MARTY LEDERHANDLER/AP

THE WORLD CHANGES:
Manhattan, September 11, 2001.

After 9.11

IN THE HOURS AND DAYS FOLLOWING THE September 11 attacks, most Americans found it difficult to fathom that we now face an ongoing threat of unexpected, mass violence. But Americans have faced such threats before, whether from Indian raids on the frontier, armed political radicals, or enemy bombers and missiles. Government has always taken the lead in countering those threats, with results that sometimes were successful but other times restricted our rights or wasted our resources.

Now, in response to the September 11 attacks, government decision-makers are considering numerous policy proposals, ranging from increasing military spending to radically changing the operating procedures of America's public health and law enforcement agencies. According to proponents, those actions are necessary to protect civilians. But opponents worry that the new proposals, like some policies of the past, will interfere unnecessarily with Americans' rights and resources.

This special report examines five policy areas that are under scrutiny in the aftermath of the September 11 attacks. In the first report, defense analysts Harvey Sapolsky and Eugene Gholz argue that a number of key Pentagon and congressional decisions made after the attacks may lead to a substantial waste of taxpayers' dollars. The second report, by technology specialist John Wohlstetter, examines the crippling effects that the terrorist attacks had on New York City's telecommunications, and calls for regulatory changes that would encourage system redundancies and robustness. The third report, by transportation analyst Laurence Phillips, describes the effects that the attacks had on a variety of transportation modes, and argues that the use of new "smart" technologies would greatly enhance our ability to identify, track, and verify the identity of airline travelers and employees. In the fourth report, public health expert J. Donald Millar examines the response of the U.S. public health system to the attacks, and considers the system's role in the fight against bioterrorism. The final report, by law enforcement expert John McNamara, points out that, despite an expansion of the federal role of protecting "homeland security," it is the local police, firefighters, physicians, and paramedics who will fight the defensive battles in the war on terrorism, and we must be careful to adopt policies that help those local emergency services personnel with their work.

In those and other policy areas, the choices that we ultimately make will define how the world has changed after September 11. R

DEFENSE

The Defense Industry's New Cycle

By Harvey M. Sapolsky, *Massachusetts Institute of Technology*
and
Eugene Gholz, *University of Kentucky*

The American defense industry is ready for the new war. In fact, it has been ready since the late 1980s when the Cold War petered out. The 40-year-long Cold War convinced industry leaders that war (or, at least, the preparation for war) was a solid if cyclical business. Vietnam followed Korea, and the Reagan buildup followed Vietnam — about every 15 years the spending cycle peaked with a Cold War crisis, but the demobilizations from the crises were never complete. Weapon acquisition spending including research investments rose and fell within a $90 – $150 billion band. In the late 1990s, even without a clearly designated enemy, weapon purchases began to climb from their post-Cold War lows. The savage September 11 attacks on America assure the development of a full new cycle of buying military hardware.

Decisions The autumn of 2001 was fraught with realignment in the defense sector. Before the attacks, some key decisions about the future had been scheduled for the fall. The Quadrennial Defense Review (QDR) report, intended to set the overall national security strategy, was due at the beginning of October. The Department of Defense was expected to decide whether it would object to the proposed acquisition of Newport News Shipbuilding by its competitors. And the military services were scheduled to choose between proposals from Boeing and Lockheed Martin for the winning version of the richest aircraft program in history, the Joint Strike Fighter (JSF).

Along with those decisions, several new ones were made in direct response to the terrorist attacks. The defense budget environment changed immediately, superseding much of the analysis in the QDR and truly starting the new uptick in the budget cycle. Decisions on specific programs were accelerated, including the purchase of two aerial refueler versions of Boeing's commercial 767 jet transport. The four key decisions made since the September 11 attacks — on the level of the defense budget, the consolidation of the shipbuilding sector, the JSF procurement, and the 767 tankers — give indication of problems that lie ahead in America's defense industrial policy.

Those problems may lead to a substantial waste of American taxpayers' resources. The short-term decisions since September 11 have continued a trend towards wasteful "jointness" without any budget constraints. But there is hope for a solution to the new defense pork barrel: The United States could remember the way that President Eisenhower managed the first great spending surge of the Cold War era, and we can apply its lessons now. Capping the topline level of defense spending — that is, imposing a budget constraint on the military services and defense contractors — can lead to military innovation if competition is allowed to flourish under the cap. The United States should not seek to plan a particular, unified response to national security problems, just as we do not seek to plan the details of the national economy.

THE DEFENSE BUDGET ENVIRONMENT

Defense is a highly politicized business. The federal government, through several purchasing agencies, is the industry's only buyer, and it is a quirky one. Money for projects must be authorized and appropriated by Congress, where

Harvey M. Sapolsky is a professor of public policy and organization at the Massachusetts Institute of Technology and director of MIT's security studies program. His areas of special interest include defense, science, and health policy. Sapolsky has authored several books, including *Science and the Navy* and *The Polaris System Development*. He can be contacted by e-mail at sapolsky@mit.edu.

Eugene Gholz is a visiting assistant professor at the Patterson School of Diplomacy and International Commerce at the University of Kentucky. His research primarily concerns defense management, the creation of national power, and the effects of public policy on high-tech competitiveness. He can be contacted by e-mail at egholz@alum.mit.edu.

DAVE MARTIN/AP

RETURNING FROM ACTION: A Navy F/A-18C approaches the carrier USS Theodore Roosevelt.

local interests predominate. Government policies determine the industry's market structure, conduct, and performance. There can be no foreign sales without the government's approval. The industry's prices and profits are regulated, as are the types of information that firms can provide to shareholders, employees, and foreign customers.

When nearly every issue in an industry is a federal case, politics becomes crucial to nearly every industry decision. And the politics that count the most in weapon purchases are often influential politicians' desires to support hometown jobs and local companies' profits — "pork," in the vernacular.

Needed: a threat But the desire for pork can be trumped. When the nation's security is at great risk, local interests are pushed aside. We took the Soviet challenge seriously. Several times during the Cold War, and especially in its early years, the nation felt gravely threatened by Soviet capabilities or actions. At those times, the military's desire for effective weapons was given preference in defense procurement decisions. Under-performing companies were fired, as Curtiss-Wright, Republic Aviation, and Todd Shipyards all discovered. Inefficient facilities were closed. New competitors were created to stimulate responsiveness from unfocused contractors, as Pratt & Whitney found out when the Air Force restored General Electric to the military aircraft engine acquisition mix in the late-1970s.

But when the external threat faded, so did the military's resistance to local interests. In the decade after the collapse of the Soviet Union, despite a wave of consolidation among defense firms and a major shift in the strategic environment, only a single major weapon system assembly line closed: the excruciatingly expensive B-2 bomber. Now, there is discussion of restarting B-2 production — partly based on a strategic vision of "global reach," but also in reaction to steady lobbying from local interest groups that would benefit from additional bomber production.

More important than the details of the B-2 saga, however, is the survival of all of the other major weapon system projects begun in the waning days of the Cold War (even though their design parameters focused on responding to a no-longer-extant Soviet Union). While individual air defense technologies used by potential American adversaries are

improving — fighters, surface-to-air missiles, advanced radars and electronics, etc. — no country is deploying or can afford to deploy the full complement against us. As a result, the United States has little need for a full new generation of super-expensive, high-performance fighters. Yet U.S. plans for sweeping tactical aviation upgrades proceeded in the 1990s without regard to the projected "budget train wreck" that the upgrades will produce. Other, perhaps more important, defense programs could be squeezed out when the tactical air programs' spending needs surge in a few years. Without a compelling argument that national security would be threatened by pork barrel spending, local interests such as those backing big tactical air programs overwhelmed efforts at rational defense planning.

Pork priority America's "new war" on terrorism has come to the rescue of the defense budget planners who failed to prioritize acquisition programs. Beginning with the supplemental defense appropriation last fall and continuing with proposals for the new year's defense budget, the financial constraints facing the defense community seem to have been voided. Even before September 11, observers had come to believe the QDR would fail to draw specific implications for resource allocation, just as its 1997 predecessor had failed. In the aftermath, trapped by the report's statutory deadline that came hard on the heels of the attack, the investigators just stapled on a few addenda about new efforts to ensure homeland security. The defense budget is certain to be sharply higher as politicians scramble to affirm their commitment to that goal.

If the heightened concern for security threats during the new war were to have similar effects on acquisition planning as Cold War fears of the Soviet threat, then there would be reason for optimism. However, the new war is likely to be different on the pork front. Terrorists savagely attacked America's civilian population, and the possibility of additional attacks seems unabated, so the security environment might be deemed very threatening, like the Cold War. But the needed response from the defense industry for the current crisis is quite small. A few billion dollars to procure specialized helicopters and other gear for special operations forces, and a few billion more for precision-guided weapons, would appear to be all that is required from traditional defense acquisition channels.

But rather than deferring to military preferences, it will likely be business as usual for defense contractors. Politicians still need to show that they are "doing something" to prosecute aggressively the war on terror, so they will do what they do best: Throw money at the problem. Congress's willingness to cough up more money for defense will mean that backlogged "legacy" projects will be funded, no matter their lack of relevance to the terror threat. With deficit spending apparently restored to political legitimacy, any pressure in favor of rational security planning that might have been brought to bear in the future is now gone. In this new war, we will both have our pork and eat it, too.

> The new war on terrorism has voided the defense community's financial constraints and rescued budget planners who failed to prioritize weapon research and acquisition programs.

DEFENSE INDUSTRIAL POLICY

Three big defense-sector events since September 11 address specific companies and projects: the Defense Department's intervention in the Newport News Shipbuilding acquisition, the hasty purchase of some modified Boeing 767 jets by the Air Force, and the multibillion-dollar Joint Strike Fighter decision. In a different defense budget environment, each of those decisions might have come out differently. But instead, each decision reveals inefficiencies and mistakes in politicians' understanding of the unique situation in the politicized defense sector.

Shipyards Two companies, General Dynamics and Northrop Grumman, already own five of the six shipyards that build large warships for the U.S. Navy. Acquisition of the sixth, Newport News, became a competition between those two suitors. General Dynamics currently owns three yards, including Electric Boat — the only yard besides Newport News that has the capability to design and build nuclear-powered submarines. Northrop Grumman owns the other two, including Ingalls in Mississippi. Last fall, the government decided to bestow Newport News on Northrop Grumman.

The government said that it blocked General Dynamics' bid for Newport News because the combination would give General Dynamics a monopoly on the design and construction of nuclear-powered warships. Such a monopoly allegedly might hinder innovation and disadvantage the government in future pricing negotiations. But such competition is already suppressed through the pork barrel policy of allocating ships among yards: There is no effective competition for ships because the current system continues to give shipbuilding contracts to a few high-cost private yards.

In the past, the Navy hedged its shipbuilding bets by using government-owned yards as a competitive threat. For instance, in the interwar period when Electric Boat was the only commercial yard kept alive to build submarines, the Pentagon formally qualified the Portsmouth Naval Shipyard to build submarines, in case the relationship with Electric Boat soured. Again, in the early years of the Cold War, government yards were called upon to supplement the private yards building nuclear-powered submarines. Today, the government yards only do repair

work, but they and other private yards could again be qualified to construct new nuclear submarines or aircraft carriers, if that were required to sanction poor performance by a private monopoly. Private shipyards hold a monopoly in new construction not because they hold the only possible capacity or are necessarily the most efficient builders, but rather because they have the best political connections. And as the Navy essentially is their only customer, they are already public wards if not public yards.

Air tankers Struggling with a commercial airliner market hard hit by terrorism fears, Boeing is about to get some government help in the form of orders for 767 aerial refuelers. The Air Force's existing fleet of KC-135 tankers, numbering in the hundreds, was built by Boeing in the 1950s and '60s and has been getting a workout in America's many overseas military ventures since the end of the Cold War. Periodic overhauls have kept the KC-135s in pretty good shape, but the war in Afghanistan has provided Congress with the opportunity to renew the fleet while helping Boeing meet the challenge of declining airliner sales. Two 767s are in the supplemental appropriations bill just approved by Congress. A lease of another hundred at a cost of about $22 million a year per aircraft has been proposed — a major windfall for Boeing.

Rushing to support Boeing by procuring 767 tankers is a bad idea for two reasons: On the military side, it circumvents normal contracting procedures that might lead to a better product. On the commercial side, it may weaken the American position in trade conflicts with Europe.

Design difficulties In accordance with a contract signed last summer, the Italians have already agreed to pay much of the fixed cost of converting the 767 into a military refueler. That agreement may appear to offer some cost savings to the U.S. Air Force, but the savings could prove to be a mirage. An Italian adaptation of the 767 airframe will be designed for Italian Air Force requirements, which are likely to be significantly different than American requirements for a tanker (given the different mission profiles of the Italian and American air forces). With a less ambitious military and a smaller overall defense budget, the Italians may be more willing to settle for a modified, off-the-shelf, "low-end" acquisition rather than the sort of optimal, long-term solution that the American military deserves. Also, allocating the tanker contract to Boeing may have negative repercussions for defense industrial policy. Political reasons already account for too much of the post-Cold War defense budget; adding tanker/utility aircraft acquisition to the pork barrel will just expand opportunities for inefficiency.

The overarching point is that we will never know the true opportunity cost of opting for the 767 tanker. The supplemental appropriation (and the potential follow-on plan to lease a large fleet of 767s) chose the Boeing airplanes without a defined list of military-technical requirements against which to measure the planes' performance. The rushed process also denied Boeing's competitors (and Boeing itself) the opportunity to propose new designs tailored to American military requirements. New designs might even capitalize on new technologies not easily retrofitted to the 767 airframe. Lockheed Martin has substantial design and production expertise in military transport and utility aircraft. That expertise may be lost if Boeing's commercial business steals the tanker market through short-term thinking during the war on terrorism. An even worse alternative is that post-Cold War pork barrel politics will find a way to support both the Lockheed and the new Boeing utility aircraft teams, further increasing the number of mouths to feed with the defense acquisition budget.

Trade troubles Furthermore, government's role in the commercial aircraft industry has been a source of trans-Atlantic friction for many years. In the past, the Europeans have alleged that Boeing's success in the commercial aircraft market is attributable to spin-off benefits of its defense contracting, and they have specifically drawn links between the company's manufacture of jet tankers like the KC-135 and commercial transport aircraft like the original 707.

The best evidence on the subject suggests that those industrial policy links between defense procurement and commercial competitiveness are weak, because the quirky, powerful military buyer always demands first priority from its suppliers and never would accept diversion of effort, funds, or technological investment to commercial projects. But whether the links really exist or not, the United States's best defense in the commercial trade conflict has always been that any connections were small, unintentional, and in the distant past. If the military now starts to buy Boeing commercial airplanes to use as tankers (especially with the explicit intention of shoring up Boeing's flagging commercial airliner business), the Europeans are bound to raise the "military subsidy" issue. They may use it to score real points in future trade conflicts, and such an opening to European trade policy negotiators might be especially hurtful at a time when WTO talks on the further opening of global markets are getting underway.

The European response to the 767 tanker buy might also directly harm openness in the aircraft sector itself, if it justifies European government support for Airbus's new super-jumbo A380. The purchase of 767 tankers in the post-September 11 defense budget supplemental should not be expanded, because it is likely to trigger a new round of trans-Atlantic trade conflict and high-tech industrial policy initiatives.

JSF In contrast to the 767 tanker buy, the Joint Strike Fighter decision process was anything but hasty. It came on schedule, war or no war, after years of engineering devel-

opment, prototype construction, and testing.

The trouble with the JSF deal is that the overall project — specifically its overwhelming size and expense — is ill conceived. The plan to buy a single basic airframe for all of the military services is dangerously inflexible in the present uncertain security environment. By forcing all players in the defense industry to work together on a single mega-project, the JSF program will introduce costly inefficiencies into the development and production process. What is more, buying so many copies of the same basic airframe will stifle the creativity of the defense industry's design teams by leaving them with little "clean sheet" design work for many years.

Scale economies In the JSF competition, Lockheed Martin's XF-35 was selected over the Boeing XF-32. Both entries were tremendously successful aircraft on technical grounds — far more advanced than any other country's best — but the secretary of the Air Force announced that the Lockheed Martin plane beat the Boeing prototype across the board. Current plans promise a buy over the next 20 years of more than 3,000 aircraft, worth more than $200 billion. Versions of the JSF are to serve the Air Force, Navy, Marines, and the British military as replacements for the F-16, AV-8, A-10, and some F/A-18s.

Commonality in design and parts manufacturing among the versions is intended to generate significant cost savings as the aircraft goes into production. Unfortunately, experience in previous efforts at cost savings via "joint" projects has not been good. A "deluxe" design that produces an aircraft with high performance across a diverse mission profile can prove much more expensive than separate, run-of-the-mill designs optimized for each specific mission. The most obvious analogy is to the 1960s-vintage F-111, which came in well over budget for a product that both the Air Force and Navy ultimately did not like.

In the end, the JSF question is about the power of economies of scale, which we know are quite strong in the aircraft industry. By combining several missions into a single basic airframe, the government hopes to drive down costs. Even if the cost curve for the deluxe, multi-function parts starts out higher, the multi-function aircraft might turn out to be cheaper — if the tail of the cost curve continues to drop rapidly for later production units (e.g., aircraft numbers 500-1,000). But experience has shown that the biggest learning effects and scale economies are achieved in the early stages of production. That experience suggests that the advantage of extending the production run is likely to be small relative to the cost of the deluxe design.

Sharing the pie Another effect of buying multiple versions of the same JSF design rather than buying several different aircraft is that the entire defense sector is forced to join this one project. Economically, it seems plausible that Boeing could stay in the military aircraft game (if there were profitable future projects) without a role on the JSF. But in the political defense business, everyone knows that JSF funding will be more secure if Boeing is not frozen out of the project. E.C. "Pete" Aldridge, the undersecretary of defense for research, acquisition, and logistics, has already announced that he would like to see Boeing as a subcontractor on Lockheed Martin's JSF.

That production sharing, which will expand on already-complex arrangements involving several manufacturers on Lockheed Martin's XF-35 "team," is usually a formula for increasing costs. As with so much of recent weapon procurement as well as warfare, coalition building becomes a requirement and distracts from efficient allocation of design and manufacturing work. Building wings here and cockpits there — long the inefficient practice in Europe — is apparently now the standard in the United States, too. Trying to build three planes in one will be a make-work project for everyone.

Diversity of design Finally, the JSF mega-project will undermine the core strength of the U.S. defense industry: its design and systems integration capability. During the 20+ years of the program, the JSF essentially will be the only game in town. Though there will be ongoing JSF engineering work (in response to demand for small adjustments to the production process and to improve certain aspects of the aircraft design, as well as more significant upgrades from the initial "A" version to later "B" and "C" versions), those small projects will not allow design engineers to exercise their true creativity or to gain experience in measuring the real advantages (and disadvantages) of creating new designs from scratch.

The United States won the Cold War by emphasizing technological prowess rather than mobilizing more capital or labor for the fight than the Soviets did. We gained tremendous expertise by experimenting with a plethora of design approaches. Designers practiced on a diverse array of projects during their careers. Under the projected JSF procurement, many top designers are likely to lose interest in the aircraft industry, and we will squander the human capital advantage that we now enjoy as a beneficent legacy of the Cold War.

THE COMPETITION SOLUTION

Wars usually force choices. Some weapon systems, some types of forces, some theaters of conflict are deemed more important to the war effort than others. The pain involved in setting priorities often is overcome by fears of failure and casualties. But the war on terrorism is heading in a different direction.

The new war's budget bounty will allow the United States to avoid setting priorities. Specific needs in transportation and other vital infrastructure security command attention, but nearly every corner of defense can claim relevance to the new war. Satellites monitor terrorist camps, tanks are ready to fight host nations, and submarines fire missiles and gather intelligence. Bureaucracies, like the military services and intelligence agencies, are good at finding

favored rationales for their work, and that makes resource allocation difficult.

Budget ceiling The task for political leaders is to prevent the war from becoming a feeding frenzy for contractors and their government patrons. If we are willing to risk blood in the fight against those who attacked the United States, then we should be willing to discipline our appetite for local advantage, pork, and the next contract. The paramount goal should be to defeat specific enemies, and the way to keep defense planners focused is to cap the defense budget. If the fight against the Soviet Union and its worldwide interests cost on average $350 billion a year in 2001 dollars, then a global war on al Qaeda and its collaborators deserves no more — and perhaps less, given the relative resource bases of the USSR and our terrorist adversaries.

A budget ceiling gives participants in the war effort a constraint against which to value their efforts. The measure of everything becomes the likely contribution to victory. That focus gives political leaders the opportunity to avoid mistakes as well as expenditures. Prior to September 11, Defense Secretary Donald Rumsfeld had ordered a multilayered review of defense programs in preparation for a "transformation" of the U.S. military from its Cold War structure to one he claimed would be appropriate for the new century. But the studies produced by that review seemed confused, with neither an enemy nor a path to a transformed military clearly outlined. Instead, there were vague notions about information warfare and a military ready to conduct it. With a real war at hand and more than enough military force of the right kind to fight it, we can jettison the quest to reorganize and reequip the military for some unspecified future conflict. The administration should sink the short-term transformation.

Meanwhile, the Department of Defense should continue to prepare options for a time when the appropriate direction for transformation becomes clear. Decisions on weapon systems development and research investment are decisions that affect the American military force structure over the long term. Future threats to the United States will take years to develop, and it is to those threats that the present acquisition decisions must cater.

Adaptation The best policy during a period of strategic uncertainty is to take steps to minimize the time it will take for American forces to adapt in the future, when a threat becomes clear. One component of that preparation is investment in intelligence efforts, so that we can identify threats sooner. But even if a future threat surprises the United States, as the terrorist threat surprised the United States on September 11, America's latent defense capability can rise to respond — as long as it is not over-committed to a specific, unsuitable path by premature defense planning.

In fact, the American pattern has always been to adjust rapidly late in the game, after the international security environment becomes clear. We prepared for the Axis threat after the start of World War II in Europe, to the communist threat in 1950 (after the unexpected attack on South Korea), etc. By moving second — and relatively quickly at that point — we did not squander resources on as many false starts. Instead, we invested them in innovative options, building technological advantages against our enemies. We should take the same steps today to get ready for possible strategic competitors in the decades to come.

> Competition among the military services and defense contractors should be valued rather than suppressed, because it is the engine that drives military and technological innovation.

Fortunately, the best way to organize America's defense for experimentation is consistent with the best organization for fighting the current war on terrorism: Promote competition both within the military and between defense contractors. Competition among the services in experimentation and war should be valued rather than suppressed, because it is an engine for military innovation. We should also stop pretending that we can rely on false competition among private sector defense firms to promote innovation; the industry is simply too politicized for supply-side competition to work. As a result, industrial policy decisions like the Newport News one are foolish. The attempt to use the defense budget to bail out Boeing's commercial aircraft business is just another example of the politics that infect the current acquisition process.

The government should take several concrete steps. A ban on joint projects like the JSF would be a start. The government has already paid to design the JSF itself, so that deluxe development is a sunk cost that we cannot get back. The best thing to do now would be to focus the "advanced development" work on the missions at which Lockheed Martin's XF-35 is most adept and to shrink the proposed JSF buy. That would enable the start of a new design competition for another aircraft — one that we might or might not buy in numbers, depending on how it matches future evolutions of the threat environment. Another useful policy idea would be to reward contractors for research and development work at least as well as they are rewarded for production work.

Most important, each of these policy proposals — promoting inter-service rivalry, trimming the JSF and banning future joint projects, and rewarding R&D work — would be easier under a binding budget cap. The first step to America's future security is holding the line on the nascent new cycle in defense spending. R

The Vulnerability of Networks

By John C. Wohlstetter
Discovery Institute

THE ATROCITIES OF SEPTEMBER 11 NOT only revealed the vulnerability of people living and working within America's borders, but also the vulnerability of our high-technology information society. Collapsing with the twin towers was a veritable mother lode of network communications equipment. For want of communications alone, the New York Stock Exchange could not have reopened that terrible week. In the aftermath of the attack, concerns about network reliability (i.e., maintaining connectivity) and security (i.e., protecting the integrity of databases and communications) have intensified greatly.

Two factors amplified the telecommunications vulnerabilities exposed on September 11:

- The vast increase in the Internet user population, and the evolution of the Internet into a form of mass communication.
- Current telecommunications regulatory policies that prefer shared local exchange facilities to separate ones, thus discouraging multiple local facilities.

As the United States looks for ways to improve the security of its citizens, government and the telecommunications industry must also find ways to improve the reliability and security of our large and vital communications networks.

THE MASS-MARKET INTERNET

The advent of broad public Internet access has transformed network security by adding vast numbers of users, many of whom have only rudimentary computer skills. That, in turn, has complicated the task of securing networks. The administrator of a private network has authority to control the behavior of users, employing such tools as frequent password changes, limiting access to portions of the network, and restricting access to work-related sites. What is more, private networks once were used primarily by people with a significant amount of general computer knowledge and particular expertise with their own network. That, in turn, provided an additional layer of security by restricting access.

But those security protections are anathema to commercial Internet service providers that compete to attract customers based on their systems' ease-of-use, ready access, and broad interconnectivity. A network is only as secure as its most careless user. And so, public networks are endemically vulnerable to hostile entry. Securing those networks will require implementing special protections as part of the next generation of computer and Internet software. Until now, security has not been a high priority of software designers, and the biggest holes are in the most popular releases. Programmers will plug holes only if consumers demand it. The federal government, as the largest buyer in the software marketplace, can insist on better security and thereby drive developers to respond.

TELECOMMUNICATIONS

Similar to the Internet, America's public-switched telecommunications networks are, in reality, a web of linked computers with terminals (computers, phones, or faxes) attached at the customers' premises. Voice networks thus share the vulnerabilities of their datanet cousins: In an effort to build systems that are easy to use, readily accessible, and have a broad activity, telecommunications companies (under the jurisdiction of federal regulatory agencies) have built systems that are vulnerable to deliberate attack. To decrease that vulnerability, significant changes must be made to both the system's hardware and software.

Hardware Network plant vulnerabilities primarily arise out of physical proximity. Switching and routing equipment that provide the telecommunications backbone for a geographic area often are located in just a few buildings, making an easy

John C. Wohlstetter is a senior fellow of the Discovery Institute, where he specializes in technology deregulation. He is a former director of technology affairs for GTE Corp.

ERIC FEFERBERG/AFP

COMMUNICATIONS IN SHAMBLES: An office near the World Trade Center.

target for attack. That fact was underscored on September 11 when the World Trade Center collapse knocked out a telecommunications facility in Lower Manhattan that supplied 80 percent of the New York Stock Exchange's communications capacity. That was not the nation's first experience with such a failure: In May of 1998, the destruction of a single station in the Chicago suburb of Hinsdale, Ill., knocked out the facilities of several major carriers.

The May 1998 incident and the September 11 attack underscore a simple truth for communications infrastructure technologists: You cannot build a smart network with dumb buildings. Despite the growth of local loop entry following the passage of the 1996 Telecommunications Act, network concentration has persisted. FCC data show that, between 1990 and 1999, the total number of Bell central offices rose by one percent to 9,968, while total phone lines they serve jumped 34 percent. As for Bell's rivals, one study shows that less than 10 percent of competing carriers have facilities fully separate from Bell networks.

Software Even more worrisome than the vulnerability of hardware is that of software. Software is global, programmable, accessible, and fragile. Its global reach means that widely separate geographic hardware infrastructure nodes can all crash if controlled by a unitary software superstructure that fails. Programmable features give network software enormous flexibility to control and reconfigure hardware, but such power potentially is available to all users (including those with malevolent intentions) who have the skill to bypass network firewalls. Open access means that hostile users have access to network innards that in earlier times were beyond user reach. And software's fragility makes fixing it a demanding task.

As an example of the software vulnerability of telecommunications networks, consider the AT&T network crash on Martin Luther King Day, 1990. A single punctuation mark at the end of a single line of software code (in a multimillion-line code switch) caused AT&T to lose over half of its long distance capacity in 19 minutes, on one of the busiest calling days of the year. AT&T's network-signaling software controlled switching hardware dispersed nationwide. Programmed mistakenly, the software altered how the network worked, and not for the better: It crashed. And that failure was the result of a simple programming mistake; one can only imagine the results of an attack engineered to produce the broadest possible effect.

In essence, software represents a kind of Information-Age Faustian bargain: Hardware controlled by software is vastly more flexible than the old-time systems of pure hardware because the contemporary systems are reconfigurable in real-time, thus offering users many options. But software's accessibility, global reach, and fragility make for vulnerable systems. It will take consequential advances in software architectures — e.g., partitioning of dual software systems to support hardware, to break that bargain — and that will be no easy task.

Diversity What remedies might be proposed for such vulnerabilities? Perhaps the best would be for networks to embrace an old piece of conventional wisdom: Never rely on one of anything. From a hardware standpoint, physical geographic diversity is essential; new local loop plants would decrease the possibility of broad disruptions in telecommunications from the destruction of a single facility. The industry could also use technology diversity to complement spatial diversity: Wireless and wireline could provide mutual redundancy.

Turning to software, diversity also would be valuable. The 1990 AT&T network crash showed that a single-point software failure can be as devastating as any hardware failure. Today's commercial software is riddled with security holes, including "backdoors" unknown to most users but exploited by hackers. It would be far better for industry to build added robustness and adaptability into networks to enable rapid return to normal should a disruption occur. It is the equivalent of the Cold War strategy of hardening missile silos so as to withstand a first strike, preserving a retaliatory capability. Telecom networks can be remarkably resilient if built wisely.

The FCC's role The Federal Communications Commission (FCC) came to network reliability reluctantly. Neither the Martin Luther King Day AT&T crash nor several Bell company network crashes in the summer of 1991 spurred the agency to act. It took an AT&T outage in September 1991 that shut down LaGuardia Airport (leaving two FCC commissioners stranded on the tarmac) to get the agency's attention.

Prodded by Congress, the FCC established the first Network Reliability Council, convened early in 1992. In all, there have been five panels, each focusing on accidental outages (the fourth and fifth panels were named Network Reliability and Interoperability Council — NRIC). The most recent panel met last October 30, and aired reports on damage and recovery after the September 11 attacks. A new NRIC will be convened this January (the panels have a statutory two-year lifespan, per the Federal Advisory Committee Act), with homeland security, no doubt, slated to be its prime focus.

FCC policies since the AT&T divestiture have endeavored to promote the entry of competitors into the local loop market, a process intensified by passage of the 1996 Telecommunications Act. Unfortunately, those policies have exacerbated the vulnerabilities discussed above: Encouraging the sharing of local loop facilities — e.g., switching centers, lines, cell towers, mobile telephone switching offices — has concentrated multiple carriers into single locations, providing attackers with attractive targets. Limiting incumbent carriers' ability to control access to their facilities (in an effort to prevent the incumbents from limiting competitor access to shared facilities) has increased the chance of successful penetration of network facilities. Promoting the use of open network architecture to facilitate network access for competitors has also increased the opportunities for malicious users to penetrate network systems. Making matters worse, the FCC has allocated only 189 MHz of spectrum for domestic wireless use (as compared to over 300 MHz in several European countries and Japan), thus limiting the use of wireless hardware to diversify telecommunications infrastructure.

The FCC and other federal agencies must alter their regulations and policies to address those shortcomings and to promote reliability and security. Among the changes that should be considered:

- Implement policies to encourage competitors to build their own facilities instead of continuing to share facilities with the local Bells.
- Allow incumbent firms to vet all personnel with access to sensitive facilities — perhaps using biometric authentication and security checks — to prevent penetration by malevolent agents.
- Allocate additional spectrum that was dedicated to high-definition television, thus enabling the U.S. domestic cellular spectrum to match European allocations. That would enhance backup reserves greatly, and also would increase wireless capacities during an emergency. (Wireless optics that are being deployed in Manhattan as part of the post-September 11 restoration will also help.)
- Amend tax law to accelerate depreciation of existing plant, and apply rapid write-off to investment in redundant critical network components.
- Implement service priority procedures (designating which users have priority in a crisis — police, fire, medical, etc.) that ration capacity in large urban areas.
- Promote broadband deployment by exempting new technology investment from regulation, including in the local loop. With enough new broadband capacity, there would be no need for priority rationing.
- Act as a trusted intermediary for the sharing of sensitive network information, in order to improve inter-network operations in the event of disaster or attack.

Above all, enhancing network reliability and security will require the market interactions of customers demanding access redundancy and service suppliers deploying duplicative assets to meet the demand. Just as no Wall Street firm that moves back to Lower Manhattan will rely on a single connection anymore, so businesses nationwide will add backup for key network assets (just as they did prior to Y2K). The FCC can further help by more deregulation, especially concerning the local loop. Software solutions will have to be largely customer-driven, as suppliers show little sign of fixing things on their own. As for the human element of security, getting people to not use "mom" as their password may prove the biggest challenge of all. R

A Crisis of Security and Economics

By Laurence T. Phillips
U.S. Department of Transportation

THE ATROCITIES COMMITTED ON SEPTEMBER 11 imposed substantial short-term and long-term costs on the U.S. economy. While all sectors were adversely affected by the attacks, many transportation firms experienced especially serious harm.

As a result of the attacks, we are beginning to see a significant reallocation of private and public expenditures away from investments that would have increased transportation capacity and raised productivity, toward those that are deemed necessary to ensure safety and security. As a result, shippers will face higher costs and fewer options, and some may be forced to redesign their just-in-time supply chains and distribution systems. Air travelers are experiencing longer trip times and more inconveniences that, in turn, threaten to reduce demand for air travel. Other transportation industries could also experience lower capital and labor productivity, higher costs, and reduced demand for their services if new federal laws, regulations, and security procedures prove ineffective.

AVIATION

Even before the September 11 attacks, analysts were predicting that the U.S. airline industry would lose $2.5 billion in 2001 because of the slowing economy and a surprisingly large decline in business travel. After the attacks, air carriers grounded hundreds of planes and cancelled thousands of flights. Industry capacity was slashed by at least 25 percent and thousands of employees were laid off. In an effort to draw customers, airlines instituted dramatic fare reductions that cut prices by as much as 40 percent in some markets.

Despite those moves, air travel demand collapsed further, and the airlines incurred enormous daily financial losses. Six weeks after the attacks, airlines reported record third-quarter losses — "hemorrhaging money," in the words of former United Airlines CEO James Goodwin. By the numbers, the nine largest U.S. air carriers had operating expenses of $26.7 billion in the third quarter of 2001 (80 percent of which had transpired prior to September 11) as compared to operating revenues of only $21.5 billion, thus producing an operating loss of $5.2 billion. The General Accounting Office now estimates that U.S. airlines will lose between $6.5 billion and $10.5 billion as a result of the terrorist attacks, an estimate that may prove to be too low. Most analysts are predicting that several carriers will be forced to file for bankruptcy in 2002.

Airports The financial tidal wave that engulfed the airlines also swept across the nation's airports. At a time when they were forced to incur tens of millions of dollars in higher security costs (e.g., paying overtime wages to local police officers), their revenues plummeted because of fewer passengers and flights. Los Angeles International Airport, for example, estimated that its revenues would decline by as much as $108 million in the first year after the attacks. As a result, credit agencies have warned that airport bond ratings could be downgraded.

Airports have responded to the financial crisis by lobbying for federal aid and delaying or deferring new terminal and runway projects — projects that only a few months earlier were deemed essential to relieve congestion and reduce delays. The airports also are considering imposing higher fees (perhaps substantially higher) on airlines and concessionaires to cover the costs of installing new security measures.

Federal aid On September 22, President Bush signed into law the Air Transportation Safety and System Stabilization Act (H.R.2926). The act provides some $15 billion in funding to implement new security measures and offset the financial losses experienced by the airlines. Given the size of the financial crisis facing the air industry after the attack,

Laurence T. Phillips is a senior policy adviser for the U.S. Department of Transportation. The views expressed in this article are solely those of the author.

the unprecedented grounding of the nation's air fleet for several days, the understandable desire by congressional and executive branch policymakers to take some action in the face of the crisis, and the effectiveness of the industry's lobby, it is not surprising that the airlines received federal assistance. What is surprising is the speed with which the aid package was enacted into law (10 days), its size, and the lack of restrictions on its distribution.

The act provides $5 billion in cash for air carriers ($4.5 billion for passenger carriers and $500 million for cargo carriers) as compensation for the "direct and incremental losses incurred as a result of the September 11 attacks." Any carrier that can demonstrate to the U.S. Department of Transportation that it has incurred such losses is eligible for assistance, regardless of its financial status before the attack or its long-term prospects. The act also authorizes the secretary of transportation to take appropriate action to ensure that all communities that received scheduled passenger service before September 11 continue to receive "adequate" service, a provision that could be used to justify partial re-regulation of the industry.

The distribution of the $5 billion is based on simple market-share formulas (share of available seat-miles for passenger airlines and share of revenue ton-miles for air cargo carriers). For example, United Airlines, the second largest domestic air carrier, should ultimately receive slightly less than $800 million.

The legislation also establishes the Air Transportation Stabilization Board, the members of which are the chairman of the Federal Reserve and the secretaries of Transportation and Treasury (the comptroller general is a nonvoting member). The board is authorized to guarantee $10 billion in loans if it determines that credit is "not reasonably available" for an air carrier, that the obligation is "prudently incurred," and that "such agreement is a necessary part of maintaining a safe, efficient, and viable commercial aviation system in the United States."

To many observers, the broad statutory discretion afforded to the board indicates that Congress expects most, if not all, loan-guarantee applications will be approved. But some parties, both inside and outside government, argue that it makes little sense to provide financial life support to airlines that, even before September 11, were seen as likely candidates for bankruptcy. Thus, even before the first loan-guarantee application was filed, it was clear that, for better or worse, the board's decisions will mean financial life or death for some air carriers and thus will alter the industry's structure and the intensity of future airline competition.

Security The consensus that made it easy for Congress and the executive branch to enact an airline financial aid package in a matter of days broke down when it came to deciding what

HEIGHTENED SECURITY:
A National Guardsman at Newark Airport.

DANIEL HULSHYER/AP

should be done to improve airport and aircraft security. Of course, there was strong agreement both in Congress and the general public about the need to adopt initiatives such as strengthening cockpit doors, increasing the flow of sensitive criminal and national security information from federal agencies to airlines, updating airline and airport employee identification credentials, conducting detailed employee background checks, deploying federal air marshals on certain routes, modifying airline computer software to better identify passengers who could pose a security risk, and restricting access to parked aircraft and secure areas within airport terminals. Policymakers in Congress and the executive branch viewed those initiatives as necessary, but by no means sufficient, to ensuring public safety.

The disputes that now are occurring involve additional initiatives, and chief among those is how to handle the screening of airline passengers and baggage. Currently, airlines in the United States are responsible for such screening, and they rely on private-sector contractors to perform the function. Because the airlines are reluctant to take actions that would raise their costs or impede the flow of the two million passengers who move through busy terminals on a typical day, a consensus quickly emerged following the attacks that the airlines should no longer be responsible for screening passengers or for hiring private firms to do so for them.

That consensus brings the United States in line with most other nations. Of the 102 countries that have an international airport, only three — the United States, Canada, and Bermuda — have assigned responsibility for screening passengers to the airlines. In Israel and most Western European nations, the local airport authority is responsible for screening passengers and baggage. The national government sets extremely high compliance standards and closely monitors security procedures, but the airport authority is free to hire private contractors or to use airport employees to screen passengers.

The Bush administration called for greater federal oversight of airport security operations and more police presence at security checkpoints. But the administration wanted the discretion to use either federal employees or private firms to provide screening services, depending on the situation at a particular airport. The Senate, however, unanimously passed legislation (S.1447) that required screeners to be federal civil servants (except at the very smallest airports where local law enforcement personnel could be used). The senators argued that only this approach would ensure that all U.S. airports are safe. Meanwhile, the House of Representatives passed legislation (H.R.3150) in tune with the Bush proposal. House Republicans, who were the main proponents of the bill, argued that the Israeli-European security model works well, that establishing a federal screener work force of 28,000 would be costly and unnecessary, and that federal personnel practices would make it more difficult to introduce new management systems or deploy new technologies to screen passengers and baggage.

The House and Senate bills contained many of the same provisions — such as a $2.50 per passenger screening fee — but the House bill required the creation of a new agency within the Department of Transportation to supervise all airport security and screening services, perform employee background checks, develop standards for hiring and retaining screeners, and adopt procedures to test and train screeners. The House bill, moreover, would have granted Transportation officials the discretion to use federal employees to screen passengers at those airports where they believe it is necessary.

While House-Senate conferees were negotiating the airport security bill, several well-publicized lapses in airport security occurred, and the resulting pressure to federalize the screener workforce became overwhelming. Under a House-Senate agreement, within one year federal employees (under the control of the Department of Transportation) will become responsible for screening passengers at 423 airports. After three years, airports could switch to using private security companies for the work, but it is highly unlikely that many will do so, despite the implementation of a pilot program that will permit five airports to employ private companies (or local law-enforcement personnel) during the three-year transition period. Airlines will help defray the cost of the new security service up to the amount they previously paid to private security companies ($700 million to $1 billion), but airline passengers will be charged an additional $2.50 security fee for each flight (with a $5 maximum on one-way trips).

Whether the Transportation Department can hire, train, deploy, and supervise 28,000 new federal workers within one year is, of course, the crucial issue. But other transitional problems could also affect the change, including whether private screening companies and their employees will leave the industry before enough federal employees are available to replace them, and whether the screening companies are entitled to compensation because of the abrogation of their long-term contracts.

Smart technology Because it will now take more time to process and screen passengers, many observers speculate that, if air traffic returns to normal levels, most airports will be clogged perpetually. That, in turn, will make air travel more costly (including the value of travelers' time) and even less enjoyable.

Fortunately, some of that inconvenience may be diminished by the deployment of new "smart" technologies that would greatly enhance our ability to identify, track, and verify the identity of travelers and employees. Smart technologies, especially those that are based on biometric data (essentially, computer-assisted recognition of unique physical characteristics), could play a major role in the war against terrorism. Already, several major U.S. airports are considering deploying face-recognition technologies, thus allowing airport security personnel to scan large crowds for specific individuals.

Smart technologies could also be used as part of a volun-

tary "pre-screening" program for travelers. For instance, an individual who opts to participate in the program would receive a "smart travel card" containing background information and biometric information that would allow security personnel to verify the individual's identity easily, thus enabling her to bypass certain airport security procedures. Amsterdam's Schiphol International has a pilot program underway that is based on iris-recognition technology: A traveler who has opted to have an image of her iris stored in a computer and who has been prescreened by Dutch police, receives expedited processing through passport control once a picture of the iris is matched to the image on file. Such uses of technology would improve security and reduce travel delays.

RAILROADS

After September 11, rail freight shipments to metropolitan New York were suspended for two days for fear that terrorists could somehow use the rails in further attacks. In the days and weeks that followed, freight railroads strengthened their security systems. Much of the initial effort focused on ways to improve security for shipments of hazardous materials. But railroad managers also restricted access to critical facilities, stopped or rerouted freight operations in the vicinity of major public events, deployed personnel to ensure the security of their physical assets (bridges, tunnels, rail yards, dispatch centers, and other structures), examined their communications and control systems to ensure that existing security systems were adequate, and worked closely with the U.S. military and national security agencies to ensure prompt delivery of critical defense materials.

To offset the costs of those measures, railroads have sought — so far, unsuccessfully — federal aid. Sen. Ernest Hollings (D-S.C.) has proposed legislation (S.1550) that would grant the U.S. secretary of transportation the authority to develop a prioritized list of projects that should be undertaken to improve railroad security and to approve loans and loan guarantees for track rehabilitation and other purposes.

Amtrak Before September 11, Amtrak, the nation's provider of intercity passenger rail service, was facing serious financial problems. Moreover, it had made only minimal progress toward achieving the statutory goal of being free of federal operating subsidies by the end of fiscal year 2002 or else face liquidation. Amtrak operates a national 22,000-mile route network (all but 650 miles is over tracks owned by freight railroads), but only in the heavily traveled Boston-D.C. corridor (and a few niche markets) does intercity rail passenger service provide a viable competitive alternative to air and auto transportation for a significant number of travelers.

Following the attacks, Amtrak experienced a spike in demand for its services, a welcome event for almost any other business. Amtrak, noting the increase in demand, promptly requested $3.2 billion in additional federal aid to upgrade security and buy equipment to handle more passengers.

Whether there has been a large, permanent increase in the demand for intercity passenger rail service is uncertain, even in light of airport delays. Time will tell; but, if history is a guide, the initial surge in Amtrak's business may be short-lived, as such surges have been in the past when national or regional air service was disrupted or when gasoline prices soared. Nevertheless, Amtrak is likely to receive some federal aid, although not as much as was requested. More worrisome is the fact that, now, policymakers may be reluctant to force Amtrak to drastically restructure its operations or to push for more thorough-going market reforms such as privatizing intercity rail passenger operations.

MARINE TRANSPORTATION

Prior to the September 11 attacks, industry analysts had expressed concerns about the security of U.S. ports. Those concerns focused on preventing theft, drug smuggling, and illegal stowaways, not possible terrorist attacks against port facilities or cruise ships. Large seaports, by their nature, are located close to major population and transportation centers, are open and accessible, and are designed to process enormous volumes of freight traffic. Many seaports rely on private security guards and, until recently, some did not even bother to issue identification cards to port personnel, limit vehicle access to sensitive areas, or restrict individuals from carrying firearms.

Legislation has been drafted that would address those deficiencies. The proposed "Port and Maritime Security Act of 2001" (S.1214) would require 50 major U.S. seaports to assess their vulnerabilities and to develop security programs. The U.S. Coast Guard would play an even larger role than it does today in ensuring port security. Much of the regulatory focus of the bill is at the local level, and a relatively modest amount of federal aid is authorized for the buying of screening and detection equipment and the provision of loans or loan guarantees for security-related infrastructure improvements.

CONCLUSION

This article, of necessity, has reviewed only the "first order" effects of the September 11 attacks on certain transportation industries. (The motor carrier industry, for example, was not discussed, although tighter security at the Canadian and Mexican borders has delayed freight shipments and reduced equipment and labor productivity.) Even after September 11, Americans still enjoy unprecedented opportunities to travel and to engage in commerce.

However, to preserve efficiency and competition in the transportation sector, we must guard against those who would justify every new spending proposal, no matter how specious the argument, or any new federal regulation, no matter how much the costs outweigh the benefits, as necessary to stop terrorism. Our economy is under stress. Now is the time to require more stringent review of proposed regulations and new government programs. If not, the economic harm we inflict on ourselves may far exceed that which the attackers have inflicted upon us. R

The Transformation of Public Health

By J. Donald Millar, M.D.
Public Health Policy Advisory Board

Lest we forget, not all of the terrorist attacks launched against the United States last fall came on September 11. In the weeks following the airliner-turned-missile strikes on New York and Washington, a number of Americans became infected, some fatally, with anthrax that apparently was spread purposely by some malevolent agent. Whether that agent is associated with the terrorists of September 11 is unknown at the time of this writing. But what is known is that bioterrorism represents a new challenge for the U.S. public health system.

The U.S. public health system is unique in all the world. It is responsible for a number of remarkable accomplishments, including the elimination or near-elimination of several deadly diseases that ravaged the nineteenth century. But, as politicians and other public officials try to respond to the bioterrorism crisis, the system is in danger of undergoing a radical change in design and purpose that could make it ineffective in meeting its traditional obligations and new responsibilities.

U.S. PUBLIC HEALTH

The business of public health is the prevention of disease and injury, especially by "health protection" — protection from environmental hazards such as impure water, contaminated foods, and infectious or "quarantinable" diseases. In many nations, responsibility for the promotion of public health is vested in the national government. But in the United States, the Constitution does not grant any such duties to the federal government; those duties instead belong to the states.

They, in turn have developed state and local health departments that hold responsibilites relating to public health. Each health department is directed by a "health officer" who holds broad authority and, at his or her discretion, can perform acts (such as the mandatory quarantining of persons with contagious diseases) that are possible for no other U.S. government agent. It is in the pursuit of health protection that the broad and sometimes coercive powers of state and local health officers have been brought to bear.

Federal role In the U.S. public health system, the traditional role of the federal government has been to assist the state and local health departments with guidance, laboratory support, people, and money from the U.S. Public Health System (USPHS) to assure that national priorities are considered. When a public health problem could affect more than one state, the federal government has used such constitutional authority as "protecting interstate commerce" to take a more direct, active role.

However, in recent decades, Congress has mandated a number of large programs that have created major perturbations for the loose federalism originally characteristic of public health. For example, the Environmental Protection Agency (EPA) and the Occupational Safety and Health Administration (OSHA) gave the federal government vast new authorities to operate directly in the states and perform functions formerly reserved for state and local health departments. Huge federal programs of medical care and nutrition — Medicare for the elderly, Medicaid for the indigent, and W.I.C. for dependent women, infants, and children — have implications for health departments and have further blurred the lines of authority for the public's health.

However, in the area of disease control, the federal Centers for Disease Control and Prevention (CDC) have continued to respect the primacy of states. As an operating philosophy to this day, the CDC engages in epidemic investigations in a state

J. Donald Millar is vice chair and a distinguished fellow of the Public Health Policy Advisory Board. He is also president of Don Millar & Associates, a consulting firm dealing with occupational and environmental health. Millar is a former director of the National Institute for Occupational Safety and Health and has headed the National Center for Environmental Health, the Bureau of State Services, and the Smallpox Eradication Program at the Centers for Disease Control and Prevention.

THE ROLE OF ACUTE CARE: St. Vincents Hospital staff wait for victims of the WTC attacks.

PETER MORGAN/REUTERS

only on request of the state health officer.

Acute care In emergencies, health officers often exercise their "convener" role in the community to stimulate and coordinate the provision of emergency medical services by hospitals, clinics, and medical societies. However, acute medical care — especially acute emergency medicine — is far afield from the preventive function for which public health has unique expertise. Most public health physicians are not equipped by their day-to-day professional experience to provide acute clinical care. Appropriately, that is the work of clinical physicians in the medical community.

Acute medical care is more dramatic, more apparently heroic, and more glamorous than public health. What is more, it is natural for conscientious human beings to want to help people who are suffering. However, those realities do not alter the vital importance of public health; it is still true that "an ounce of prevention is worth a pound of cure." Hence, the diversion of public health professionals from prevention to acute medical care is, at best, a less-than-profitable investment, and the longer such a diversion persists, the greater the compounded loss.

MISSION, DISTORTED?

In its response to both September 11 and the anthrax bioterrorism that has followed, the federal government has altered the distribution of fundamental authorities and responsibilities in public health. Immediately after the airliner attacks, U.S. Department of Health and Human Services (HHS) Secretary Tommy Thompson ordered USPHS teams to Manhattan to provide acute care to the injured and support rescue workers. However, the USPHS, along with state and local public health officials, could not take the lead in handling the anthrax attacks — a role that better fits the agencies' traditional public health duties — because of Presidential Decision Directive 39. That directive, issued under the Clinton administration, designates the Federal Bureau of Investigations as the lead agency in the event of a biological or chemical attack on the United States, and charges the Federal Emergency Management Agency (FEMA) with ensuring adequate federal response to the consequences of terrorism.

In contrast to the 1976 outbreak of Legionnaires' disease that was managed by the local/state/CDC system, the FBI's handling of the anthrax attacks is not especially impressive. We are two months into the field investigations with no iden-

tification of an apparent source, and the federal agency has drawn sharp criticism from Congress over the lack of progress. But one should not expect the FBI to have the particular epidemiological skills required for the task. There is a profound difference between an epidemiological investigation aimed at identifying the source and preventing transmission of a disease, and a criminal investigation aimed at identifying, apprehending, and convicting a perpetrator. Is there a need for cooperation between the FBI and CDC? Of course. Is there a need for reassignment of lead responsibility for epidemiological investigations to the FBI? I think not.

More bureaucracy A further compromise of existing authorities is exemplified in Secretary Thompson's establishment of the new Office of Public Health Preparedness (OPHP). The office's stated purpose is to "coordinate national response to public health emergencies." One wonders what the OPHP can do that could not be done better by FEMA, which already exists and is well funded. Or, if there is need for better coordination between the agencies of the USPHS (CDC, National Institutes of Health, Food and Drug Administration, etc.), why could that not be done by the assistant secretary for health or the surgeon general? Each of those positions has the authority to convene the agency directors for any necessary clarification of roles and operational "ground rules." If there is "jawboning" to be done, why should it not be done within existing lines of authority? Why add a new "coordinating" bureaucracy to make more miserable the lives of agency directors already distracted by the challenges of dealing with bioterrorism and the accompanying media circus?

Congress is considering further compromising HHS authorities by establishing a new position: assistant secretary for emergency preparedness. In so doing, Congress would take that responsibility away from the Public Health Service. The new assistant secretary would leave the assistant secretary for health with a diminished portfolio and alter agency priorities to favor emergency preparedness instead of traditional public health efforts to prevent disease and promote health.

Compromised credibility The bioterrorism has provoked round-the-clock media coverage that has heightened public fears. Those fears have not been allayed by public health officials' seeming inability to answer, in timely fashion, such important questions as, "Is this bioterrorism or not?" "If this is bioterrorism, how did it happen?" and, "What do these environmental tests mean?" Citizens' expectations that public health experts could speak confidently on such issues are reasonable. But, because those experts lacked necessary preparedness, each new finding of an anthrax spore fed the media frenzy and increased public worries.

In truth, there has been much less to fear than what the public may believe. As weapons go, anthrax seems a bit under-whelming: The number of cases generated by the attacks is, at the time of this writing, less than one week's worth of deaths from occupational injuries. Compared to the effects of an influenza epidemic, the anthrax bioterrorism seems almost trivial. Unfortunately, public health officials failed to communicate that message effectively to the media and the public.

> There is a profound difference between an epidemiological investigation aimed at identifying and halting a disease and a criminal investigation aimed at capturing a perpetrator.

MORE POWERFUL WEAPONS

Recognition of the comparatively small number of anthrax cases generated by the bioterrorism attacks may ease public worry, but there still is great fear about future attacks using more potent weapons. Stirred by media reports about the federal government's "Dark Winter" hypothetical doomsday model, the public has given tremendous support to the creation of new offices and the spending of vast sums of tax dollars to counter such threats.

The gravest fears involve smallpox, and they are not without warrant: If terrorists were to use the *variola major* strain of the virus, which once racked the Indian subcontinent, 40 percent of the people who are infected would die. But if the federal government, through the CIA, military intelligence, and the State Department, has convincing evidence that terrorists possess weaponized smallpox, it has not been revealed to the public.

Stockpiling vaccine However, the federal government is acting as though that threat is real, and is spending the kind of money justified only if it were. The antiterrorism bill moving through Congress at the time of this writing includes some $2 billion in new spending to buttress public health programs, including hundreds of millions for the purchase of smallpox vaccine. (The new purchases would add to the 15 million doses the government already has stockpiled, and the 40 million doses ordered by the CDC in 2000.)

However, the plan calls for no availability of that vaccine to the public until there is a confirmed smallpox outbreak. That is, the federal government — which is the sole owner of a highly effective preventive measure — will sit on its stockpile until several Americans actually become victims of smallpox. The idea that the government would withhold the only effective means of protecting the population from a terrible disease until an epidemic is confirmed is new to public heath. Prevention, in this new context, obvious-

ly has no meaning for the "sentinel" Americans who will become ill and die of smallpox as trigger for the government's response. Truth is, this is not prevention and not public health as we have known it before.

The stated reason for withholding the vaccine is potential side effects, especially for persons with HIV/AIDS. According to Surgeon General Dr. David Satcher, "You're always hesitant to immunize people against the disease unless there is going to be a risk." That quote presents a significant contrast to the traditional "ounce of prevention" public health philosophy. To see that contrast more clearly, consider the statement made several years ago by former CDC director Dr. David J. Sencer, who headed the agency when it spearheaded the World Health Organization's global smallpox eradication program: "Stockpiling antibodies in the body is preferable to stockpiling vaccines on warehouse shelves."

Last year, when all bioterrorism was still hypothetical, the Public Health Policy Advisory Board examined the smallpox vaccine availability issue. The board suggested the option of making the vaccine available as it is produced, informing the public of the risks and benefits, and allowing individuals to decide whether or not to avail themselves of the protection. For those of us not infected with HIV, the risks of vaccination are known and negligible when compared to smallpox.

Cost Major financial resources are being committed to combat the anthrax bioterrorism and the threat of smallpox attack. Because resources for public health are always limited, there is no "fat" in public health budgets. One wonders, which ordinary public health functions are being sacrificed in order to pay for the bioterrorism measures? As yet, nobody's talking about such tradeoffs, but rest assured, loss is being incurred in public health as Congress fixates on bioterrorism, real or imagined. One can only hope that the phantoms we now chase are worth the losses suffered by public health, or, that the phantoms will soon disappear.

THE NEED FOR PROFESSIONAL LEADERSHIP

Potentially, the worst consequence of September 11 for U.S. public health would be reduced visibility of its national professional leadership. A lot of public health functions are non-regulatory and non-coercive, and depend on broad acceptance by the public of measures for which the value is not immediately obvious. Effective, persuasive professional leadership of the kind exhibited by President Reagan's surgeon general, C. Everett Koop, is critical to success.

The most prominent national governmental voice in the current crisis has been that of HHS Secretary Thompson, the former governor of Wisconsin. Secretary Thompson is well known for his expertise in reform of state welfare programs, but to my knowledge he does not possess extraordinary experience in public health, and these are extraordinary times for public health. In turn, the public has seen and heard less than it should have from the assistant secretary for health, the surgeon general, and the directors of the public health service agencies.

In addressing the felt need for "preparedness," Secretary Thompson had an opportunity to strengthen the leadership capacity of the talented professionals who work for his department. Existing units within HHS could have been organized to meet the challenges of the bioterrorism crisis, but he chose to create the Office of Public Health Preparedness and look outside of government for an appointee to run it. Rather than create new bureaucratic structures and bring in outside hires, I believe much would have been gained from leaning on and learning from professionals already in place inside HHS. Not to do so diminishes the stature of public health professionals and threatens the effectiveness of public health leadership in the future.

CONCLUSION

While "an ounce of prevention…" is an accurate truism, the work of public health under ordinary circumstance is largely prosaic. When prevention is at its best, calamities are not happening and the public and the media are not stimulated. Those of us who directed the smallpox eradication campaigns were puzzled by America's reaction (or lack thereof) to that enormous achievement. Smallpox eradication was without precedent in human history, yet the public remained blasé and no leaders in that successful "war" became Nobel laureates. The same might be said of other major triumphs of prevention — pure water supplies, reduced infant and maternal mortality, increased longevity, improved quality of life — all of which are attributable almost entirely to prevention. Prevention is not glamorous, but it is powerful and important.

Our society benefits greatly from an effective public health system and should be interested in the events that affect public health for good or bad. September 11 and its aftermath were major events that have affected public health. Some of those effects already are visible, others will become manifest later. Some are transient; others will persist from here on. Some offer opportunities to better understand the importance of prevention. Others, ominously, threaten the ability of public health to achieve important goals in the future.

Public health is too valuable to this society to be abandoned to a fate dictated by media-driven fear and the idiosyncrasies of shallow thought. Much that has happened to public health in the last three months, and much that is being pushed in Congress today, is ill advised and unnecessary, and potentially hazardous to the future of public health. We have cause to fear that public health could become one of the victims of September 11. R

The Defensive Front Line

By Joseph D. McNamara
Hoover Institution

September 11 was not the first time that terrorists struck targets within the United States. Only eight years before, a band of Islamic extremists led by Ramzi Yousef successfully detonated a minibus filled with 1,100 lbs. of explosives in the parking garage of the same World Trade Center. Three years before that, associates of drug kingpin Pablo Escobar firebombed a Drug Enforcement Administration office in Fort Myers, Florida. Before he was apprehended in 1996, Unabomber Ted Kaczynski killed three people and injured 23 over a 17-year period. And in 1995, Timothy McVeigh killed 168 people when he detonated a massive bomb just outside the Alfred R. Murrah Federal Office Building in Oklahoma City.

America responded to those attacks through law enforcement agencies and the legal system: Yousef, the Escobar associates, Kaczynski, and McVeigh were arrested, tried, and convicted of felony crimes. In marked contrast, the magnitude and international origin of the September 11 attacks have led President Bush and other U.S. leaders to label the events as acts of war. America properly responded with military force.

It would be a travesty of our legal system to regard the slaughter of thousands of our people as anything but a declaration of war against the United States. After all, the fundamental duty of government is to protect the life, property, and liberty of its citizens. But, despite the crucial role of the military, law enforcement agencies and other civilian emergency services still have key responsibilities in the fight against terrorism: to identify terrorist perpetrators, to respond to the tragedies that do occur, and to assist in security and target-hardening measures. Unfortunately, history offers little insight into the sacrifices, responsibilities, and challenges that this new war will impose upon citizens and their federal and local governments.

Joseph D. McNamara is a research fellow in criminal justice at the Hoover Institution. He is a retired police chief of San Jose, Calif., and a former police chief of Kansas City, Mo. McNamara also once served as director of crime analysis for the New York Police Department, working out of an office near the World Trade Center.

TURF BATTLES

There are only about 11,500 FBI agents in the United States, as compared to approximately 650,000 state and local police officers and probably an equal number of local firefighters and public health workers. Because of those numbers and their deployment, local and state law enforcement and emergency services providers will be the first on the scene of any tragedy, including a terrorist strike inside the United States.

Just because these are, in a federally coined phrase, the "first responders to a terrorist attack" does not mean that federal workers and troops later take over operations. It is local personnel who stay with catastrophes — including attacks — from beginning to end. Obviously, the federal government can offer invaluable technical assistance in examining explosions, providing analyses and responses for biological or chemical weapons attacks, and (most importantly) sharing intelligence information when possible. But it is the local police, firefighters, physicians, and paramedics who will fight the defensive battles in the new war on terrorism. That fact produces far different policy challenges than we are prepared for under superficial "first responder" paradigms.

Need to know The term "homeland security" conveys an empty promise: Given the nature of our free, open society that enjoys a $30 trillion world economy, not all terrorist plots can be discovered ahead of time and prevented. Domestically, law enforcement agencies and the courts can work against terrorism by countering the next Kaczynski or McVeigh through preventive measures, enforcement of criminal laws, and punishment. But the more serious threats come from state-supported terrorist networks. And though the U.S. military can score decisive victories against those networks by eliminating terrorist bases abroad and

THE DEFENSIVE FRONT LINE: NYPD officers patrol the reopening of the New York Stock Exchange.

AMY SANCETTA/AP

demonstrating to other governments that they will not be allowed to harbor such groups, foreign-spawned terrorists will continue to pose threats. To counter them, local officials must learn of plots that are underway, depending almost entirely on federal intelligence sources.

Unfortunately, such intelligence sharing is impeded by turf battles between federal, state, and local levels of government. And at the moment, there are great tensions among those agencies. A number of police chiefs complain that Attorney General John Ashcroft, by continuously placing local law enforcement on "the highest level of alert," has overwhelmed their systems, exhausted their cops, and busted their budgets without providing any specific threat information to which they can respond.

The feds, however, have reason to gripe about local and state officials, as shown by the Gray Davis "bridge-watch" fiasco. In early November, the FBI sent out a low-priority interstate information notice to local officials that bridges in eight western states might be targets of terrorists. It was one of hundreds of threats, all of which seemed to be false, but the FBI, perhaps stung by post-September 11 charges of not sharing information, decided to err on the side of caution and report the threat to local agencies.

FBI agents subsequently were dismayed when California Governor Gray Davis called a national press conference to announce the threat and declare that he was assigning National Guard personnel and California Highway Patrol officers to guard four suspension bridges in the state. Interestingly, the governor made no recommendation to motorists to avoid the bridges or stay home from work. At no time were the bridges closed, nor was it ever clear what were the duties of the National Guard and extra police. But Davis, a potential Democratic presidential candidate in 2004, received national television coverage and his picture even appeared on the front page of the *New York Times.* (None of the governors of the other seven states commented on the low-credibility warning.) Although the FBI quickly announced that the threat was not credible and cancelled the bridge alert, a degree of public panic followed. The terrorists had scored one for their side, while tensions increased between federal and local agencies over the sharing of information.

It is a basic rule of intelligence gathering that information is shared only on a "need to know" basis. Public announcements can warn the enemy that their communi-

cations systems and codes have been penetrated. In some cases, the individuals who provide us with valuable information can lose their lives. Consequently, it is imperative that information be made public only when necessary to warn people of danger and to save lives.

REASSESSING PRIORITIES

As Secretary of State Colin Powell has indicated, an attack of the magnitude of September 11 involved a long period of planning, communication, and coordination. Secretary Powell conceded, "We [top officials] did not get the cueing we needed." But as former FBI and CIA chief William Webster has argued, "It probably is not the case that we did not have enough information, but that we had too much." Our extensive intelligence systems missed the indicators that surfaced about the impending attack.

The coming critique of government intelligence agencies should not be an exercise in scapegoating in the name of holding people accountable for human error, except in the unlikely event that the failure was due to a traitor in our midst, or incompetence so great that it requires dismissal. Fact-finding to prevent future disasters is much better accomplished when those questioned are not inappropriately threatened as part of political grandstanding. Such career threats have a way of producing remarkably negative consequences. After all, some months ago, Congress held hearings on the airline industry during which lawmakers railed against late arrivals and canceled flights, but hardly mentioned security. Congressional pressure led airlines to expedite baggage check-in and other airport functions, all of which had a negative effect on security.

Foreign aid Another area that is in need of review encompasses the activities of the State Department, itself. We have long criticized the Taliban extremists controlling Afghanistan for harboring Osama bin Laden and implicitly approving of his terrorist network. So why did Secretary Powell, last May, issue a press release announcing a package of $43 million in new humanitarian aid for Afghanistan? And why did the Clinton administration designate $114 million in aid for Afghanistan last year?

Powell, in the press release, claimed that the aid would lead the Taliban to halt their support for terrorism, and would reward their promise to ban poppy cultivation. But they clearly continued to back bin Laden, and stockpiled tons of opium. Ironically, humanitarian aid to the Taliban, which likely engendered Afghani support for their government, not ours, and the many millions of dollars they made selling opium at highly inflated prices on the black market, no doubt helped to finance the September 11 attacks and other terrorist acts against us. It is noteworthy that our new allies, the Northern Alliance, also profit from the illegal opium trade.

The wrong war On the same note, we should mark the irony that, on September 11, Powell was in Peru, trying to overcome the resistance of surrounding countries to our contribution of almost a billion dollars in aid to Colombia to wage war against cocaine producers. The countries surrounding Colombia rightfully complained, without success, that this "Plan Colombia" aid is pressuring drug producers and their private armies to move into adjacent nations, destabilizing the area to the point where the United States may be drawn into a Vietnam-like quagmire of insurrections, and creating new anti-American terrorist groups.

The war against terrorism requires a reassessment of law enforcement and security priorities, especially in regard to the resources we now expend in the "war on drugs." In budget requests made four months prior to the September 11 attacks, the FBI asked for only eight additional agents to combat terrorism — a meager increase that follows the agency's paltry two-percent manpower growth over the past two years. The Drug Enforcement Agency, on the other hand, has enjoyed a 26-percent increase in personnel. It is worth pondering whether the September 11 attacks would have occurred if Congress had increased FBI anti-terrorism resources by 26 percent, instead of DEA resources.

Drug war expenditures are not yielding many returns. The National Academy of Science recently released a report on a study requested by the Clinton administration on the effectiveness of America's anti-drug efforts. The report noted that some $30 billion were spent on the drug war last year alone, twice the amount spent on "Desert Storm," but no reliable data exist to enable a judgment of the success of anti-drug efforts.

IN HONOR OF HEROES

My dad, my brother, cousins, uncles, and I all once carried badges of the New York Police Department, and our collective service to that agency totals more than 150 years. We were not unlike the cops, firefighters, and paramedics who ran past fleeing crowds into the burning World Trade Center at the cost of their lives. Just as President Bush now carries the badge of Port Authority police officer George Howard who was killed in the Trade Center attack, I have begun carrying my old NYPD shield as a reminder of the service of those heroes.

The professionals in public safety and our armed forces, along with ordinary citizens who refuse to be intimidated and who turn out in the millions at sporting and other events to sing the national anthem and wave flags, are the real America, the one that the terrorists never saw, but have now awakened. Those Americans are willing to risk their lives rather than surrender to terror. For their sake, we must ensure that bureaucratic blundering and turf battles do not detract from our implacable determination to destroy the enemy who attacked us. A deeper patriotism means that we should unite and not expend our resources on a drug war that we cannot win. Instead, we must marshal our energies for a war that we can, and must, win: the war against terrorism. R