advisory System are an effective way of communicating the prevailing degree of danger to mass audiences. Many citizens are too disengaged or distracted to assimilate more nuanced information. Most of the difficulties associated with the system are traceable to incomplete or ambiguous intelligence, which forces policymakers to make subjective judgments about whether and how to describe threat conditions.

Given the nature of terrorist threats, even an optimum public-communications plan deftly executed will be accompanied by considerable confusion and resentment. Issues of presidential style and philosophy can influence the effectiveness of counter-terror communications, as can the continuous jockeying of contending bureaucracies for money and visibility. The absence of follow-on attacks to 9-11 suggests that Bush Administration efforts to combat domestic terrorism are working reasonably well. One paradox of terrorism is that the longer such violence is averted, the less inclined many citizens will be to heed government warnings and advice. Given that dynamic, the proper metric of success in counter-terror communications will always be ambiguous: the public that listens most closely may well be the one that is most in fear.

IS CYBER-TERRORISM GETTING CLOSER?

Dr. Martin C. Libicki

Even before the dust and the smoke of the Twin Towers had cleared, there were warnings that September 11th portended the advent of a wave of cyber-terrorism. One could no longer argue that it could not happen here. Many felt that a full-blown cyber-terrorist attack would make September 11th seem positively benign. As if to underscore the link, Richard Clarke, the National Security Council's (NSC) point man on terrorism became the administration's newly minted czar of cyber-security.

Reuters

The association between terrorism and cyber-mischief, however, did not spring forth fully formed on that day. Indeed, Secretary of Defense Rumsfeld's transformative six-part strategy for the Department of Defense (DoD) explicitly promoted cyber-defense as one of these six parts. No one needs reminding that DoD is so reliant on information systems that their protection is a military priority. But, were the cyber-defense mission limited solely to defense systems it would properly rate no more mention than does safety -- both encompass the essential but everyday requirements of dealing with complex and dangerous machinery. Only in direct defense of the country would the cry to dominate cyberspace make sense as a priority.

How safe is the country from cyber-terrorism, anyway? The administration takes great pains to claim that we are safer from terrorism today than we were on September 11th. However, on September 10th, 2001, most Americans felt secure enough -- a belief that proved unwarranted, or at least overly optimistic. Granted, September 11th was not a cyber-terrorist attack (the Nimda worm attack that took place a few weeks later was thought by some to be related, but there is no evidence that it was). The event itself is evidence only that the United States has enemies who would not shy away from anything and thus certainly not from cyber-terrorism. It says nothing about what capabilities they have or how vulnerable the U.S. infrastructure is. As with many other forms of terrorism that have not yet taken place, it is almost impossible to know exactly how vulnerable the United States was on September 11th to cyber-terrorism. It is as hard to determine how more vulnerable the U.S. infrastructure is relative to whatever may constitute "good enough."

Fortunately, the challenge of determining some vectors of improvement is a little more tractable. One can measure inputs: i.e., how much is being spent on cyber-security. One can try to measure outputs: i.e., how much damage is caused annually by viruses and worms. But how well related are measures of today's constant low-scale barrage and the risk to the economy and society of a large-scale but as-yet unseen event (IDC, the computer consultancy, has warned that a cyber-terrorism attack is a near certainty for 2003 -- but they define an incident that closes the Internet for a day to be an act of cyber-terror). Indeed, the run of small events and the risk of large ones may evolve in different directions. As Edward Tenner argues in *Why Things Bite Back*, it is characteristic of modern technology to reduce the likelihood of acute conditions (e.g., acute childhood respiratory failure) in a process that leads to far more chronic ones (e.g., asthma). The same progression may well take place in cyberspace -- as the volume of spam, distributed denial-of-service attacks, script kiddy jaunts and the like go up, the ability to do serious mischief may be going down -- and for that reason.

The remainder of this essay attempts to lay out the prospects for countering cyber-terrorism in several sections:

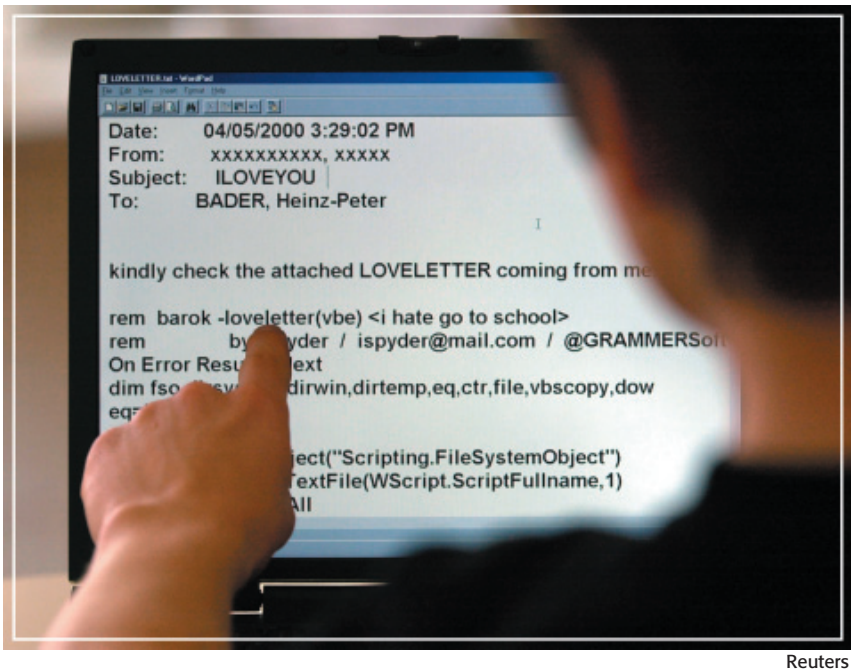
- A brief description of the cyber-terrorist threat;
- An attempt to create metrics for assaying such a threat;
- First-order trends in cyber-security;
- An agenda of potential policy improvements to reduce the threat of cyber-terrorism to "adequate" levels; and
- The prospects of such an agenda.

The Cyber-Terrorist Threat

It does not take much to write a plausible-sounding cyber-terrorist scenario. They are the stuff of popular fiction (e.g., the stock market hack in Tom Clancy's *Debt of Honor*). Take this one (*Economist* survey, "Securing the Cloud," 24 October 2002):

> It is a devastating prospect. Terrorists electronically break into the computers that control the water supply of a large American city, open and close valves to contaminate the water with untreated sewage or toxic chemicals, and then release it in a devastating flood. As the emergency services struggle to respond, the terrorists strike again, shutting down the phone network and electrical power grid with just a few mouse clicks. Businesses are paralyzed, hospitals are overwhelmed, and roads are gridlocked as people try to flee.

Since computers are involved in almost every facet of modern life, it is easy to enumerate the touch-points where a malfunctioning computer -- one that refuses to perform or relies on deliberately queered data -- can cause havoc. The usual places -- electric power, petroleum pipelines, natural gas distribution, air traffic control, railroad switches, traffic signals, phone systems, satellite controls, the Internet, banks, credit card validation, stock markets, hospitals, and emergency services -- have been on everyone's list for a long time (e.g., since the 1996 PCCIP report). One could add less obvious but equally critical nodes (e.g., check clearing), or acts of terrorism against individuals rather than societies (e.g., blackmail enabled by surreptitious access to sensitive data such as medical records).



Reuters

A plausible threat exists, at least in theory. In practice, there are two questions that have to be asked of cyber-terrorism that are less necessary when considering terrorism in the physical world: what is actually possible, and what would be the motivation for certain types of attacks?

Questioning the art of the possible is required because of the artificial nature of cyberspace. We know what two thousand pounds of explosives can do, even to a steel-reinforced concrete building. It is possible to calculate, to well within an order of magnitude, how many people would be at risk

of infection given the dispersal of anthrax spores under specific sun, wind, and dispersal conditions. These data can be derived from the laws of physics and biology. It is far harder to determine what a systematic attack on a power plant's SCADA (supervisory control and data acquisition system) would produce. Why the difficulty? First, every electric power company is different -- and in ways that are not at all obvious from the outside, and not even very clear from the inside. Some firms take security more seriously than others (they could be, for instance, more fastidious about configuration management or installing patches); some connect their SCADA systems more promiscuously to the rest of the company's intranets, some less; some SCADA systems are accessible through dial-in and with various levels of protection. Not only would the security of such systems vary from one owner to another, but they would also vary from one week to the next depending on what software was in place, or who is exercising how much diligence in protecting passwords. Insofar as many types of hacker attacks exploit race conditions (when two processes contend to see which gets the attention of the processor), it is possible for security levels to literally change by the microsecond. Wide variations in the security of information systems are the rule not the exception.

Assessing damage also depends on the relationship between the information systems and whatever machinery they control. How tightly are they coupled? What are the fail-safe and default conditions? How are they managed and monitored? Is there manual override? When can it be exercised? Again, answers vary greatly. Studies of industrial accidents suggest the great role played by chance, panic, misunderstood communications, and the presence of the right person (or the wrong person) at a critical spot. The ability of systems managers to recognize abnormal conditions, bring them under control, and clean up the damage expeditiously is also critical (and hard to assess from the outside). Complicating this, in the case of cyber-terrorism, is the possibility that the means of attack (e.g., an implanted back door in a system) may be set into position far earlier than the attack itself.

The last consideration is the relationship between the system attacked and its counterparts elsewhere. Electric power systems are heir to cascading faults, but the mechanism by which faults -- even natural ones -- cascade from one system to the next is poorly understood.

Complexity is key to all this uncertainty. Since there is no forced entry in cyberspace, every attack has to proceed along paths either established for some legitimate purpose or left over as an undocumented feature of systems programming. In theory, it is possible to exercise complete control over access by guarding every path in. In practice, it is very difficult because information systems are complex and growing ever more so. It is this very complexity which also makes it so difficult to know what the effect of an attack may ultimately be.

Further complicating any sense of what a plausible cyber-terrorist incident looks like is that the motives for cyber-terrorism are anything but obvious. In truth, the motives for almost all acts of terrorism are obscure by the standards of rational strategy. It is hard to think of any terrorist campaign waged against a developed nation that has achieved its political aims. But clearly, terrorism happens. Thus, it must have a motive. The most plausible set of motives relate to what was termed, in the 19th century, the "propaganda of the deed." Terrorism is attention-getting, and, as such, a demonstration of power, a sign that the perpetrators have struck a blow against a power against which sympathizers harbor ill will.

Judged by the standards of attention getting, however, cyber-terrorism lacks a certain "something." First, it is the rare attack on a computer system that can hurt anyone, much less people in large numbers as captured by television cameras. Second, by contrast to a truck bomb, the link between the hacker and the damage is easily obscured. There are few cyber-attacks that produce effects that cannot be explained as some sort of software malfunction (no attack in cyberspace has ever reduced service levels as much as what happened to AT&T in January 1990 as a result of a faulty piece of software). The closest analog to cyber-terrorism that anyone has noticed has been the defacement of web sites for political purposes -- an act that damages nothing, but signals to the world the attackers' ire and talents. Finally, terrorists from countries that are unwired by U.S. standards may lack the intuition that suggests that attacks on computers can be weapons of mass disruption.

Metrics

By this point it should be clear that no metric is self-evident. Most vectors of the metric matrix will, of necessity, be measures of inputs rather than outputs.

To echo the sequence of the preceding section, the risk from cyber-terrorism can be gauged by looking at:

- The state of information security technology;
- The steps taken to implement security throughout the infrastructure;
- The extent to which people can respond effectively to emergencies;
- Interconnections among infrastructures; and
- The many factors that affect motives to attack.

The state of information security technology has to be examined at two levels. The first is the inherent stability and safety of the systems that people install. Without putting too fine a point on the matter, the greatest single factor in the vulnerability of the national (or, for that matter, international) infrastructure to cyber-terrorism is the quality of the operating systems and closely-related products (e.g., web servers) shipped by Microsoft. The second is the quality of tools designed specifically for enhancing security: firewalls, virus defenses, intrusion and anomaly detectors, as well as configuration management and network management software in general. One could include the quality of service providers who monitor networks for a living (e.g., Bruce Schneier's company, Counterpane).

The steps taken to implement security also have various components. The resources allocated to information security and the quality of people entering the computer security field certainly count. Often ignored in the counting are the policies that enterprises adopt to secure their own systems: e.g., who can access what files and processes, how are firewalls configured, what is being done to inculcate security throughout the entire organization.

To reiterate, computer security in general, and defenses against cyber-terrorism in particular, are not identical concepts. Actions taken, for instance, to prevent others from stealing corporate secrets help with the former but are peripheral to the latter.

Likewise, improvements in the ability of organizations to manage disasters have a greater scope than simply warding off cyber-terrorism. Good people with experience and thorough training supplemented by sufficient exercises, strong security policies, and clear lines of communication all help.

Very little is known about the ability to contain the effects of cyber-terrorism from spreading within sectors or across them (and what little we know relates to the effects of natural events on power companies or software errors on telecommunications companies). Transmission can be direct (e.g., a virus) or indirect (a power outage shuts down credit card authorizations). The best one can hope to do is assess firewalls and circuit-breakers, but even a thorough census without deeper understanding is of limited help.

Metrics for motivation would amass several factors. One is the extent to which cyber-terrorism comes up in what can be learned about terrorists' plans: do they want to allocate effort to it; do they understand what it takes to carry out cyber-terrorism? Another includes the legal and social norms associated with computer hacking: what are the odds of getting caught (computer hacking is not considered a suicide mission); what are the penalties for so doing; what level of social condemnation (or applause) is associated with the deed? A last factor may well be the degree to which victims believe they would be hurt by cyber-terrorism: the greater their fear, the more terrorists may be motivated to try something.

Even the existence of good metrics (and no set of metrics for cyber-terrorism can be considered better than mediocre) does not make it measurable in practice. Data must still be collected. In some cases the data is good, or at least consistent and reliable. CERT (Computer Emergency Response Team) keeps a careful log of exploited faults. CSI (Computer Security Institute) conducts annual surveys of what per-

centage of responding organizations have been hacked and how much damage was thereby caused. Reporting on viruses and worms is vigorous. Graduate degrees in computer security are diligently tallied. But try to find out what is happening *within* organizations (many of whom do not know, themselves, how vulnerable they are). For the last several years the federal government has been trying to form various ISACs (industry sector advisory committees) as a forum through which organizations can share stories of computer intrusions and what came of them. Success has been modest. Of the six sectors targeted, ISACs have been, after great effort, formed in only four of them, and two of the four have no government participation (the two sectors with government participation have long been heavily regulated).

Incidentally, such confusion is at play even when the facts are there for distribution. Richard Clarke used to claim that a twelve-year old hacker had achieved control over the floodway machinery of the Roosevelt Dam. This was accepted as true until the story reached *The Washington Post* and was thereby brought to the attention of the plant's managers. After puzzling over the matter, they reported that the closest possible incident in question was a hacker attack by someone twice that age which never came anywhere close to those controls.

The State of Play

The best guess at this point is that the United States is somewhat better protected against cyber-terrorism today than it was prior to September 11th. But, that judgment is necessarily a reserved one based on only a year's worth of trends, many of which could turn around overnight based on the next piece of popular but buggy software or the next flash of inspiration among terrorists.

Security Awareness

September 11th, itself, certainly made people more aware of security in general, and therefore, cyber-terrorism. The collapse of the World Trade Center atop a Verizon central office switch eliminated most telecommunications services to lower Manhattan, forcing a mad scramble to recover service. A large percentage of the offices in the building, itself, had offsite data storage areas and therefore did not lose irreplaceable files. However, the experience provided a sharp reminder of why such backup and recovery plans were important and prompted people everywhere to revisit and upgrade their plans and procedures. A Morgan Stanley survey of CIOs taken after the attacks found that security software had jumped from their fifth to their first priority (*Economist* survey). That said, techniques of physical security differ from those of cyber-security: e.g., the networking that allows one system to fail over to another outside the blast zone, also makes it possible for attacks on one system to propagate to the other.

Incidents

Conceding that catastrophic cyber-terrorism and everyday cyber-mischief are but tangentially related, the correlation of forces between information security and systems attackers can be at least glimpsed in day-to-day statistics. Are things getting worse?

Yes and no. The most often quoted indicator of mischief is the CERT's tally of exploited weaknesses. The index rose apace with the growth of the Internet through 1995 and then leveled off for about three years (perhaps inexplicably, or perhaps the proliferation of CERT clones had resulted in incidents being reported to them and not getting to CERT). After 1998, the tally began to rise again, and exceed the Internet's growth rate somewhat. So here, it would appear that attackers are ascendant.

If one looks at really serious incidents, or the level of damage, the results are less grave. With all due caveats for the dynamic nature of conflict in cyberspace, the hit-or-miss quality of reporting, the usual perils of cost estimation by enthusiasts, and the perils of extrapolation from a thin base, it is entirely possible that history will record that the danger already peaked. The two most publicized incidents actually took place in 2000. One was the notorious I-Love-You virus in May. Although the Code Red worm (July, 2001) was notable (as were echoes such as SirCam and Nimda), it does not compare in terms of damage. The other was the distributed denial of service (ddos) attack that hit multiple Web (e.g., Yahoo,

Amazon.com) sites in February 2002. It is worth noting that a more seriously conducted ddos attack was carried out on 21 October 2002 against the 13 domain-name service root servers. Although eight were blocked for large periods of time, the other five picked up the load with the result that very few end-users noticed any difference at all in service. Hence, the CNET take on the incident: "Attack on Net Services Fails."

Worth asking -- to gauge the destructive potential of cyber-terrorism vis-à-vis more conventional terrorism -- is exactly how much damage these incidents caused. The ddos attack did put the major e-commerce sites out of business, but in no case was anyone down for more than three hours. If one estimates that these sites combined did $10 billion worth of business a year, then a three hour outage (in the context of a 24/7 operation) is about $5 million of lost business (plus cleanup costs). Copycats that emerged over the next few weeks had one to two orders of magnitude less effect. Estimates for the cost of the I-Love-You virus, by contrast, ranged as high as $10 billion (which would be equivalent to a major natural disaster were such information at all believable). When one considers that at very most 12 million people were affected (if that -- only one in twenty businesses reported any significant impact) and that the average loss in productivity among them cannot have been very large (for some, a day without e-mail may have been even more productive), a true figure has to be ten to one-hundred times less. The Computer Security Institute maintains an annual poll of damage from *all* cyber incidents effecting major organizations; their numbers have yet to cross a billion dollars a year (among responders). A final statistic, useful more for its value as a trend than as an absolute sum: the London consultancy, mi2G, estimates that the projected economic damage for overt digital attacks worldwide, despite the numbers having doubled from 30,000 to 70,000, will have actually fallen from $7.7 billion in 2001 to $7.3 billion in 2002.

It is undeniable that the amount of junk flowing through the Internet is on the rise. One source even estimated early this year that as much as five to ten percent of all packets in circulation may be part of one ddos attack or another. What is more apparent to the average user is the rise in junk mail, from perhaps less than one in ten e-mail messages a year or two ago, to something close to one in three. It remains an open question whether the worldwide commons of cyberspace can be protected against pollution of such sorts as long as the cost of sending any given packet is zero. Nevertheless, the volume of junk has not yet created a groundswell in favor of metered pricing of the sort that would impose costs on spammers (although this hesitancy may be cultural and historic rather than economic: GSM's messaging service is growing quite lustfully despite per-byte metering).

Lest a rising tide of cyber-pollution be considered symptomatic of a growing risk of cyber-terrorism, the reverse may well be true. It is now well-accepted that a modicum of pathogens in a child's environment (e.g., from dirt or house pets) leads to a decrease in serious diseases because the child's reactions build up its immune systems. Similarly, the growing understanding that cyberspace is a chancy environment is prompting a healthy growth in attention to cyber-security.

Preparation

There is considerable evidence that the software sector (both the money-making and the open source sides) is paying more attention to security.

The most important announcement to that effect was Bill Gates' declaration in January 2002 that Microsoft would, henceforth, take security as seriously as it took the Internet. As a result, Microsoft's development staffers, 8000 strong, were told to stand down for six weeks while they learned or re-learned the essentials of security and the techniques for reliable code-making. Microsoft executives now declare that a security hole, once discovered, is enough to cause shipments to be slipped. Microsoft has also been liberally announcing security holes and patches, averaging roughly one and a half major bugs a week since then. There are three ways to look at this announcement. One: Microsoft could be taking responsibility for the awful state of computer security occasioned by its past inattention to the matter (unlikely). Two: Microsoft is responding to publicized complaints (notably, but not exclusively, by the Gartner group) that its inattention to security makes it ineligible for mission-critical applications (likely).

Three: Microsoft, which is laboring mightily to alter its business base from one-time sales to subscriptions for periodic upgrades, is using the security argument to bolster the market for upgrades by castigating its old products as insecure by comparison to what will be coming (anyone's guess). It is too soon to say whether the announced attention to security will result in dramatically more secure products. Nevertheless, the newest versions of its operating system, SQL server software, and web-servers being shipped, now default to secure rather than insecure mode; many security-problematic features have to be explicitly turned on rather than explicitly disabled.

The continued rise in Linux and other open-source products is also a source of some encouragement for computer security. This is not necessarily because Linux is more secure than Microsoft's Windows (there is considerable dispute on that point even though an elder cousin of Linux, BSD Unix, has a very good security reputation). The point is more that Linux is more open and therefore putatively easier to patch but clearly easier to tweak for the precise security policies that an organization wants to follow. Over the last few years, Microsoft has been more willing to show large customers (e.g., the U.S. Government) more of its source code, but it is the rare case where they will allow others to tweak it for their own use. Incidentally, overseas governments (notably China) have started to favor Linux out of highly paranoid fear that Microsoft has placed back doors in its operating system that would permit the U.S. Government to manipulate customer systems in a crisis.

The academic and research community has continued, with ever-more generous funding, to improve the state of knowledge of computer security. It is noteworthy that in the last year, security holes have been found in established erstwhile-faultless programs (e.g., Keberos security suite) and protocols such as SNMP (for network management) and ASN.1 (for expressing formatting). Since all three are well into their second decade of use with no record of these holes having been exploited, such activity is tribute to the increasing diligence and competence of the white-hat hacker community.

How well the white-hat hacker community will thrive in the years to come, ironically, has a great deal to do with the current struggle over the protection of intellectual property. Why? The rise of the Internet has placed owners of music, video and other forms of entertainment in a bind. On the one hand, the economics of distribution are clearly moving from atoms to bits. On the other hand, it is far easier to pirate and disseminate digitally encoded entertainment than its analog counterpart (e.g., the quality of analog material deteriorate with every copy; not so with digital material). The technical response to this dilemma has been to develop cryptographic locks for certain forms of media so that they can only be played by the (hardware of the) person who bought the first copy. The effort has been frustrated by the truism that embedded encryption has a short lifespan (hackers that physically possess the product can bang away at until they "break" it). To supplement what is fragile technology, the media industry persuaded Congress to pass the Digital Millennium Copyright Act, which makes it a federal crime to circumvent security systems *or even describe how it would be done*. A Russian software engineer was charged, under the DMCA, with publicizing exploits against weaknesses in Adobe's electronic book format. Until HP thought better of it, the DMCA was also held as a club over a company that distributed techniques for breaking its Tru64 Unix operating system.

In March, 2003, Executive Order 12958 was amended to permit vulnerabilities of the national infrastructure -- and thus, presumably, the Internet -- to be classified at a secret level or higher. Whether this chills the current discussions of information system vulnerabilities remains to be seen; unlikely, but not impossible.

The security community has also been engaged in a debate over what to do when a bug is found: should there be a quiet communication with the vendor or an announcement to the world? Microsoft has been campaigning for the former but others respond that Microsoft, itself, has been slow to patch bugs. Unfortunately, even an announced bug patch is likely to lead to a wave of exploits inasmuch as hackers are likely to reverse engineer the patch to discover the bug, and then develop and deploy an exploit for the bug -- and all this before the patches are widely installed.

The rise of wireless networking is one other trend whose impact on security merits note. In the wave of enthusiasm over the wireless local-area-networking technology, 802.11b (or Wi-Fi: wireless Ethernet), the

security holes in the protocol have received insufficient attention. As a rule of thumb, for every three 802.11b networks; one of them has no security turned on whatsoever (so that anyone within broadcasting range can listen and inject anything into the network); one has turned on the easily-breakable security that comes with it standard; and one layers a real security package (e.g., a virtual private network) on top. Many organizations have found themselves plagued with rogue 802.11b junctions just waiting for trouble. Expect more of the same if and when electronic devices appear pre-equipped with Bluetooth (a short-range point-to-point networking protocol that allows equipped electronic devices to "find" one another, and begin conversation). Finally, now that palmtops are beginning to be infected by viruses, the convergence between palmtops and telephones suggests the possibility of telephone zombies which may have a lot more potential to congest phone lines than ddos attacks can congest the Internet.

The Environment

Threat, standards, insurance, and laws bear note: evidence of intent to commit cyber-terrorism remains hard to find. A great deal was made of the discovery in Afghanistan that someone had downloaded descriptions of various SCADA systems. This, by itself, proves nothing more than a cursory interest in the field. (One could speculate that someone may have heard that attacking SCADA systems could disable power infrastructures and decided to see what the fuss was about -- concluding such attacks were too difficult or insufficiently exciting). Among all web sites defaced, the percentage done for political reasons, although rising, is only ten percent so far -- and defaced web sites hardly fit the definition of "terror."

The good news on standards is that the metrics community is intensifying its efforts to try to measure good security. The use of "common criteria" to measure software quality, for instance, is increasing. Of perhaps greater relevance is the adoption of ISO 17799 (an international adaptation of a British Standard 7799), which attempts to measure the quality of an organization's information security process. ISO 17799 is analogous to ISO 9000 (dealing with the quality control process) and ISO 14000 (dealing with the environmental management process). If it works it will be possible to assess (and thereby create pressure to raise) the quality of an organization's information security on an ongoing basis. The development of a robust insurance business to cover damage from cyber-attacks would also put the wind behind standards. There is some activity (enough so that the aforementioned Cyberpane can claim that the use of its services will cut insurance premiums by a quarter), but such insurance is by no means universal.

On the legal front, the European Commission has crafted a directive on cyber-crime that has already been converted into legislation in multiple European countries. This should make it easier to both investigate and prosecute alleged attacks of cyber-terrorism. In the United States, the most noteworthy development has been the Department of Homeland Security's absorption of the Critical Infrastructure Assurance Office (CIAO) and the National Infrastructure Protection Center (NIPC) (except for cyber-crime prosecution). In September 2002, Richard Clarke (then point-man for cyber-security at the National Security Council) released a for-comment draft of a new national strategy on cyber-terrorism, which was more remarkable for its lack of content than for anything it actually said. Emblematic of its approach was its focus on the security of home computers lest they be involved in zombie attacks.

After Richard Clarke left, the report that was finally issued had what little content was in it completely flushed away. To illustrate as much, consider the recommendations from each of the five sections by focusing on the verbs (either as stated or as inferred: e.g., develop an assessment = "assess"). Section 1 had seven recommendations: appoint, complete, evaluate, encourage, encourage, raise awareness, and encourage. Section 2 recommended: share, assess, convene, cooperate, develop (best practices), disclose, share (e.g., implement a clearinghouse), encourage, partner, support volunteers, coordinate, coordinate, encourage, facilitate, and facilitate. For Section 3 the verbs were: facilitate, encourage, convene, encourage, encourage, (no verb), implement (training programs), develop, and encourage. Section 4 would: deploy (automated security tools within federal networks), review, consider, review, explore, and encourage. Finally, Section 5 boldly declaims: ensure, attribute, coordinate, reserve (the national right to respond in an appropriate manner), facilitate, identify, encourage, foster, encourage, and, finally, encourage. None of this is terribly encouraging.

As the *Economist* concluded, "the lily-livered approach [of the for-comment draft of the national strategy on cyber-terrorism] approach might, in fact be the best one. When a risk has been overstated, inaction may be the best policy." That noted, even Richard Clarke makes the case that cyber-security is less justified by its ability to thwart the low-risk possibility of cyber-terrorism, but to counter the day-to-day run of cyber-attacks (from November 2002 *Washington Monthly*).

Toward an Agenda

To frame the policy discussion, start with the basic economics question: do people systematically underinvest in systems security? There are two quick reasons that they might -- both familiar ones. First, those who invest in research create positive externalities (e.g., a spillover in knowledge) that they cannot harvest thus they do less than they should. Of course, cyber-security is not the only place this holds. The force of this argument is why government investment in R&D is well-accepted and substantial -- even, perhaps especially, for information security (although much of the research is motivated by government-unique problems). Second, in concentrated industries, a firm's incentives reflect not only cost/value calculations but the effects of investment in market share. So, a company with a dominant market share could conceivably ignore security and not sweat the consequences.

Perhaps, people are simply unaware of how insecure they are. After all, computer security is an arcane topic to most people, and attempts to master the subject are constantly undermined by rapid shifts in the essential particulars (e.g., within the last few years the most common source of malicious code shifted from boot-sector viruses to macro viruses and then from macro viruses to worms). But, ignorance does not necessarily indicate under-investment. Over-investment -- especially if driven by fear -- is also possible. The more experience people have with their own security environment, the harder it is for government (or any other "expert") to claim it knows better.

Two other reasons for under-investment bring us closer to policy responses.

One is the harm done to others. Both feckless users that allow their computers to be turned into zombies, or spewers of spam levy costs on others by their polluting the medium. A potentially greater problem may arise from attacks on public utilities (again, in theory). Someone dependent upon electricity, for instance, can experience great discomfort by losing it. Unless power companies (phone companies, etc.) feel the pain (lost sales are a trifle in such cases) they may be apt to be a little sloppy about securing their own systems (although empirical evidence to that effect is not compelling at this point). There is also some, albeit ill-understood, potential for induced faults to hopscotch from one victim to another within consolidated infrastructures.

The second has to do with scale. Some may believe that they have to cover small losses, but reason with some basis, that the costs of a widespread catastrophe will be borne by others. Indeed, one of the more pernicious aspects of any discussion about cyber-terrorism is that, by likening it to war, the appearance is given that attacks give rise to their declaring force majeure. As war victims, people or companies can demand and hope to get indemnification for third party losses.

Comparison to what happened in preparation for the year 2000 may be apposite here. Prior to the event, at least one prominent analyst (Edward Yardeni) claimed that there was almost a 50:50 chance of a resulting recession. The National Intelligence Council was braced for a wave of chaos as infrastructure failed globally. Remediation costs upwards of $100 billion were multiplied by expectations that a subsequent wave of finger-pointing would culminate in a trillion dollars worth of lawsuits. Federal officials manned command centers to watch over a country celebrating, in the event the transition to a new millennium proved to be the Comet Kahoutek of computerdom. What failures occurred were minor and the total sum of inconvenience even more so. True, close to $50 billion was expended in warding off disaster, and it is clear that the problem would not have gone away on its own. It is less clear, in retrospect, whether the right amount of money was spent. Countries and sectors less frightened about the problem, and thus more inclined to put things off until much closer to the date, did not seem to experience the ill-effects of their ostensible improvidence. Two lessons may be drawn from all this. One is that today's

infrastructure -- the combination of systems and people -- may perhaps be more robust than commonly believed. Two is that the problems one sees coming are not the ones likely to cause problems. Networks may be resilient to the extent that people worry that they are not.

An Agenda for Appropriate Action

These factors suggest a modeled agenda to reduce the risk level from cyber-terrorism down to fair levels.

First, stop thinking of cyber-security in terms of cyber-terrorism. Do not lodge the issue in the National Security Council and link it only lightly with other concerns in the Department of Homeland Security. System owners have no one but themselves to blame if they are hacked. People, by contrast, cannot avoid breathing and thus cannot avoid being victims of, for example, an anthrax attack. Vulnerabilities matter; attackers, less so. Encourage others to think of security as a "best practice," not as a fortification.

Second, establish as a matter of law and expectation that a regime of strict liability will apply to those whose fecklessness in the protection of their own systems harms third parties -- force majeure should not be accepted. In other words, institutions that have legal, charter, or contractual requirements to provide services (e.g., electricity), assure information (e.g., keep proper bank accounts), or protect information (e.g., confidentiality of health records) cannot blame cyber-terrorists for their failures. National Academy of Science (NAS) reports have advocated a regime of liability for software makers as well, but this may be premature until much better software quality metrics exist.

Third, within a vigorous R&D program, emphasize research on metrics for security (see above), and a more fundamental understanding of how faults propagate across infrastructures (see below).

Fourth, insofar as the government exercises its concern of information security it should concentrate strongly on public infrastructures -- not the least of which are its own. These sectors have historically been associated with tests of public convenience and necessity. Most of them also interoperate with their peers, creating the possibility that the weaknesses of one may become the weaknesses of all.

Fifth, laws and rules that mandate that incumbent infrastructure providers grant potential competitors fair access to their networks and facilities should be reviewed to ensure that such access does not create information security vulnerabilities.

Sixth, anything that can encourage the transition from the fourth to the sixth version of the Internet Protocol (i.e., from IPv4 to IPv6) is a good step on the way to limiting the potential of ddos attacks.

Prospects

As with any policy, were the merits so obvious and the countervailing interests so weak, it would have come to pass by now. That noted, the prospect for such an agenda is not daunting. As people grow more sophisticated about information security, they will recognize cyber-terrorism for the exaggeration that it is -- while also recognizing system security for the necessity that it is. So, stopping the over-reacting (item 1) and concentrating on infrastructures (item 4) are plausible. Two other items require modest funding reallocations (no more than $100 million a year): shifting the emphasis of information security R&D (item 3) and leaning towards IPv6 (item 6). Neither are impossible, and item 6 is inevitable, if not immediate.

The two agenda items related to regulation and liability (items 5 and 2) are within range. The impact of deregulation on infrastructure security has largely been an esoteric and technical topic and thus not yet part of the political agenda. Anything that would harm competitors at the expense of incumbents would be opposed by the former and applauded by the latter -- but the first agenda item is to understand what needs to be done to cauterize such connections. The paucity of cases dealing with third party harm as a result of computer intrusions means that no one knows that the liability regimes actually are in practice.

Government policy could be leaning on an open door. Software liability, for its part, would be vigorously opposed. But until software metrics improve, it is a deservedly notional idea.

Conclusions

The Beltway sniper's attacks of October 2002 provided a reminder, as if anyone needed any, of what terror was. People worried for their own safety. Parents were especially worried for their children. By contrast, there is nothing anyone can do to a person's computer that can generate such terror. Were it possible that attacks on information systems were capable of killing people, then at least some element of terror would be present. As a general rule, however, those systems whose misbehavior could put people at risk are well protected, or should be. Any system that can harm people through software faults and does not accord to widely-recognized fail-safe principles may therefore be considered badly engineered -- with or without the existence of terrorists.

That said, the national (and international) information infrastructure is by no means secure, and it is possible that a persistent, clever, and/or lucky attack upon portions of it can cause far more grief than it should. The best way to manage such a risk is to recognize the risk for what it is. The trick is to focus on the few critical infrastructures, understand them, and ensure that their owners have incentive to protect them.

AN ASSESSMENT OF FEDERAL CRITICAL INFRASTRUCTURE PROTECTION EFFORTS SINCE SEPTEMBER 11

Michael Scardaville

The September 11 attacks on the World Trade Center and the Pentagon demonstrated the willingness and ability of international terrorist organizations to take advantage of unrecognized weaknesses in the aviation industry[1] to conduct large-scale attacks against the United States. Further, this interest has apparently not subsided nor is the aviation sector Al Qaeda's only target. Computers have reportedly been found during the military campaign in Afghanistan containing structural analysis programs for dams and other information related to supervisory control and data acquisition (SCADA) systems for water facilities.[2] More recently, FBI Director Robert Mueller testified in front of the Senate Select Committee on Intelligence that "symbols of U.S. economic power" and the "transportation and energy infrastructures" are prime targets for Al Qaeda due to their belief that attacks on such targets would cause substantial economic disruption. As a result, efforts to protect the critical infrastructure nodes that support the physical and economic well being of the United States are more important than ever.

More robust security programs need to be infused into the business practices of those industries that are crucial to national operations, economic vitality, and public well being. Doing so, however, is a complex undertaking that involves actors both in and out of government. In order to succeed in making private industries more secure the federal government will need to assist the private sector in developing its security programs, and business must provide government with sufficient information to evaluate the vulnerability and potential consequences of a successful attack. In fact, the extent to which business and industry are able to assist each others' infrastructure protection policies is likely to prove one of the most central determinants of whether or not critical infrastructure protection efforts are succeeding.

Such cooperation will require a closer partnership between the public and private sectors. Developing a strong working relationship between industry and government for critical infrastructure protection will necessitate a major reassessment of pre-September 11 programs and policies and a restructuring of the federal bureaucracy to meet current needs. Infrastructure protection efforts must be built into a layered national strategy to combat terrorism. An effective critical infrastructure protection program should establish a deterrent against attacks on vital nodes, point-of-incident protections and consequence mitigation, and reconstitution efforts to lessen the impact of a successful attack.

Presently, the federal critical infrastructure protection program is in the design and early implementation phase and will likely require additional time to be fully implemented. Nonetheless, some crucial building blocks have been laid over the last eighteen months.

Challenges and Opportunities

Like most aspects of homeland security policy, critical infrastructure protection presents unique jurisdictional and governance issues that are not as prevalent when considering traditional defense and national security matters. Responsibility for protecting vital nodes is shared among federal, state, and local authorities as well as the owners and operators of the facilities in question. An effective policy will require close cooperation between all levels of government and between government and the private sector. Furthermore, this relationship must be developed in a manner that promotes security while not harming the economy.

Private industry owns between 85 and 90 percent of the assets vital to national operations and well-being. Private owners, however, did not go into business to secure an industry's nodes for public use, but to make a profit. As a result, their investment decisions are based primarily on bottom-lines, consumer and shareholder confidence, and other market forces. This does not mean, however, that industry does not spend money on security. On the contrary, most business owners recognize that excessive vulnerabilities can affect their profits through decreased consumer and shareholder confidence and reduced productivity, as well as higher insurance premiums. This is particularly true if their facilities were the target of a successful terrorist attack or were used by a terrorist to facilitate an attack. Indeed, one only need look at the dramatic economic effect the September 11 attacks have had on the aviation industry to recognize that there is a strong business case for private investment in security.[3] Nonetheless, decisions

on how much security and what kind will be based on a balanced consideration of a variety of economic factors including the need for protective measures.

In order to balance such competing interests, most businesses rely on risk management tools to identify risks, evaluate how serious they are and suggest appropriate counter measures based on the potential likelihood and consequences of a disruptive event. For example, in November 2002, the National Infrastructure Protection Center (NIPC) recommended a five-step risk management tool to industry that included:[4]

1. An Asset Assessment to identify those nodes critical to operations;
2. A Threat Assessment to identify potential adversaries, their intent and their capability;
3. A Vulnerability Assessment to determine weaknesses in the assets in step one that an adversary identified in step two may exploit;
4. A Risk Assessment, which is intended to balance the findings of the first three steps; and,
5. The Identification of Countermeasure Options.

In this process, each step builds off the decisions made in the previous steps. In short, a manager must first identify what assets are crucial, determine whether there exists a credible threat to those assets, evaluate what aspects of that asset make it accessible to attack, and decide what to do about it.

Of these five steps, the one that has the greatest risk of causing an under-investment in a business's critical infrastructure protection efforts is step two, threat assessment. In the past, industries have viewed the likelihood of terrorism as low[5] and had little understanding of the nature of the threat. September 11 has convinced many in industry that they and their systems are, in fact, potential terrorist targets and that some kind of attack is likely to occur in the near future. However, they still need a more comprehensive understanding of what the nature of threat is in order to develop and implement the most effective protection and response strategy. In fact, NIPC recommends that the person conducting the risk assessment must "determine if [the potential adversaries] have the *intent and capability* to cause an unwanted event and their *history* [proven track record] of successful attacks against types of assets identified in step one."[6] While there is a broad appreciation of groups like Al Qaeda and their intent and capability to attack American targets as well as their history of recent success, rarely is this information available with sufficient detail to guide business procurement practices.


Reuters

From the government's perspective, the greatest challenge facing officials responsible for infrastructure protection policy is how to affect the size and scope of private investment in security. There are many means a government agency could use to achieve these goals, but like their commercial sector counterparts, policy makers must weigh the potential costs and consequences of the various tools at their disposal. For example, regulation is a tool frequently used by government agencies to ensure businesses follow certain practices (i.e. safe working conditions) but regulation typically has a net negative effect on the industry and the broader economy. Indeed, according to the Cato Institute, regulation already cost industry $854 billion in 2001, or 8.4 percent of the United States gross domestic product.[7] In addition, the Office of Management and Budget has estimated that regulation currently costs businesses seven billion hours of employee time per year.[8] Adding to this burden may help meet one national objective, improving security, only to detract from others, including a healthy and vibrant economy. In addition, the frequent use of strong-arm tools such as regulation is likely to create a hostile environment between the regulator and the regulated.

Therefore, a better policy would be to attempt to influence the risk management calculations made in boardrooms across America through information sharing, cooperation and incentives instead of coercion

or regulation. Developing a close working partnership between industry and government members of one sector can provide the other with the information it lacks to make a fully informed decision. Industry needs to better understand the threat as well as lessons learned about vulnerabilities and different corrective means. Government, on the other hand, needs a better assessment of the vulnerabilities in America's infrastructures to better analyze the risk a particular threat may pose so it can develop policy and technological countermeasures. Likewise, the two can collaborate to determine what policies would best deter, prevent and respond to attacks. However, this will require an unprecedented degree of cooperative communication between government and industry. In the past, a number of roadblocks, including mistrust of how government will use information industry shares with it and the legal consequences of collaboration, have prevented such coordination. Removing such obstacles must be a top priority and, fortunately, Congress and the Bush Administration are already removing some of the most glaring.

With the major roadblocks to partnership removed, however, individual businesses may still choose to invest in sub-par security programs. When this proves to be the case, the federal government will have to take more direct action to promote investment. While regulation is the typical means by which government moves industry into particular policy decisions, providing incentives can be a more economical and amicable method. Government security incentives can act as a catalyst to the existing market forces that drive business decisions. For example, most investors seek a degree of security in the shares they buy in a business. That security is based in part on the company's ability to continue operations. Since a terrorist attack has the potential to disrupt operations, private security measures should be of concern to somebody considering buying shares in a company. Similar forces drive the decisions of consumers and insurers. The Department of Homeland Security (DHS) could use this tendency to promote better security investment by an individual corporation by operating a security credentialing program to certify that a given company meets DHS minimum standards for infrastructure protection. Investors, consumers and insurers could then look for DHS certification when deciding whether or not to invest in, purchase from or insure a given company.

In addition to challenges inherent in the private sector and those that arise from the intersection of private and public interest, potential problems can arise due to the number of federal agencies with a role to play in critical infrastructure protection policy. In fact, prior to the establishment of the Department of Homeland Security, the United States General Accounting Office identified the lack of a clear division of responsibilities among federal agencies with critical infrastructure protection policies as a major obstacle to policy implementation.[9] While the creation of the DHS solves some of these problems, the current National Strategy for the Physical Protection of Critical Infrastructure and Key Assets assigns responsibilities for infrastructure protection efforts to, in addition to the Department of Homeland Security, the Departments of Agriculture, Health and Human Services, Defense, Energy, Treasury, Interior and the Environmental Protection Agency. While on the surface this arrangement seems like a recipe for a bureaucratic disaster, it is also necessary as these other federal agencies have direct regulatory responsibilities for a variety of critical industries and will have relationships with industry for more daily operational matters. Secretary of Homeland Security, Tom Ridge, will have the additional responsibility of ensuring these other federal agencies adhere to plans developed by the DHS and also cross-sector convergence.

What Determines Success?

A successful critical infrastructure protection policy will respond to these challenges and establish a deterrent against attacks on vital infrastructure nodes, point-of-incident protections through industrial efforts to prevent attacks as they are being initiated, and consequence mitigation and reconstitution plans to lessen the impact of a successful strike. Preventing all future attacks on critical infrastructure or the use of vulnerabilities in one sector to conduct an attack is not a reliable measure of success in and of itself. However, being able to prevent the majority of attacks and reduce the consequences of a successful attack must continue to be a primary national objective. A successful attack with unconstrained consequences would, nonetheless, illustrate a single point of incident failure if not broader systematic deficiencies.

Since neither the federal government nor industry alone can fully secure national infrastructures from attack, the broad objective needs to be the creation of an environment where government and industry can freely share information related to threats, protection/deterrence measures, and consequence mitigation and reconstitution efforts while collaborating over the specific objectives and security visions. Such an arrangement can provide both industry and government with the knowledge to make better investment and policy decisions. However, such a program cannot be developed overnight and will require a number of steps before it can be realized, including:

- Removal of pre-existing roadblocks to effective cooperation and establishing the federal government as a reliable interlocutor for industry. Both sides must be able to trust each other and believe that the relationship will provide them with a constant benefit.

- Re-evaluation of pre-September 11 policy priorities in light of the changed international security environment and new objectives must be developed to fit these circumstances. For example, the historical emphasis on cyber-security and incident response measures should be reconsidered in light of Al Qaeda's ability to exploit systematic vulnerabilities in the aviation sector using low-tech means to conduct mass casualty attacks.

- Development of structures around the determined objectives instead of trying to force new ideas into old bureaucracies. The establishment of the Department of Homeland Security this year creates an opportunity to restructure federal critical infrastructure protection efforts to operate as efficiently as possible.

- Forming partnerships which can be sustained and are mutually beneficial. Both business and government must feel their needs are being met for an effective partnership to be sustainable.

A prime determinant of the federal government's success in developing such a collaborative environment will be an increase in private security practices without a corresponding increase in regulation. If a federal agency determines that regulation is necessary in a specific area it will be a prime indicator that partnership and market-based efforts have failed in that sector. At that time, policymakers will have to weigh what can be gained through security regulation versus the economic and other costs associated with such rules. Like the responsibility for securing infrastructure itself, the burden for ensuring that partnership efforts do not fail and regulation does not become the norm rest with both industry and government.

A Brief History of Critical Infrastructure Protection Prior to September 11

Like many areas of homeland security policy, critical infrastructure protection efforts are not new but have become more visible and more important. In fact, most of the structures and policy perspectives that continue to guide federal critical infrastructure protection policy grew out of Presidential Decision Directive 63 (PDD-63) signed by President Bill Clinton on May 22, 1998, and the report of the President's Commission on Critical Infrastructure Protection[10] on which it was based.

The President's Commission recognized that communication between government and industry would be crucial to protecting the cyber assets of critical infrastructure[11] owners and operators and recommended the creation of a variety of programs in the federal government to better achieve such information sharing, including a White House policymaker, a National Infrastructure Assurance Office in the National Security Council (with a support staff in the Department of Commerce), a Presidential advisory board and clearing houses for each industry sector identified. It also emphasized the need for better analysis on the nature of the threat to critical infrastructure and the vulnerabilities in its operations. The Commission early on also recognized that a number of legal obstacles, such as a lack of clarity in the freedom of information act, might result in impediments to effective information sharing.

The findings of the Commission were largely incorporated into PDD-63. It stated the Clinton Administration's policy as "the United States will take all necessary measures to swiftly eliminate any sig-

nificant vulnerability to both physical and cyber attacks on our critical infrastructure, including especially our cyber systems" and established a national goal of establishing an initial critical infrastructure protection policy by 2000, and a fully implemented program by 2003. The directive called for the establishment of a "genuine, mutual and cooperative" relationship between industry and government. PDD-63 also sought to improve cooperation without regulation or unfunded mandates "to the extent possible."

Most importantly, PDD-63 established a structure for implementing this policy that carried through the establishment of the DHS with some elements continuing today. Specifically, the directive designated 11 federal agencies as Lead Federal Agencies and assigned them the responsibility to interact with the nine industries identified as critical.[12] In addition, the directive created a National Coordinator for Security, Infrastructure Protection and Counter-terrorism in the National Security Council who would also chair the interagency Critical Infrastructure Coordination Group, the National Infrastructure Assurance Council to provide the President with advice from the private sector. PDD-63 also required the federal government to begin developing plans for analyzing vulnerabilities, correcting them, warning, response, reconstitution, education, research and development, intelligence collection, international cooperation, and legislative and budgetary requirements.

While PDD-63 established critical infrastructure protection as a national priority and created a structure for its implementation, neither the goals of the directive or the vision of the President's Commission on which it was based have been fully met. As recently as last year, the General Accounting Office (GAO) concluded "efforts to perform substantive, comprehensive analyses of infrastructure vulnerabilities and the development of remedial plans has been limited."[13] The GAO also concluded that federal threat analysis and warning efforts were insufficient although programs initiated by the National Infrastructure Protection Center laid groundwork for effective distribution once developed.[14] Most importantly, federal efforts to date have yet to result in an effective public private partnership for critical infrastructure protection.[15] In short, prior to the September 11, 2001 attacks on the World Trade Center and the Pentagon, critical infrastructure protection policy was recognized as a necessity but was not pursued with sufficient vigor to meet the growing threat.

In addition, federal critical infrastructure protection efforts since 1998 have focused heavily on securing information systems and the internet. In fact, PDD-63 directly called for such an emphasis. While addressing cyber-security concerns is an important component of critical infrastructure protection, particularly with the ever increasing number of cyber intrusions occurring annually[16] and the internet's quality as an enabler of other systems, physical security and interdependent network protection must form a comparable priority as their disruption or destruction could cause extensive public harm. Likewise, most efforts to date have focused on analyzing cyber intrusions after they occur and cataloging hacker trends in order to learn how to prevent similar future attacks and mitigate the impact of the attack. Such a program relies on a successful attack as the motivating factor for new protective measures, a situation that is unacceptable in the age of mass casualty terrorism.

New Policies Initiated Since September 11

September 11 required a comprehensive reassessment of what was being done and the scope of the program. On October 16, 2001, President Bush signed Executive Order 13231 (EO13231), which outlined the administration's initial policy on critical infrastructure protection as "to protect against the disruption of the operation of information systems for critical infrastructure and thereby help protect the people, economy, essential human and government services, and national security of the United States, and to ensure that any disruptions that occur are infrequent, of minimal duration, and manageable, and cause the least damage possible." EO13231 also created the President's Critical Infrastructure Protection Board (PCIPB), which was comprised of members of the senior executive staff[17] and chaired by the Special Advisor to the President for Cyberspace Security, and the National Infrastructure Advisory Council (NIAC) comprised of members of the private sector.[18] The PCIPB was directed to "recommend policies and coordinate programs for protecting information systems for critical infrastructure" but has been disbanded by Presidential Directive since the creation of the Department of Homeland Security.[19] Its responsibility for coordinating federal critical infrastructure protection policy will likely be absorbed by the new Homeland

Security Council. Meanwhile the NIAC was given the responsibility of providing "the President advice on the security of information systems."[20] The directive's statement of policy and the establishment of the PCIPB and the NIAC codified the pre-existing tendency to focus on cyber-security issues to the detriment of physical security efforts by specifically concentrating federal efforts entirely on information systems. In addition to the policy initiatives of EO13231, the establishment of the Department of Homeland Security in November 2002 offers significant advantages to the implementation of federal CIP policy. Specifically the Homeland Security Act of 2002 (P.L. 107-296), which established the department, transferred the National Infrastructure Protection Center (NIPC), the Critical Infrastructure Assurance Office (CIAO), (FedCIRC), the energy security and assurance programs of the Department of Energy, the National Infrastructure Simulation and Analysis Center (NISAC), the National Communication System (NCS) and consolidated them into the Department's Information Analysis and Infrastructure Protection Directorate (IAIP). Combined, these agencies were responsible for most broad aspects of federal CIP policy (with specific sector coordination handled by other offices within the designated federal lead agencies). It is important to recognize that when these agencies were transferred to the Department they lost their unique identities and were melded into six offices: Competitive Analysis and Evaluation and Planning and Partnerships, both of which report to the Under Secretary for Information Analysis and Infrastructure Protection; the Infrastructure Coordination Division and Infrastructure Protection Division, which fall under the Assistant Secretary of Homeland Security for Infrastructure Protection; and the Risk Assessment Division and Information and Warnings Division, which answer to the Assistant Secretary of Homeland Security for Information Analysis.

By consolidating the functions of these agencies within IAIP, many of the coordination problems that previously existed can be resolved. Under the new department, responsibility for policy, planning, analysis and warning will all ultimately fall under one Undersecretary instead of being spread across the federal government. Partnership initiatives will still be undertaken by a variety of federal agencies, but with the DHS responsible for the overall partnership initiative, national strategies and priorities and the fusing of terrorism-related information analysis with information on business practices and vulnerabilities.

Reuters

The creation of the DHS also affords the federal government the opportunity to fundamentally reassess how it conducts CIP policy in light of the new strategic environment post-September 11. By placing those federal agencies responsible for critical infrastructure protection policy in the same directorate that is responsible for information analysis, the DHS should allow for an unprecedented incorporation of threat assessment data into infrastructure protection efforts. As a result, the DHS should be better equipped to provide industry with the detailed threat analysis it needs to adequately undertake its risk management calculations. This increased emphasis on information analysis should also allow the DHS to work with industry to include more preventive measures absent an attack instead of stressing new mechanisms industry should adopt in response to a successful attack. Likewise, by combining responsibility for analyzing threats and vulnerabilities into one directorate, the DHS should be able to develop a more comprehensive assessment of the level of risk various industries and regions currently face. This should enable the department to better prioritize its research, funding and targeted outreach efforts. This, however, is not to suggest that broad industry partnerships should be disavowed in favor of targeted relationships based on intelligence data. The intelligence community will rarely know the full scope of plans current and future terrorists may be developing. Likewise, these organizations can change their plans much more quickly than relationships can be developed and security investments made. Any program that focused only on those sectors being targeted by terrorists would likely then create new vulnerabilities and potential targets.

The Homeland Security Act of 2002 also offered a number of legal protections private industry had long been calling for as a prerequisite to closer cooperation with government. First, the Act provided anti-trust protections to businesses that shared information related to infrastructure vulnerabilities or protection measures either directly or through an ISAC. This provision allowed them to share information in order to protect an entire sector without fear of being brought to court for uncompetitive business practices.

Second, the Act expressly exempted information related to critical infrastructure protection efforts voluntarily shared by industry with government from release under the Freedom of Information Act (P.L. 93-502). Many in the private sector had long viewed such an explicit exemption as necessary before they would share information with government.[21] Industry sought this exemption even though the existing exemptions in the Act already protected "trade secrets and commercial or financial information obtained from a person and privileged or confidential"[22] because it was feared that the Act's existing exemption language was too vague to reliably protect voluntarily shared information.[23] While lawyers may quibble whether or not this was the case,[24] the important thing was that the lack of clarity in FOIA created an obstacle to effective information exchange. As Ronald L. Dick, former Director of the National Infrastructure Protection Center has noted, "the question of whether in the abstract we could protect the information becomes meaningless if the companies will not give us the information in the first place. Many companies seek certain outcomes, and they don't want to rely on a judge's decision"[25] or more succinctly, "if the private sector doesn't think the law is clear, then by definition it isn't clear."[26]

Critics of this provision argue that it is a dramatic increase in government secrecy. However such concerns are mistaken. First, if pre-existing FOIA exemptions did, in fact, already protect such information, then the amendment included in the Homeland Security Act merely clarified what was already a law. If existing law did not protect this proprietary information, industry would likely continue to abstain from sharing it with government. As a result, individual citizens would not be able to obtain it through a FOIA request. Simply put, no information that was previously public has been made secret.

The DHS has not yet released a final ruling on how it will manage voluntary submissions of critical infrastructure information, but is currently accepting comments on a draft rule,[27] which should meet the concerns voiced by industry. While the draft rule meets this important challenge it should also incorporate a checklist that the program manager responsible for reviewing voluntary submissions will follow to determine whether the information submitted is truly related to critical infrastructure protection. While the ruling requires the program manager to make such a determination, increasing transparency over how that decision is made is important in ensuring the spirit of the FOIA is not trampled on.

Since the program details have yet to be finalized, it is too early to determine the impact of these exemptions. However, by providing the legal clarity business had long sought, a major hurdle to effective information sharing has been removed. The onus is now on industry to begin sharing more information with the DHS and other federal lead agencies. How industry responds to this burden will be instrumental to the administration's success in building a partnership with industry for critical infrastructure protection and is necessary for a successful policy. If industry fails to live up to its word and increase information sharing after the removal of these obstacles, a dramatic shift in policy may be necessary and may need to include more drastic measures, including regulation, to ensure a minimum baseline of security is met. Such a policy, however, would likely be more expensive and less effective.

National Strategies

In addition to the creation of DHS, the Bush Administration has issued a series of national strategies with implications for critical infrastructure protection policy including: the *National Strategy for Homeland Security* in July of 2002, the *National Strategy for the Physical Protection of Critical Infrastructures and Key Assets* in February 2003, and the *National Strategy to Secure Cyberspace* also in February 2003. Of these documents, the Physical Protection Strategy has the most direct impact on non-cyber infrastructure protection efforts and presents three significant evolutions of critical infrastructure protection policy from the pre-September 11 era. First, the expansion of definition of critical infrastructure to include agriculture

and food, water, public health, emergency services, the defense industrial base, telecommunications, energy, transportation, banking and finance, chemicals and hazardous materials, postal and shipping and key assets, which are defined as "individual targets whose attack – in the worst-case scenarios – could result in not only large-scale human casualties and property destruction, but also profound damage to our national prestige, morale, and confidence."[28] Second, an increased emphasis on physical security measures; and finally, a further emphasis on the interdependencies between different infrastructures.

The Physical Protection Strategy reiterates the national policy outlined earlier in EO13231 and PDD-63 but adds "public morale and confidence in our national economic and public institutions" to those things infrastructure protection policy is intended to secure. In order to protect critical infrastructure, the Physical Protection Strategy outlines eight principles:

- Assure public safety, public confidence and services;
- Establish clear lines of authority;
- Promote partnership between government and industry;
- Encourage market-based solutions with limited government intervention when necessary;
- Facilitating information sharing;
- Foster international cooperation;
- Developing new technologies to combat terrorism; and
- Accomplish these tasks while safeguarding privacy and constitutional freedoms.

More importantly the Physical Protection Strategy adopts a three-layer approach to securing critical infrastructure consistent with these principles. First, in recognition that not all infrastructures are equal, the strategy seeks to identify and assure protection of "those assets, systems and functions deemed most critical for national operations." In order to determine which assets are the most critical the strategy calls for the Department of Homeland Security to develop a "uniform methodology" for prioritization to be used by federal, state, local and private sector entities. Second, to secure those assets that may face an immediate threat through better threat analysis and warning. Third, to develop a collaborative environment to promote security in all sectors. The Physical Protection Strategy also divides infrastructure protection priorities between those that would have systematic impacts if disrupted from those whose destruction would cause significant consequences by themselves (referred to in the report as "key assets"), and recognizes that vulnerabilities in infrastructure can be used to conduct direct attacks, promote indirect consequences, or to facilitate an attack. As noted earlier, the long-term intent of the Department of Homeland Security is to more fully integrate intelligence analysis into its critical infrastructure protection mission, a position that is clear in the physical protection strategy.

The Physical Protection Strategy also seeks to delineate the responsibilities of the federal government, state and local agencies and the private sector. For itself, the federal government has reserved the role of strategic planner, facilitator and coordinator and lays out eleven specific responsibilities:[29]

- Taking inventory of the nation's most critical facilities;
- Ensuring cooperation between federal, state, local and private sector stakeholders;
- Providing threat information, assessments and warnings;
- Developing and implementing "multi-tiered" protection policies;
- Exploring incentive programs;
- Developing cross-sector and cross-jurisdictional practices;
- Facilitating sharing of best practices;
- Embarking on demonstration projects;
- Research and development and technology transfers;
- Education and awareness; and
- Improving its ability to work with local responders and service providers.

In meeting these responsibilities, the Department of Homeland Security will play a central role as the central interlocutor for other federal agencies, state and local governments as well as the private sector. The DHS will also be responsible for defining the national strategies for physical and cyber critical infrastructure protection and for cross-sector protection efforts which it breaks into five initiatives: planning

and resource allocation, information sharing and indications and warning, personnel surety, research and development, modeling, simulation, and analysis.[30] Other federal agencies are supposed to provide expert support to the Department in fulfilling its strategy. State and local governments are expected to undertake similar roles as the federal government, but focusing on the needs of their local communities in addition to continuing their role as the primary first responders in the event of an attack. Nonetheless, the Physical Protection Strategy recognizes that the private sector remains its own "first line of defense."[31] It calls on industry to reassess its security needs and investments in light of the terrorist threat. In fact, the strategy dedicates a section to analyzing the security challenges in each sector identified as critical.

However, in order to achieve this vision a number of hurdles still have to be overcome. First, efforts to construct the Department need to be accelerated. Even though the Department was barely over 100 days old at the time this article was written, the appointment and confirmation process of the DHS's senior leadership has gone painfully slowly, including those in the Information Analysis and Infrastructure Protection Directorate. Fortunately, personnel responsible for critical infrastructure protection policy prior to the Department's creation are still completing their missions, but staffing levels are low and are based on pre-September 11 threat assessments and prioritization. While one of the broad goals of the Department is to improve effectiveness by reducing redundancy through consolidation, the significance of the gains achieved by consolidation cannot be recognized until the Directorate is fully assembled.

In addition, relying more heavily on information analysis as an enabler of infrastructure protection efforts requires that intelligence reform measures that have just begun are successful. The information analysis section of the DHS will require direct, real-time access to intelligence reports, other terrorism related information from the enforcement community, raw intelligence and enforcement data, and information on vulnerabilities and protection efforts provided by the private sector. Presently it is too early to determine if new programs designed to ensure that this information is provided to DHS, including the Homeland Security Act's FOIA exemption discussed earlier and the Central Intelligence Agency's new interagency Terrorist Threat Integration Center,[32] will be successful. Nonetheless, success in protecting the nation's critical infrastructure will be as dependent on reforms being conducted in the intelligence arena as on any new programs to analyze and correct vulnerabilities.

Conclusions

Overall, the Bush Administration's approach to securing critical infrastructure is ample for meeting the challenges posed by the division of responsibility for infrastructure protection between the private sector and government and should lay the groundwork for an enduring relationship that will be sufficiently flexible to meet an ever evolving threat. The Freedom of Information Act and anti-trust exemptions in the Homeland Security Act of 2002 should open the door to increased public-private communication. Likewise, the establishment of the Department of Homeland Security and the issuing of the *National Strategy for the Physical Protection of Critical Infrastructures and Key Assets* resolve many of the interagency coordination efforts of the past and clearly establish the DHS as the central figure in the federal government's program. In addition, both the Department's structure and many of the priorities outlined in the Strategy seek to significantly build on previous efforts. The fusion of information analysis with vulnerability assessments and closer cooperation offers the prospect of dramatically increasing the synchronization and comprehensiveness of the infrastructure protection efforts at all levels of government and in the private sector. In addition, the administration's emphasis on cooperative partnerships over regulatory action provides an opportunity to advance the causes of security and economic vitality hand-in-hand.

Nonetheless, both the Department and its plan are only in the earliest stages of implementation. Much will hinge on how quickly the myriads of federal agencies transferred to the Department are consolidated into a focused effort. This will depend in large part on the rapid appointment and confirmation of political leadership for the Information Analysis and Infrastructure Protection Directorate and the relationship it forges with the appropriate oversight committees in Congress. Likewise, since so much of the administration's efforts hinge on information analysis, reforms in how intelligence is shared will be crucial to the

success of the department's efforts. If the new Terrorist Threat Integration Center fails to overcome the stovepiping of the pre-September 11 era, it will likely create a major obstacle for the administration's critical infrastructure protection efforts. Further, it has yet to be seen how industry will react to these initial changes. The main obstacles to increased communication have been removed, but the Department will still have to work hard in order to sell its product and convince industry of its business value, particularly as the attacks of September 11 begin to fade in people's memories. As a result, it is too early to judge the success or failure of the administration's new infrastructure protection efforts. Certainly more can, and should, be done -- particularly in the area of providing incentives -- but devising a bold plan and constructing the Department's infrastructure protection programs around it is a good first step.

An Assessment of Federal Programs

Joseph A. Barbera, MD

Introduction

Reuters

In this new era of potential mass casualty consequences from ever more threatening terrorism methods, the response issues facing the public health and the medical communities are daunting. The tasks involved in managing and responding to traditional mass casualty incidents are already enormous. But now, increasing prospects of mass chemical, biological, nuclear, radiological, and explosive (CBRNE) attacks add issues that include very unusual casualty needs, responder protection concerns, and unpredictable incident parameters. This paper therefore addresses Health and Medical Consequence Management preparedness as it relates to federal Homeland Security. This is perhaps the most difficult preparedness area, and yet also the most vital: since the new goal of modern terrorism is no longer purely to create terror, but to effect *mass assassination*, it becomes imperative to develop a public health and medical capability that will absolutely minimize the human casualty consequences of an accomplished terrorist act. Additionally, mass casualty[1] incident management is critical because the United States is not yet adequately prepared for the catastrophic medical impact of more common hazards, such as the massive earthquake in densely populated areas of California, the Pacific Northwest, New Madrid (Missouri), Charleston (South Carolina), and Alaska.

Federal Public Health and Medical Preparedness Goals

As stated by Governor Tom Ridge in an address to the Associated Press in April 2002:

> The very first 'mission' in the President's Executive Order creating the Office of Homeland Security reads: 'to develop and coordinate the implementation of a comprehensive national strategy to secure the United States from terrorist threats or attacks'.[2]

To accomplish this, the President defined four major "budget initiatives -- first responders, biodefense, border security and information-sharing. The four were chosen because of risk management." The Governor explained the importance of bioterrorism:

> Bioterror has one of the highest rates of consequence, and our preparedness has historically lagged behind the threat.[2]

So how is this bioterrorism preparedness to be accomplished? Goals were further elucidated by Secretary of Health and Human Services Tommy Thompson:

> …That federal, state and local government have come together on a unified plan to strengthen our public health system and prepare to respond to a terrorism attack… plans will usher in a new era of cooperation between all levels of government when it comes to protecting the public's

> health… Secretary Thompson asked governors and three mayors, in conjunction with their health departments, to develop comprehensive plans… to strengthen preparedness.[3]

Five months earlier, the Secretary had recognized that planning and preparedness for mass bioterrorism had not, prior to this renewed effort, reached an acceptable capability. At that time, he stated:

> HHS has been taking steps since 1999 to prepare for these challenges -- and the anthrax attacks of 2001 constituted a sudden test of these initial steps… the attacks also demonstrated significant gaps… the need to move much more quickly in building the public health network…[4]

At that time, he announced the $1.1 billion initiative to upgrade state and local public health capacities and capabilities for bioterrorism preparedness. Funding was structured such that recipient jurisdictions had to submit plans for how they would use the monies to improve bioterrorism detection and response capabilities before the funding was released. The Secretary's 16 goals presented during this January 2002 press conference were further expanded, refined, and re-released five months later as the "17 critical benchmarks" used to review the state and city plans presented to obtain the follow-on components of the $1.1 billion package (see Table 1).

As noted by Benchmarks 15-17, HHS also recognized the need to address acute care medicine's surge capacity and integration into the emergency response community for bioterrorism preparedness in metropolitan areas. This funding component was targeted towards improving hospital care capacity and for regional hospital plans.[5]

The acute medical care capacity goal was manifested further by the expansion of the HHS Metropolitan Medical Response System program:

> This additional funding, through the MMRS [Metropolitan Medical Response System] will help even more cities prepare for large-scale public health emergencies and ensure that more Americans will receive health services if a catastrophic event occurs.[6]

The MMRS program promotes increased medical capacity by encouraging coordination and integration of all emergency response disciplines, including hospitals, clinics, and other acute medical care resources, into a metropolitan response *system*.

Thirdly, the U.S. government, under the specific direction of President Bush, is developing a Medical Reserve Corps (MRC) of retired healthcare workers to assist with surge capacity in a mass casualty incident:

> One purpose of the USA Freedom Corps will be homeland security. America needs retired doctors and nurses who can be mobilized in major emergencies…[7]

The MRC program is described in the Citizen Corps web site as:

> The Medical Reserve Corps (MRC) Program coordinates the skills of practicing and retired physicians, nurses and other health professionals as well as other citizens interested in health issues, who are eager to volunteer to address their community's ongoing public health needs and to help their community during large-scale emergency situations.
>
> Local community leaders will develop their own Medical Reserve Corps Units and identify the duties of the MRC volunteers according to specific community needs…[8]

Other efforts are also ongoing, including those of the Veterans Administration, the National Institutes of Health, and the National Guard Civil Support Teams, but this essay will focus upon the three primary health and medical preparedness initiatives highlighted by President Bush and the Secretaries of Homeland Security and Health and Human Services for bioterrorism response preparedness.

Table 1: 17 Critical Benchmarks For Bioterrorism Preparedness Planning*

The individual state and city plans were reviewed based on criteria including 17 critical benchmarks. The critical benchmarks are:

I. PUBLIC HEALTH PREPAREDNESS (CDC)

1. Designate a Senior Public Health Official within the State health department, to serve as Executive Director of the State Bioterrorism Preparedness and Response Program.
2. Establish an advisory committee with members from a variety of health agencies and first responders.
3. Prepare a timeline for the development of a statewide plan for preparedness and response for a bioterrorist event, infectious disease outbreak, or other public health emergency.
4. Prepare a timeline for the assessment of statutes, regulations, and ordinances within the state and local public health jurisdictions regarding emergency public health measures.
5. Prepare a timeline for the development of a statewide plan for responding to incidents of bioterrorism.
6. Prepare a timeline for the development of regional plans to respond to bioterrorism.
7. Develop an interim plan to receive and manage items from the National Pharmaceutical Stockpile, including mass distribution of antibiotics, vaccines and medical material.
8. Prepare a time line for developing a system to receive and evaluate urgent disease reports from all parts of the state (or city) and local public health jurisdictions on a 24- hour per day, 7 days per week basis.
9. Assess current epidemiologic capacity and prepare a timeline for providing at least one epidemiologist for each metropolitan area with a population greater than 500,000.
10. Develop a plan to improve working relationships and communication between Level A (clinical) laboratories and Level B/C laboratories, (i.e. Laboratory Response Network laboratories) as well as other public health officials.
11. Prepare a timeline for a plan that ensures that 90 percent of the population is covered by the Health Alert Network (HAN).
12. Prepare a timeline for the development of a communications system that provides a 24/7 flow of critical health information among hospital emergency departments, state and local health officials, and law enforcement officials.
13. Develop an interim plan for risk communication and information dissemination to educate the public regarding exposure risks and effective public response.
14. Prepare a timeline to assess training needs--with special emphasis on emergency department personnel, infectious disease specialists, public health staff, and other health care providers.

II. HOSPITAL PREPAREDNESS (HRSA)

15. Designate a Coordinator for Bioterrorism Hospital Preparedness Planning.
16. Establish a Hospital Preparedness Planning Committee to provide guidance, direction and oversight to the State health department in planning for bioterrorism response.
17. Devise a plan for a potential epidemic in each state or region. Recognizing that many of these patients may come from rural areas served by centers in metropolitan areas, planning must include the surrounding counties likely to impact the resources of these cities.

* HHS Press Release 6 June 2002, available at http://www.hhs.gov/news/press/2002pres/20020606a.html

Assessment of Progress on Stated Bioterrorism Preparedness Goals

Preparedness Assessment Metrics

Developing metrics to determine, with accuracy and validity, the *actual* preparedness level of federal, state and local efforts is complex and difficult. Indeed, an esteemed group of medical and related professionals had great difficulty addressing this task in an Institute of Medicine guided effort to provide advice for evaluating the MMRS.[9] It was recognized that evaluation of a program designed for very infrequent mass casualty incidents can only be inferential, since little opportunity (fortunately) exists for direct assessment of adequacy.

The issue is specifically the *validity of metrics* used to define the readiness and the capacity of health and medical capabilities for a mass bioterrorism incident. Validity is called into question because the evaluative focus is a *capacity to respond during an unexpected mass bioterrorism incident*, which is very different from everyday medical and public health experience. Indeed, it has become quite clear that "emergency public health" is distinct in concept and practice from "normal public health," similar to the recognition in the 1980s-1990s by the business community that "business crisis management" is distinctly different from "business management." The corollary to this is that using normal public health parameters to assess emergency public health capability are immediately suspect, and there are few obvious, commonly occurring proxy situations for emergency response to major bioterrorism attacks. To further emphasize this concern, it has become readily apparent that the public health preparedness preceding the anthrax dissemination incident of 2001 was woefully inadequate to manage the incident in the National Capital Area, and yet this was *not reflected* in any informal metrics used by the CDC, National Capital Area state and local public health authorities, the GAO and others who were assessing public health preparedness for biological terrorism prior to October 2001.

The United States has not experienced any further biological incidents or attacks to date. Without experiential success to demonstrate effective systems under actual circumstances, it is difficult to confidently define valid inferential preparedness indicators. What can be proffered, however, is that informal metrics used by program managers in the past, some which continue to be used today, have no reliable predictability. These include:

- **Dollars spent on preparedness as an indicator.** The CDC in particular seems to often measure its accomplishments by the amount of funding provided, without mentioning the development, validation, and use of any evaluative proxies for preparedness capacities. For instance, their Program in Brief series describes each of their initiatives related to bioterrorism, but their response to "What has CDC accomplished?" reflects an inordinate reliance on the dispensation of "funding" as a sign of accomplishment.[10]

- **Implementation and completion of training programs as a metric.** Since most training programs have undergone no rigorous or formal validity evaluation, it is not surprising that the implementation of "training programs" and the completion of "training" by personnel don't necessarily correlate with actual system performance during an incident.

- **Conferences, committee efforts, and the completion of Bioterrorism Response Plans.** Experience in many other areas of emergency management have demonstrated that these also do not serve as valid proxies for response preparedness.[11,12]

Assessment of public health preparedness

Much change of direction has occurred in federal public health planning and preparedness since the events of 2001. Most are relatively new initiatives, and recognizing that it takes time to acquire funding and direction for programs focused on improving state and local public health practice, it is difficult to assess recent progress.

It is particularly difficult to comfortably assess any preparedness parameters by the CDC, and as an extension state and local public health, based upon written guidance and plans. Careful review of the

CDC website (www.bt.cdc.gov) demonstrates many very insightful documents on specific hazard agents (biological, chemical, and others). These documents, however, generally have specific technical and narrowly focused guidance (for instance, a flow-chart recommending notification sequences, or worker safety guidelines for anthrax). It is difficult to find significant guidance for developing and implementing a public health and medical response *management system* for bioterrorism, since a comprehensive system description delineates *processes* for accomplishing objectives, and provides a detailed concept of operations. For example, in reviewing the CDC document "Bioterrorism and Public Health Preparedness,"[13] little was found that recommends the application of operational processes for emergency response to bioterrorism.

Surveillance guidance is similarly superficial and operationally vague. This is of particular concern since there seem to be significant deficits in most current major surveillance programs, including lack of flexibility, poorly defined analysis processes, and limited data collection/information dissemination methods. Without clear CDC leadership in developing more defined surveillance system requirements, it is doubtful that the U.S. will soon have adequate systems in place across the U.S.

With the markedly increased federal spending on public health, many federal, state, and local public health initiatives are underway. Overall direction at state and local levels, however, is often not clear. What is *least clear* are well-defined systems, processes, and procedures to rapidly mobilize, efficiently gather and analyze data to develop and maintain accurate epidemiological profiles, and coordinate widely disparate health and medical entities at the time of a mass bioterrorism incident.

Even the 6 June 2002 "Public Health Preparedness 17 Critical Benchmarks..." guidance seems not to emphasize the importance of incident management systems as the overarching need to effectively manage a bioterrorism attack. In fact, each benchmark is presented as an individual item, and they are not intuitively tied together to promote the development of a single management "system" to accomplish all 17 tasks.

In an attempt to move beyond written documentation alone to assess federal public health preparedness programs, the author evaluated proxy situations as metrics for assessing emergency public health and medical response capability. An attractive proxy is the current attempts to implement a smallpox vaccination program across the U.S. under very urgent circumstances. A successful program of this nature requires effective incident management, information processing (including communications), and operational coordination across jurisdictions, which may be arguably similar to bioterrorism incident response requirements. The ability of federal, state and local health and medical systems to institute urgent health evaluations, make decisions, and effectively and rapidly implement actions to accomplish the decisions may be a valid reflection of emergency public health response capability.

If the smallpox program is an acceptable metric, it reflects a significant gap between current capability and the goals of HHS bioterrorism preparedness programs:

- The decision process to develop the smallpox program was prolonged, with unnecessary *public* disagreements by experts and political officials, including the appearance of excessive influence of political factors on scientific/public health decisions. The CDC has had difficulty demonstrating definitive program leadership, and the many publicly circulated "drafts" of the smallpox plan suggests the lack of an effective planning process.

- Clearly defined problem issues such as personal and healthcare facility liability, workers compensation, and paid furlough for vaccinated healthcare workers, were *not* rapidly addressed with resolution communicated effectively to the affected community, causing consternation and a reluctance to participate in the smallpox vaccination program.[14,15,16] It must be recognized, however, that this was not primarily a problem caused by federal health agencies or assets. Liability protection, workers compensation coverage, and other issues require actions by other Executive branch agencies, and by Congress. A federal government mechanism to recognize and rapidly effect these cross-departmental and Congressional actions will also be necessary for future unusual disease

control (including bioterrorism), just as it would have expedited the current smallpox vaccination effort. What has also become clear from this experience is that attempts to verbally minimize issues of concern to the state and local medical professionals (such as liability and workers compensation coverage) will not resolve valid concerns.

- A changing public message about the smallpox vaccination program, including conflicting versions without readily apparent explanation, heightened public and healthcare community concerns, and indeed appear to have significantly increased the difficulty in obtaining vaccination consent by workers and by hospital authorities.[17] Again, many of these conflicting messages occurred through lack of coordination by non-health federal agencies that extended beyond DHHS and CDC. A federal mechanism to avoid this in the future is essential to avoid public confusion and loss of confidence in authorities in a major and fast-moving public health emergency.

- Many state and local public health officials, as they struggle to implement the federal smallpox vaccination program, describe the effort as an extraordinary burden, in many cases severely curtailing work on regular public health activities and on other aspects of emergency public health preparedness.[18,19] Upon examination, it is suggested that some of this burden may have been minimized by providing effective templates for organizing and establishing vaccination centers, for standardized and widely available staff training programs (validated after development and before release to program operators), and information instruments for vaccinators, for orienting the public, and for addressing issues and concerns of the targeted vaccine population.

The smallpox vaccine program "development and implementation as a metric" gains the appearance of validity upon careful examination, because the demonstrated problems are distressingly similar to those that were presented during the anthrax dissemination incident in 2001: poor data acquisition, ineffective management decisions by health authorities and others, conflicting messages causing crises in confidence among both the target population and responders, and greater than necessary efforts (due to program inefficiencies) in order to accomplish identified tasks.

Assessment of hospital preparedness

With the 2002 funding for hospitals through the HRSA Hospital Bioterrorism Preparedness Program, the federal government has for the first time financially acknowledged the critical infrastructure nature of hospital preparedness for mass casualties. HRSA money from this program has only very recently begun to reach hospitals in most states, so little progress to date can be assessed for this program. This is of concern, given the months of heightened interest by hospitals in improving response capacity and capability.

Hesitancy in providing clear guidance to hospital planning (occurring at the state and local levels), and the inefficient distribution of the allocated funding (again, a state and local issue more than federal), risks re-alienating the hospital and private medical communities. If the efficacy and effectiveness of the process of state public health pass-through of HRSA funds to hospitals is a metric for integration between the two communities, it should cause serious concern.

Future HRSA funds must be rapidly provided to their target hospitals. This future program funding, if continued through state public health officers, should stipulate that the coordination of public health and acute care medicine within its jurisdiction is a primary program goal, and efficient, effective, and accountable distribution of funds from public health to hospitals will be a metric used to evaluate their public health/hospital integration. Guidance should also be more specific as to what the funds are supporting, and provide a clear method to determine accountability for the funded capability. The federal efforts should always encourage the development of local funding streams to provide ongoing healthcare preparedness for mass casualties, since this is not just a federal government concern, but an issue for government at all levels.

Assessment of community/regional preparedness - the MMRS program

Review of MMRS plans suggest that this program has prompted closer planning between public health, acute care medicine, and the more traditional public safety disciplines in MMRS locations. In fact, this may be the best-targeted and most effective federal preparedness program for promoting systems to address the new era of CBRNE mass casualty threats. It emphasizes an all-hazard approach to planning, which promotes multi-use, sustainable capacities. Several problems, however, are apparent:

- Locals in at least some metropolitan areas continue to view the MMRS as a purely federally funded program, and complain that lack of continued federal support will result in their MMRS not being sustained.[20] The program would serve better if it emphasized that the federal funds are targeted for *improving the coordination* between local entities rather than primarily purchasing and maintaining equipment and supplies. It should emphasize *process*, which should be developed so that it is sustainable at the local and regional levels without further federal funding. Federal funding must also be carefully presented to avoid the current misconception that programs can be developed and then maintained only through federal dollars.[21]

- The MMRS contracts are somewhat disjointed, lacking clear guidance for comprehensive management systems and precise, easily monitored system capabilities. The defined program requirements are listed in a manner that is similar to those of Secretary Thompson's "17 Critical Benchmarks For Bioterrorism Preparedness." The requirements are listed individually, without promoting a single system of coordination and management, which may be the most essential component for managing a large-scale bioterrorism incident.

- The program requirements could be much more specific in the degree of capacity and timeliness for the indicated process (such as notification). They also could have been delineated in a manner that made evaluation of MMRS contract performance more objective and meaningful, and the recipient jurisdictions more accountable for developing and maintaining truly effective capability.

Assessment of the Medical Reserve Corps

This program is maintained under the Office of the Surgeon General (OSG), and the Office has to date provided little specifics on state and local program development. The published guide (available at http://www.medicalreservecorps.gov/guide.htm), for instance, provides only broad guidance. Instead, OSG has undertaken a strategy to provide $50,000 grants to a number of communities for demonstration projects. It is too early to determine the effectiveness of this program, but concern arises with any program for developing and coordinating medical volunteers, who generally need detailed system structure and administrative oversight to be effectively used in emergencies. It is unclear that this type of detailed mentoring or guidance will be forthcoming.

Future metrics for assessing preparedness

As noted above, urgently developed and implemented preparedness programs and contingency preparedness activities (similar to the current smallpox vaccination program) may be employed as preparedness metrics. Response to hoaxes and pranks may also provide proxy measurements, particularly for the aspects related to the effectiveness and timeliness of notification, mobilization and coordination. Objective evaluation of full-scale field bioterrorism exercises is another attractive source for investigating preparedness accomplishment. For example, TOPOFF 2000 appears to have been considered a reasonable metric indicating to some experts a lack of bioterrorism response preparedness.[22] This view was evidently also held by federal authorities, who have *never* released the formal after-action evaluation to the public or the general response community. Future similarly realistic full-scale bioterrorism exercises, including the impending TOPOFF 2003, should have exercise evaluation carefully developed during the planning stage to accurately and objectively assess for bioterrorism response capability.

Since "integration" of the many diverse medical and health assets is considered essential to bioterrorism response, and it is well recognized that this doesn't "just happen" and that good intentions alone are

insufficient, program evaluators must be especially interested in developing proxy indicators for this competency. Validation criteria may be developed by searching for systems that legitimately promote effective integration of local, state and federal assets: it is the author's opinion that few are currently identifiable in the public health/medical realm.

Assessment of the Appropriateness of the Federal Goals: Recommendations

A discussion of the appropriateness of the federal goals in bioterrorism public health and medical preparedness must be framed by the realities of mass bioterrorism incidents and credible response requirements.

Promoting state and local preparedness

In a sudden onset or rapidly progressing mass casualty incident, the bulk of medical resources required to make a difference in the affected population's health outcome must be rapidly, almost immediately available for use. This limits the strategy of centrally stockpiling equipment/supplies in a few locations in the U.S. and developing fixed site specialty medical capabilities for many types of patient needs.


Reuters

Careful analysis and understanding of the issues makes it clear that while there must be an urgency to prepare for terrorism at the national level, including a national response plan, successful response and incident management requires effective *local capability and capacity* in the affected jurisdictions. Federal goals incorporate an understanding of this concept. The federal difficulty in attempting to influence improvements in local preparedness, however, is similar to the experience found in education: with the *total* federal funds so small for each local entity, and the cost of developing *and maintaining* normally unused capacity and capability so expensive, little federal influence occurs through current funding alone. It may be that more careful attention to the federal development of effective templates, to be considered by state and local entities when accepting federal dollars, will more effectively advance local and state preparedness. Templates are *not* detailed prescriptions of exactly how a jurisdiction must implement a capability, or exactly what comprises that capability in an individual jurisdiction. Rather, templates are explanations of systems, and compilations of *requirements* for a defined system and its critical components. How the jurisdiction meets those requirements depends upon the unique historical, political, and interpersonal characteristics of each jurisdiction. Interfaces between jurisdictions, and up and down the federal-state-local levels, must have clearly defined templates to ensure effective integration and coordination. Templates must also guide jurisdictional authorities and responders toward the skills and capabilities that must be both *available* and *operational* during a mass casualty incident, including biological terrorism consequence management. Properly constructed templates meet the concept described by Governor Ridge when he spoke of state and local needs: "They want direction from us, not micromanagement."[23]

Programs under DHHS are evolving in this important direction.

Establishing operational coordination between public health and acute care medicine

Public health and acute care medicine encompass very diverse resources, which are widely separated in management methods, goals, funding, and operations. It is essential that this reality be fully recognized and better addressed in preparedness, since in a rapidly moving, high-stakes health emergency, the vast majority of health and medical assets lie within the purview of acute care medicine, *not* public health, at the local, state or federal levels. An example of the pre-9-11 state of coordination between hospitals and local public health is illustrated by a study done in West Virginia:

> While nearly two-thirds [of county health directors - CHDs] rated their communication with hospitals as moderate to strong, a similar proportion stated they had no protocol for communicating with hospitals about a WMD event. Eighty-six percent of CHDs reported that no new collaborative efforts were directed towards the early identification of new or emerging infectious diseases possibly related to bioterrorism.[24]

Unlike fire, law enforcement, emergency medical services, and even public works, public health and acute care medicine is not a discipline organized into a single jurisdictional *response* system, and is not operationally connected at the local/regional levels through regularly tested mutual aid, planning, or other similar activities. Federal attempts to address this deficiency are therefore very appropriate. They may be more effective if they emphasize the importance of having in place effective management systems, rather than the current emphasis on individual, narrow training programs and initiatives. Validated, effective public-private partnership templates are essential to accomplishing this objective.

Promoting capability for emergency response in public health – state and local

Public health, at the local and state level, has chronically been under-funded in terms of meeting its traditional public health commitments, and therefore attention to planning, preparedness, asset acquisition, training, and exercise for emergency response have not received a balanced effort. Over the middle decades of the last century, major public health hazards such as polio, tuberculosis, lead paint, and other hazards were eliminated from causing epidemics requiring large-scale mobilization and response. As a consequence of this public health success, public health as a capability has gradually evolved into a primarily *preventive* mode. Understanding of, and capability for, major mobilization and emergency response faded. Public health has been under-appreciated by other public safety responders as filling any significant role, even in mass casualty emergency response to terrorism. For example, little to no public health presence existed at the 1993 World Trade Center Bombing, the 1995 Oklahoma City Bombing, the Pentagon 9-11 response, and only late/awkward involvement occurred with NYC DoH in WTC Ground Zero. As a result of this lack of focus on emergency response, public health has generally not participated, until very recently, in the evolution of the ICS-based coordination of emergency response that has occurred nationally for fire/police/EMS/emergency management in many jurisdictions. Unlike other public safety functions, public health and acute care medicine do not have widely implemented mutual aid systems, they have little operational coordination with emergency management, and they are not oriented to incident management methods. These weaknesses were painfully apparent during the anthrax dissemination event of 2001 in the National Capital Area.[25] As public health incident response capability is reconstituted, it must adjust to the new realities of modern response management, technology, and additional "players." This is a very appropriate, important federal program goal.

The MMRS program is an excellent start in this direction, and has promoted the *beginnings* of integration between acute medical care, public health, and public safety agencies in metropolitan areas. Many MMRS cities are attending to the issue, earnestly working to develop integration concepts, but without a *well-defined* template are developing many misunderstandings and misconceptions. MMRS templates must be more tightly and comprehensively defined, and be particularly focused on "all-hazard/all-disciplines" management and information processing. To accomplish this, a more widely applicable incident management system and processes must be defined, ideally using an efficient working group process that includes many disciplines and a geographic balance such as that used in the development of the FEMA US&R System. The system must effectively integrate public health and private medicine into management processes with emergency management and the other emergency response disciplines. Again, Governor Ridge manifests an understanding of these concepts:

> 'Comprehensive.' We must wrap our arms around every aspect of homeland security. Our strategy must not just raise questions, but provide solutions.[27]

The Institute of Medicine report on the MMRS concludes with an excellent assessment of the MMRS (page 170):

> The importance of the MMRS program effort is no longer equivocal, questionable, or debatable.

> The philosophy that it has developed has become an essential and rational approach … The enhanced organization and cooperation demanded by a well-functioning MMRS program will permit a unified preparedness and public health system with immense potential for improved responses not only to a wide spectrum of terrorist acts but also to mass casualty incidents of all varieties.

Promoting capability for emergency response in public health – federal

Federal public health and medical capability has also not, in the past, been organized for a *single* system emergency response to assist state and local authorities. The public health component has traditionally been organized through the CDC, with response generally routed through networks forged by the CDC and state public health offices in non-disaster situations. These coordination routes have not blended easily into a wider, federal-state coordination mechanism during major emergencies. Federal authorities must organize to have the federal public health and medical assets train and respond in a coordinated fashion, and be capable of interfacing as a single organized entity with state and local assets, using the same mechanisms during preparedness that will be used during an alert and a response. It is particularly important that the CDC better organize to manage its assets during emergency response and integrate into the overall federal health response. A focus by the CDC on having an effective emergency response center indicates positive movement on this critical issue.[28]

Other federal medical assets generally have been organized and deployed through the Office of Emergency Response (OER), formerly Office of Emergency Preparedness, of the U.S. Public Health Service. These are managed through the National Disaster Medical System and its component response capabilities: Disaster Medical Assistance Teams (DMATs), Commissioned Corps Reserve Force (CCRF), Disaster Mortician Teams (DMORTs), National Medical Response Teams (NMRTs), etc. The majority of these medical assets (except for the CCRF) are drawn from the non-governmental medical realm at the time of need and are processed into temporary federal employees for the response. They were coordinated during response through a Management Support Team under the USPHS Office of Emergency Response (which in the past did not coordinate closely with CDC deployed teams). DMATs and other OER teams become directly managed through the local incident management system once they are assigned in the incident. This process has worked well, but team organizational, training and equipment efforts have traditionally been very under funded. OER has transitioned to the new Department of Homeland Security. NDMS and the DMAT programs have transferred with them. The CCRF and MRC have remained under the Office of the Surgeon General (DHHS) but will be deployed through OER. It is unclear how well this split of medical assets between the two federal agencies will be supported and coordinated during maintenance and response. Federal goals that are evolving under DHHS (particularly through the recently created Office of the Assistant Secretary for Public Health Emergency Preparedness) and the new Department of Homeland Security indicate that federal deployment of health and medical assets will be more tightly coordinated in the future, and this is a very appropriate goal.

The federal interface with local resources must be clearly defined as "in support," following the effective practices of other federal emergency response assets over the past many decades. Any confusion in this role (as occurred with the CDC and Washington DC public health authorities during the 2001 anthrax incident) must be carefully avoided.

Improving preparedness in healthcare facilities and other acute care medical assets

Most local acute care medical assets are private, and even governmental medical resources are not operationally associated with public safety. Severe economic pressures of the past several decades have reshaped medical care resources into modern businesses, with efficiencies such as bare minimal staffing, just-in-time resources, and restructuring to eliminate costly and poorly performing (from an economic standpoint - not a clinical one) specialty capabilities.

All of this has led to extremely restricted surge capacity (the volume of patients that can be evaluated and appropriately managed) and capability (the provision of medical and health specialty care that are not regularly available at the location where they are established - burn care, pediatric care, decontami-

nation, and others). Little or no funding can be directed from operational income into emergency preparedness, and with increased administrative burdens due to the decrease in staffing, hospital administrators and clinical staff have more restrictions upon their time.

The old ideas of emergency preparedness, preparing for traditional types of multiple casualties such as blunt trauma victims in a bus accident, do not apply well to the new concerns of truly *mass* casualties, with unusual hazard types and patient problems. New systems and capabilities are needed, but few in the acute healthcare community have a background that provides an operational understanding of the needs, let alone efficient, effective development processes to adequately address those needs. Funding issues *during* response must also be addressed, again highlighting the needs for an effective, over-arching *single management system* for all health and medical assets in a jurisdictional incident response. The author has co-developed such a conceptual incident management system,[29] incorporating the successful management and information processing concepts of the Incident Command System. The project was supported by the Alfred P. Sloan Foundation (upon the recommendation of a senior official in the Office of Homeland Security), and both the new Department of Homeland Security (DHS) and DHHS are considering the product for application. While DHS and HHS are promoting the implementation of this type of system in local and regional jurisdictions across the U.S., it is unclear how the federal agencies intend to accomplish this goal.

Future HRSA program funding, if continued through state public health officers, should stipulate that the coordination of public health and acute care medicine within its jurisdiction is a primary program goal, and efficient, effective, and accountable distribution of funds from public health to hospitals will be a metric used to evaluate their public health/hospital integration. Guidance should also be more specific in what the funds are supporting, and provide a clear method to determine accountability for the funded capability. The federal efforts should also encourage the development of the concept of local funding streams to provide ongoing hospital and healthcare preparedness for mass casualties. This is not just a federal government concern, but an issue for government at all levels.

Conclusions

It is important to note that many of the currently concerning CBRNE threats have never been widely experienced during the modern medical era. Exact medical and health needs during a response are therefore poorly understood and, as occurred during the anthrax dissemination incident of 2001, will need to be determined *during* the specific event. This highlights the importance of having data collection and analysis capacity, paired with excellent clinicians and epidemiologists, all of which can be rapidly organized as an event is recognized.

With this backdrop, the federal government has embarked upon an ambitious undertaking of developing "adequate" capabilities for public health and medical consequence management. From the themes that run through HHS press statements since 9-11-01, it is clear that the federal government is focusing in appropriate directions and addressing many of these identified deficits. Changing prior courses, developing fresh ideas and concepts to address the new realities and overcome preparedness obstacles, implementing programs that cross many culturally and operationally diverse disciplines, are daunting tasks, akin to trying to rapidly maneuver a battleship. One must accept that visible change in consequence management health and medical capability will appear slower than desired, but must continue as a steady, relentless, and permanent process.

It is most important for federal health authorities, and the new Department of Homeland Security, to continue to promote vigorously the development of new, overarching *systems* that can coordinate both preparedness and response across many disciplines and wide geographic areas. Indeed, GAO has identified this as important *across all* federal government programs, but they specifically emphasized how important it is for homeland security:

> In most federal mission areas -- such as homeland security…national goals are increasingly achieved through the participation of many organizations. State and local governments,

> nonprofit institutions and governing bodies, all play a vital role in formulating and implementing federal initiatives. Promoting effective partnerships with third parties in the formulation and design of complex national initiatives will prove increa singly vital to achieving key outcomes, such as protecting the nation from the threat of terrorism.[30]

These concepts appear to be well understood by top federal authorities. This includes Governor Ridge, as reflected in his 29 April 2002 statement:

> 'National strategy.' That's national, not federal. That means the states and localities, the private sector and academia, and the American people will [help] make it happen.

To effect this intention, clearer templates for implementing cross-disciplinary and multi-level government coordination must be established and disseminated. While other more focused improvements are also necessary, having a truly effective, over-arching *single management system* for all health and medical assets in a jurisdictional incident response should be identified as a *threshold capability* necessary for successful incident management and for maximizing the benefits of the many other improvements currently underway. Mr. Jerry Hauer, Acting Assistant Secretary of Health for Public Health Emergency Preparedness, expressed this philosophy well:

> "So much of the federal money over the last three years that has come out of the terrorism programs has gone for toys...[not] for building systems," he told the HHS Council in August [2002].[31]

Many indicators suggest that the responsible federal government departments are moving in the correct directions:

- Key personnel positions have recently been filled with experienced, respected emergency management and response experts, particularly at the DHHS Assistant Secretary for Public Health Emergency Preparedness[32] and the DHS Director of the Office of Emergency Response.

- Many planning meetings, particularly in public health, have been accomplished recently, with evidence of a renewed earnestness in addressing preparedness deficiencies.

Mass casualty terrorism will be an enduring threat. Preparedness to meet that threat must become and remain real, and be assimilated into the all hazard funding for disaster preparedness at all levels of government: "federal funding" for state and local programs should transition to *federal, state, and local* sharing of expenses for mass terrorism health and medical consequence management, reflecting the new reality that this is a permanently expanded public safety requirement to "protect American families."[33]

Funding for public health and medical preparedness, training, equipment purchases and other activities must be refocused so that it is dispensed only for resources that fit within the defined *systems*. The current "training" glut, for instance, has been relatively useless, since federal funding sources do not require the contractors to first define the "systems" upon which they are basing their training, and since contractors are not required to include training on *systems development*, even though the trainees do not have the systems and don't intuitively know how to construct and maintain the systems upon which they are "trained."

One cannot fault the earnestness of the health and medical preparedness effort, or the intensity of both the federal and overall national effort itself. But much in the past has been misguided and redundant, and has allowed very large preparedness gaps to remain uncovered. We need truly interdisciplinary, all-hazard, one-system planning and preparedness. This will only occur through effective federal guidance, with accompanying, carefully presented templates and funding initially proffered by the federal government.

Appendix 1: An Assessment of Federal Critical Infrastructure Protection Efforts Since September 11

1. Namely allowing passengers to carry small blades, directions not to oppose hijackers and a failure to compare airline passenger manifests to lists of known and suspected terrorists.
2. National Infrastructure Protection Center, *Terrorist Interest in Water Supply and SCADA Systems,* Information Bulletin 02-001, January 30, 2002.
3. According to officials at Delta Airlines, the nine major U.S. airlines lost $7.4 billion dollars in 2001 alone as the result of the September 11, 2001 attacks. <http://www.delta.com/docs/ir_speeches_2002/oct0802_aviation_and_economy.html> Similar figures have been offered by the Air Transport Association in their most recent briefing on the *State of the U.S. Airline Industry.* Available at <http://www.airlines.org/public/industry/bin/IndustryUpdate.pdf>.
4. National Infrastructure Protection Center. *Risk Management: An Essential Guide to Protecting Critical Assets.* November 2002.
5. *Ibid.,* p. 9. Ironically and unwisely, NIPC only used one example of terrorism (terrorist attacks on key personnel) and rated the risk as low. Although NIPC's example was only hypothetical, it's labeling the risk associated with terrorism as low while trying to get industry to invest more in protective measures was counterproductive.
6. *Ibid.,* p.4. Italics included in original.
7. Crews, Clyde Wayne Jr. *Ten Thousand Commandments: An Annual Snapshot of the Federal Regulatory State.* 2002 Edition. (Washington, DC: The Cato Institute, 2002) p. 2. <http://www.cato.org/tech/pubs/10kc_2002.pdf>.
8. United States Office of Management and Budget, <http://www.whitehouse.gov/omb/egov/gtob/compliance.htm>. (Accessed April 2003).
9. United States General Accounting Office, *Critical Infrastructure Protection: Federal Efforts Require a More Coordinated and Comprehensive Approach for Protecting Information Systems,* GAO-02-474, July 2002, p. 25.
10. The President's Commission on Critical Infrastructure Protection, *Critical Foundations: Protecting America's Infrastructures,* October 1997.
11. *Ibid*, p. 55. Defined to include: Information and Communications, Electric Energy, Gas/Oil Production and Storage, Banking and Finance, Transportation, Water Supply, Emergency Services and Government Services.
12. Specifically: information and communications; banking and finance; water supply, transportation (including aviation, highways, mass transit, pipelines, rail and maritime); law enforcement; fire services; public health; electrical power; and oil and gas.
13. United States General Accounting Office, *Critical Infrastructure Protection: Significant Challenges Need to Be Addressed,* GAO-02-961T, July 24, 2002, p. 9.
14. *Ibid,* p. 20.
15. *Ibid,* p. 26.
16. See for example; Symantec, *Internet Security Threat Report,* Volume 3, February 2003.
17. Specifically the Secretaries of State, Treasury, Defense, Commerce, Health and Human Services, Transportation, Energy, the Attorney General, the Director of Central Intelligence, the Chairman of the Joint Chiefs of Staff, the Director of the Federal Emergency Management Agency, the Administrator of General Services, the Director of the Office of Management and Budget, the Director of the Office of Science and Technology Policy, the Chief of Staff to the Vice President, the Director of the National Economic Council, the Assistant to the President of National Security Affairs, the Assistant to the President for Homeland Security, the Chief of Staff to the President, and other executive branch officials as the President may designate.
18. With the creation of the Department of Homeland Security, the NIAC is now managed by the Department. Department of Homeland Security, "Department of Homeland Security Facts for March 1, 2003," at <http://www.dhs.gov/dhspublic/display?theme=43&content=489>. (Accessed March 2003).
19. *Ibid.*
20. During its April 22, 2003 teleconference, the members of the NIAC decided to study 5 issues for 2003, including; cross sector interdependency and risk assessment, post-incident restoration of services measures, the division of authority between the NIAC and other federal councils, an assessment of regulatory best practices and areas where regulation may be warranted and where it may not, and how to enhance the roles of the private sector information sharing and analysis centers (ISACs).
21. Discussion of the need for a clear FOIA exemption for information voluntarily shared by industry dates back, at least, to the Report of the President's Commission on Critical Infrastructure Protection in 1997.
22. Freedom of Information Act, as amended. P.L. 93-502 (b)(4).
23. Dick, Ronald L. "Private/Public Information Sharing and Infrastructure Security." Testimony before the Senate Government Affairs Committee. May 8, 2002.
24. Summerill, Joseph. "Is It Safe for Your Client to Provide the Government with Homeland Security Data?" *Federal Lawyer,* January 2003.
25. Federal Document Clearinghouse, "U.S. Representative Stephen Horn (R-CA) Holds a Hearing on Cyberterrorism and Critical Infrastructure," *Verbatim Transcript,* July 24, 2002.
26. Federal Document Clearinghouse, "U.S. Senator Joe Lieberman holds a hearing to examine infrastructure security, focusing on private and public information," *Verbatim Transcript,* May 8, 2002.
27. National Archives and Records Administration, "Department of Homeland Security: 6 CFR Part 29: Procedures for Handling Critical Infrastructure Information; Proposed Rule," *Federal Register,* April 15, 2003, pp. 18524-18529.
28. The White House, *The National Strategy for the Physical Protection of Critical Infrastructure and Key Assets,* February 2003, p. VIII.
29. *Ibid,* p. IX.
30. The Physical Protection Strategy devotes a substantial section to its cross-sector initiatives discussing a number of measures designed to complete each initiative. While many are summarized throughout this paper the precise measure can be found on pages 21 to 35 of the strategy.
31. The White House, *The National Strategy for the Physical Protection of Critical Infrastructure and Key Assets*, February 2003, p. X.
32. As part of his State of the Union Address, President Bush announced the creation of the Terrorist Threat Integration Center. The Center would be an interagency effort to unify information held throughout the federal government on terrorist threats to ensure that the kind of information sharing that inhibited the efforts to prevent the terrorist attacks on September 11, 2001 were not repeated. See, for example: The White House, "Fact Sheet: Strengthening Intelligence to Better Protect America": at <http://www.whitehouse.gov/news/releases/2003/01/20030128-12.html>. (Accessed January 2003).

1. "Casualty" refers to any human accessing health or medical services, including mental health services and fatality care, as a result of a hazard impact.
2. "Tom Ridge Speaks to the Associated Press Annual Luncheon," The Associated Press Annual Luncheon, The Hilton New Orleans Riverside Hotel, New Orleans, LA. 29 April 2002. Available at: http://www.whitehouse.gov/news/releases/2002/04/print/20020429-3.html, accessed 2 February 2003.
3. "HHS approves state bioterrorism plans so building can begin." HHS press release 6 June 2002. Available at: http://www.hhs.gov/news/press/2002pres/20020606c.html, accessed 2 February 2003.
4. "Bioterror Funding Provides Blueprint to Build a Strong New Public Health Infrastructure." HHS press release 25 January 2002. Available at: www.hhs.gov, accessed 2 February 2003.
5. The Health Resources and Services Administration (HRSA) provided this portion of funding, which is being distributed to states to create regional hospital plans to respond in the event of a bioterrorism attack.
6. "HHS provides new aid to cities for disaster preparedness." HHS press release 10 July 2002. Available at: http://www.hhs.gov/news/press/2002pres/20020710.html, accessed 2 February 2003.
7. White House Press Release: "President Delivers State of the Union Address," 9 January 2002. Text of address available at: http://www.whitehouse.gov/news/releases/2002/01/20020129-11.html, accessed 11 February 2003.
8. http://www.citizencorps.gov/programs/medical.shtm, accessed 12 February 2003.
9. Manning, F.J. and L. Goldfrank (ed). Preparing for Terrorism: Tools for Evaluating the Metropolitan Medical Response System Program (202002). Institute of Medicine, National Academy Press, Washington DC. Available at: www.nap.edu; Chapter 5: "Measurement and Data Collection in Evaluation," pp. 75-90.
10. "CDC Programs in Brief," Available at: www.cdc.gov/programs, accessed 12 February 2003.
11. Both the Metropolitan Washington DC Council of Governments and the Washington DC Department of Health released their completed Bioterrorism Response Plans or Planning Guides in September 2001, one month before the anthrax letter dissemination in the National Capital Area. Neither guide was used substantially during the ensuing anthrax biological incident.
12. http://www.citizencorps.gov/programs/medical.shtm, accessed 12 February 2003. "Why an adequate written plan is not sufficient assurance of preparedness," pages 82-85.
13. "Bioterrorism and Public Health Preparedness." Available at: http://www.cdc.gov/programs/bio.htm, accessed 12 February 2003.
14. "Connecticut Smallpox Plan Could Be Revised." Available at: http://www.cnn.com/2003/HEALTH/2002/13/conn.smallpox.ap/index.html, accessed 13 February 2003. ("Hampered by fewer volunteers than expected, Connecticut is revising its plan…")
15. Connolly, C. "Caregivers Protected Against Smallpox Lawsuits." 15 January 2003. Available at: http://www.washingtonpost.com/wp-dyn/articles/A56861-2003Jan14.html.
16. Union Says Smallpox Plan Falls Short. CNN, 3 December 2002. Available at: http://www.cnn.com/202002/HEALTH/12/2003/smallpox.vaccine/index.html, accessed 5 December 2002. ("The nation's largest union of health care workers said Tuesday a smallpox vaccination plan being considered by the Bush administration would not do enough to protect such workers.")
17. McNeil, D.G. "Many Balking at Vaccination for Smallpox." *The New York Times*, 7 February 2003. ("Dr. Paul Offit, chief of infectious diseases at Children's Hospital of Philadelphia… 'People are voting with their arms.'")
18. Altman, L.K. and A. O'Connor. "Health Officials Fear Local Impact of Smallpox Plan." *The New York Times*, 4 January 2003.
19. "Hospitals Wary Of Smallpox Vaccine." Washington Times, 12 January 2003. Available at: http://www.washtimes.com/metro/200230112-89432220.htm.
20. Peckenpaugh, J. "Local first responders struggle with federal anti-terror programs," 8 November 2002. Available at: www.govexec.com, accessed 9 November 2002.
21. *Ibid.*
22. Inglesby T.V., Grossman R., O'Toole T. A Plague on Your City: Observations from TOPOFF; Clinical Infectious Diseases 2001; 32:436-445. Available at http://www.journals.uchicago.edu/CID/journal/issues/v32n3/001347/001347.html, accessed 12 October 2002.
23. Tom Ridge Speaks to the Associated Press Annual Luncheon," 29 April 2002. Available at: http://www.whitehouse.gove/news/releases/2002/04/print/20020429-3.html, accessed 2 February 2003.
24. Hoard, M.L., J.M. Williams, and J.C. Helmkamp, et al. "Preparing at the Local Level for Events Involving Weapons of Mass Destruction" (letter). Emerg Infect Dis 8(9), 2002. Posted October 16, 2002.
25. Barbera, J.A. and A. G. Macintyre. "The reality of the modern bioterrorism response." The Lancet (Supplement), December 202002; 360:2-3. Available at: www.thelancet.com.
26. Barbera, J.A. and M. Lozano. "Urban search & rescue medical teams: FEMA task force system." Prehospital and Disaster Medicine 1993; 8(4):349-355.
27. Tom Ridge Speaks to the Associated Press Annual Luncheon," 29 April 2002. Available at: http://www.whitehouse.gove/news/releases/2002/04/print/20020429-3.html, accessed 2 February 2003.
28. Carney, E.N. "U.S. Response: New CDC Director Julie Gerberding Takes the Helm." *National Journal*, 30 September 2002.
29. Medical and Health Incident Management (MaHIM) System. Available at http://www.seas.gwu.edu/~icdm/. The model depiction is attached to this report as an appendix.
30. Major Management Challenges and Program Risks: A Governmentwide Perspective, January 22002003. U.S. General Accounting Office; GAO-2003-95, page 4-5.
31. "CDC Programs in Brief." Available at: www.cdc.gov/programs, accessed 12 February 2003.
32. "Thompson names Hauer to new assistant secretary post," 28 June 2002. Available at: http://www.hhs.gov/news/press/2002pres/20020628a.html, accessed 11 February 2003.
33. "Statement by HHS Secretary Tommy Thompson, on the passage of the Homeland Security Bill," 20 November 2002. Available at: http://www.hhs.gov/news/press/2002pres/20021120.html, accessed 11 February 2003.

Contributors

Dr. Joseph Barbera, M.D.

Joseph A. Barbera, M.D. is Co-Director of the George Washington University Institute for Crisis, Disaster, and Risk Management. Dr. Barbera is an Associate Professor of Engineering and Clinical Associate Professor of Emergency Medicine at The George Washington University. He is residency trained in emergency medicine and family medicine and has been involved in disaster response and emergency management since 1986. He has participated in responses to hurricanes, the Oklahoma City Bombing, mine disasters, earthquakes (Baguio City Philippines, Northridge California, Tou-Liu Taiwan), and biological terrorism threats. He has been the lead medical consultant for the Federal Emergency Management Agency in the development of the National Urban Search & Rescue Response System, and has provided extensive consultation to the U.S. Public Health Service and the Veterans Administration in the development of the National Disaster Medical System.

Dr. Barbera is a medical officer for the Office of Foreign Disaster Assistance International Search & Rescue Program, and has conducted national and international educational programs on medical response to collapsed-structure incidents. As chair of the emergency preparedness committee for the George Washington University Hospital, Dr. Barbera oversaw implementation of a mass patient decontamination and treatment facility and, at the request of the U.S. Public Health Service, is developing a national hospital preparedness model for chemical terrorism. As founder and chair of the District of Columbia Hospital Association (DCHA) Emergency Preparedness Committee, Dr. Barbera led the implementation of a comprehensive Hospital Mutual Aid System for Washington, D.C.

Dr. Barbera provides emergency management and medical preparedness consultation to the U.S. Capitol Office of the Attending Physician, including contingency planning for the Presidential Inauguration and State of the Union Addresses. Dr. Barbera has provided emergency management expertise to multiple other organizations, including the White House Medical Staff, Walter Reed Army Medical Center, and the Washington D.C. Veterans Administration Medical Center. He is a national and international lecturer on emergency management and medical contingency planning subjects.

Dr. Martin C. Libicki

Dr. Martin C. Libicki joined RAND in 1998 as a Senior Policy Analyst. His present field of interest is the relationship between information technology and national security. In that context, he has written *Illuminating Tomorrow's War* (NDU Press, 1998), which examines aspects of the revolution in military affairs, and its impact on DoD's requirements for integrated information. His prior employment included twelve years at the National Defense University, three years on the Navy Staff as program sponsor for industrial preparedness, and three years as a policy analyst for the GAO's Energy and Minerals Division.

Dr. Libicki's other published works include: *The Mesh and the Net: Speculations on National Security in an Age of Free Silicon; Information Technology Standards: Quest for the Common Byte* (Digital Press, 1995); *What is Information Warfare, Defending Cyberspace and Other Metaphors;* "Dominant Battlespace Knowledge and its Consequences" (a chapter in *Dominant Battlespace Knowledge*); "Emerging Military Instruments" in INSS's Strategic Assessment 1996; and the concluding chapters of Strategic Assessment 1998. Earlier monographs include *What Makes Industries Strategic* and *Industrial Strength Defense*.

Dr. Libicki holds a Ph.D. in Industrial Economics from the University of California at Berkeley.

Mr. Michael Scardaville

As a Policy Analyst, Michael Scardaville is primarily responsible for analyzing American homeland defense policy. During his time at The Heritage Foundation, Scardaville has also done research on the United Nations and the Balkans, including the UN and NATO peacekeeping missions in Kosovo and Bosnia.

Scardaville was a key member of The Heritage Foundation's Homeland Security Task Force, which convened shortly after the September 11 attacks. Headed by former Attorney General Edwin Meese and former Ambassador Paul Bremer, the task force developed a detailed plan for the federal government to help reduce the likelihood of future attacks. Scardaville penned a chapter in the final task force report, focusing on infrastructure protection and internal security. He continues to monitor and assess the efforts to create a Department of Homeland Security, including laying out principles to be followed in creating an effective department. He has also analyzed how Congress must reorganize itself in response to the changing threats facing America, gauged the international community's reaction to the terrorist attacks, and looked at actions that other nations can take to show support for the U.S. and the war on terrorism.

In addition to his homeland security studies, Scardaville has written on why the International Criminal Court of the United Nations needs to be reformed, why an open-ended mission in Kosovo was a bad idea for the United States, and how continued ballistic missile proliferation around the world reinforces the need for the U.S. to develop a missile defense system. He has discussed homeland security and national defense with multiple television news outlets and his work has appeared in major newspapers across the country, including *USA Today*, the *Chicago Tribune*, the *San Franciso Chronicle*, and *The Boston Globe*. Scardaville holds a bachelor's degree in international relations from Boston University. He joined The Heritage Foundation in 1999 and was previously employed in the Asian Studies Center and as a Research Assistant in the Kathryn and Shelby Cullom Davis Institute for International Studies.

Dr. Loren B. Thompson

Dr. Loren B. Thompson is Chief Operating Officer of the Lexington Institute where his primary task is to oversee security studies, the institute's largest project. Dr. Thompson is a long-time advisor to high-tech companies, the federal government, and foundations. He conducts most of his for-profit activities through Source Associates, a consulting firm that he heads in Northern Virginia. The areas on which he advises Source clients range from nonlethal weapons to industrial policy to military strategy.

For twenty years, Dr. Thompson has taught graduate-level courses at Georgetown University in military strategy, new technology, and the media. During the 1980s, he was Deputy Director of Georgetown's Security Studies Program, part of the university's School of Foreign Service. He has also taught classes at Harvard University's Kennedy School of Government. Dr. Thompson is widely quoted on military affairs in the national media, having been interviewed by every major newspaper and broadcast network. His commentaries have appeared in publications such as *The Wall Street Journal*, *The Washington Post* and the *Los Angeles Times*. He has also been interviewed by overseas media such as *The Economist*, the *Financial Times*, and Al Jazeera.

Dr. Thompson holds a Ph.D. in government from Georgetown University.

Homeland Security Working Group

Mr. Joseph Barbera, M.D.
Institute for Crisis, Disaster
and Risk Management
George Washington University

Mr. Richard L. Cañas
Betts Global Consulting, LLC

Mr. Frank Cilluffo
Office of Homeland Security

Mr. Joel Feldschuh, MBA
Ganden Security Services Solutions

Ms. Elin A. Gursky, Sc.D.
ANSER Institute for Homeland Security

Dr. Martin C. Libicki
RAND

Mr. Reynaldo P. Maduro, Sr.
Trusted Mission Solutions, Inc.

Dr. David McIntyre
ANSER Institute for Homeland Security

Dr. Steven Metz
Strategic Studies Institute
U.S. Army War College

Mr. Thomas E. Mitchell
Gray Hawk Systems

Mr. Michael Scardaville
The Heritage Foundation

Dr. Loren Thompson
Lexington Institute

Printed in the United States of America

August 2003

Lexington Institute

1600 Wilson Boulevard, Suite 900
Arlington, Virginia 22209
Phone: (703) 522-5828
Fax: (703) 522-5837
www.lexingtoninstitute.org
mail.lexingtoninstitute.org