Catastrophic Terrorism:

Elements of a National Policy

By

Ashton B. Carter, John M. Deutch

and Philip D. Zelikow

A Report of

Visions of Governance for the Twenty-First Century

A Project of the John F. Kennedy School of Government

Harvard University

This report was made possible in part by the Carnegie Corporation of New York, the John D. and Catherine T. MacArthur Foundation, and the Herbert S. Winokur Public Policy Fund at Harvard University. The statements made and views expressed are solely the responsibility of the authors.

Contents

Foreword: Preventive Defense

Through more than four decades of Cold War, American national security strategy was difficult to implement but easy to understand. America was set on a clear course to contain Soviet expansionism anywhere in the world, all the while building a formidable arsenal of nuclear weapons to deter the Soviet Union from using military force against it or its allies. Now, with the end of the Cold War, the underlying rationale for that strategy—the threat from the Soviet Union—has disappeared. What strategy should replace it? Much depends on finding the correct answer to this question.

The world survived three global wars this century. The first two resulted in tens of millions of deaths, but the third—the Cold War—would have been even more horrible than the others had deterrence failed. These three wars trace a path that leads to the strategy needed for the post-Cold War era.

At the end of the First World War, the victorious European allies sought revenge and reparations; what they got was a massive depression and another world war. The United States sought "normalcy" and isolation; what it got was total war and leadership in winning it. Because it failed to *prevent* and then to *deter* Germany's aggression, America was forced to mobilize a second time to *defeat* it.

At the end of the Second World War, America initially chose a strategy based on prevention. Vowing not to repeat the mistakes made after World War I, the Truman administration created the Marshall Plan, which sought to assist the devastated nations of Europe, friends and foes alike, to rebuild. The Marshall Plan and other examples of the preventive defense strategy, aimed at preventing the conditions that would lead to a future world war, were an outstanding success in Western Europe and in Japan.

But the Soviet Union turned down the Marshall Plan and, instead, persisted in a program of expansion, trying to take advantage of the weakened condition of most of the countries of Europe. The resulting security problem was clearly articulated by George Kennan, who forecast that the wartime cooperation with the Soviet Union would be replaced with a struggle for the heart of Europe and that the United States should prepare for a protracted period of confrontation. Kennan's analysis was accepted by the Truman administration, which then formulated a strategy that would get us through the Cold War: deterring another global war while containing the Soviet Union's demonstrated expansionist ambitions. Deterrence supplanted prevention: there was no other choice.

Even deterrence was a departure from earlier American military strategy. The United States had twice previously risen to defeat aggression, but it had not maintained the peacetime military establishment or the engagement in the world to deter World Wars I or II. Marshall and other defense leaders around Truman created the peacetime posture and new security institutions required. In time, as George Kennan had forecast, the Soviet Union disintegrated because of the limitations of its political and economic systems. Deterrence worked.

The result is a world today seemingly without a major threat to the United States, and the U.S. is now enjoying a period of peace and influence as never before. But while this situation is to be savored by the public, foreign policy and defense leaders should not be complacent. This period of an absence of threat challenges these leaders to find the vision and

foresight to act strategically, even when events and imminent threats do not compel them to do so.

To understand the dangers and opportunities that will define our nation's strategy in the new era, we must see the post-Cold War world the way George Marshall looked upon Europe after World War II, and return to prevention. In essence, we now have another chance to realize Marshall's vision: a world not of threats to be deterred, but a world united in peace, freedom, and prosperity. To realize this vision, we should return to Marshall's strategy of preventive defense.

Preventive Defense is a concept of defense strategy for the United States in the post-Cold War Era. It stresses the need to anticipate security dangers which, if mismanaged, have the potential to re-create Cold War-scale threats to U.S. interests and survival. The foci of Preventive Defense are: proliferation of weapons of mass destruction, catastrophic terrorism, "loose nukes" and other military technology from the former Soviet Union, Russia's post-Cold War security identity, and the peaceful rise of China.

Preventive Defense is the most important mission of national security leaders and of the defense establishment. They must dedicate themselves to Preventive Defense while they deter lesser but existing threats—in Iraq and North Korea—and conduct peacekeeping and humanitarian missions—in Bosnia, Haiti, Rwanda, and so on—where aggression occurs but where American vital interests are not directly threatened.

This report is the sixth in a series of Preventive Defense Project reports on key applications of Preventive Defense. We are grateful to our colleagues in the Catastrophic Terrorism Study Group and the Visions of Governance for the Twenty-First Century for their collaboration

Acknowledgments

This report is a product of the Catastrophic Terrorism Study Group, a nine-month long collaboration of faculty from Harvard University, the Massachusetts Institute of Technology, Stanford University, and the University of Virginia. The Group involves experts on national security, terrorism, intelligence, law enforcement, constitutional law, technologies of Catastrophic Terrorism and defenses against them, and government organization and management. The Group is co-chaired by Ashton B. Carter and John M. Deutch, and the project director is Philip D. Zelikow. Organized by the Stanford-Harvard Preventive Defense Project, the work of the Study Group is part of the Kennedy School of Government's "Visions of Governance for the Twenty-First Century" project, directed by Dean Joseph S. Nye, Jr. and Elaine Kamarck.

While the danger of Catastrophic Terrorism is new and grave, there is much that the United States can do to prevent it and to mitigate its consequences if it occurs. The objective of the Catastrophic Terrorism Study Group is to suggest program and policy changes that can be taken by the United States government in the near term, including the reallocation of agency responsibilities, to prepare the nation better for the emerging threat of Catastrophic Terrorism.

An article based on this report will be published in the journal *Foreign Affairs* in the November/December 1998 issue.

The authors would like to thank the members of the Catastrophic Terrorism Study Group:

Graham T. Allison, Jr.

Zoe Baird

Vic DeMarines

Robert Gates

Jamie Gorelick

Robert Hermann

Philip Heyman

Fred Ikle

Elaine Kamarck

Ernest May

Matthew Meselson

Joseph S. Nye, Jr.

William J. Perry

Larry Potts

Fred Schauer

J. Terry Scott

Jack Sheehan

Malcom Sparrow

Herbert Winokur

Robert Zoellick

Though practically all of these group members are sympathetic to the conclusions in this report, and some enthusiastically endorse them, none is responsible either for particular opinions expressed here or for the way we have written this report and expressed those judgments.

We would also like to thank the staff who was responsible for organizing the Study Group in addition to assisting in the preparation of this report: Gretchen Bartlett, Lainie Dillon, Hilary Driscoll, Sarah Peterson, and Kristin Schneeman.

Finally, the Study Group is grateful for the support of the Carnegie Corporation of New York, the John D. and Catherine T. MacArthur Foundation, and the Herbert S. Winokur Public Policy Fund at Harvard University.

CATASTROPHIC TERRORISM: ELEMENTS OF A NATIONAL POLICY

Imagining the Transforming Event

We find terrorism when individuals or groups, rather than governments, seek to attain their objectives by means of the terror induced by violent attacks upon civilians. When governments openly attack others, we call it war, to be judged or dealt with according to the laws of war. When governments act in concert with private individuals or groups, the United States government may call it war, or state-sponsored terrorism, and retaliate against both the individuals and the governments. Whatever the label, terrorism is not a new phenomenon in national or international life, although terrorists may be animated by a greater variety of motives than ever before, from international cults like Aum Shinrikyo to the individual nihilism of the Unabomber.

What is certainly new is that terrorists may today gain access to weapons of mass destruction (WMD). These can come in a variety of forms: nuclear explosive devices, germ dispensers, poison gas weapons, or even the novel destructive power of

computers turned against the societies that rely on them. What is also new is an unprecedented level of national and global interdependence on an invisible infrastructure of energy and information distribution.

Americans were shocked by the tragic results of the August 1998 terrorist attacks against their embassies in Kenya and Tanzania. By comparison with the threat of catastrophic terrorism, we believe that the threat of ordinary terrorism of the kind we have known over the last generation is being taken seriously. The United States government's commitment to address that danger is fundamentally sound. We are not as confident that the United States government is suitably prepared to address the new threat of catastrophic terrorism that utilizes weapons of mass destruction or intensive cyber-assault.

Long part of Hollywood's and Tom Clancy's repertory of nightmarish scenarios, catastrophic terrorism is a real possibility. In theory, the enemies of the United States have motive, means, and opportunity. The U.S. government has publicly announced that terrorist groups are attempting to manufacture chemical weapons and destroyed one such facility operating in the Sudan. As India and Pakistan build up their nuclear arsenals and Russia, storehouse for tens of thousands of weapons and the material to make tens of thousands more, descends toward a future none can foresee, it is not hard to imagine the possibilities. The combination of available technology and lethality has made biological weapons at least as deadly a danger as the better known chemical and nuclear threats. The bombings in East Africa killed hundreds. A successful attack with weapons of mass destruction could certainly kill thousands, or tens of thousands. If the device that exploded in 1993 under the World Trade Center had been nuclear, or the distribution of a deadly pathogen, the chaos and devastation would have gone far beyond our meager ability to describe it.[1]

Experts combining experience in every quadrant of the national security and law enforcement community all consider this catastrophic threat perfectly plausible *today*. Technology is more accessible, society is more vulnerable, and much more elaborate international networks have developed among organized criminals, drug traffickers, arms dealers, and money launderers: the necessary infrastructure for catastrophic terrorism. Practically unchallengeable American military superiority on the conventional battlefield pushes this country's enemies toward the unconventional alternatives.[2]

Readers should imagine the possibilities for themselves, because the most serious constraint on current policy is lack of imagination. An act of catastrophic terrorism that killed thousands or tens of thousands of people and/or disrupted the necessities of life for hundreds of thousands, or even millions, would be a watershed event in America's history. It could involve loss of life and property unprecedented for peacetime and undermine Americans' fundamental sense of security within their own borders in a manner akin to the 1949 Soviet atomic bomb test, or perhaps even worse. Constitutional liberties would be challenged as the United States sought to protect itself from further attacks by pressing against allowable limits in surveillance of citizens, detention of suspects, and the use of deadly force. More violence would follow, either as other terrorists seek to imitate this great "success" or as the United States strikes out at those considered responsible. Like Pearl Harbor, such an event would divide our past and future into a "before" and "after." The effort and resources we devote to averting or containing this threat now, in the "before" period, will seem woeful, even pathetic, when compared to what will happen "after." Our leaders will be judged negligent for not addressing catastrophic terrorism more urgently.

Using imagination, we hope now to find some of the political will that we know would be there later, "after," because this nation prefers prevention to funereal reconstruction. When this threat becomes clear the President must be in a position to activate extraordinary capabilities. The danger of the use of a weapon of mass destruction against the United States or one of its allies is greater at this moment than it was during the Cold War, or at least since 1962. The threat of catastrophic terrorism is therefore a priority national security problem, as well as a major law enforcement concern. The threat thus deserves the kind of attention we now devote to threats of military nuclear attack or of regional aggression, as in the Defense Department's major regional contingencies that drive our force planning and the resources we devote to defense.

The first enemy of imagination is resignation. Some who contemplate this threat find the prospects so dreadful and various that they despair of doing anything useful and switch off their troubling imagination. They are fatalistic, like someone contemplating the possibility of a solar supernova, and turn their eyes away from the threat. Some thinkers reacted the same way at the dawn of the nuclear age, expecting doom to strike at any hour and disavowing any further interest in the details of deterrence as a hopeless venture. But as in the case of nuclear deterrence, the good news is that more *can* be done.

We formed a *Catastrophic Terrorism Study Group* to move beyond a realization of the threat to consider just what can be done about it. This group began meeting in November 1997. We examined other studies that consider this problem. We received information and advice from some current government officials as well as from those who had considered the problem

from the perspectives of governments in Great Britain, Israel, Germany, and Russia. We now advance *practical* proposals for consideration and debate. We avoid a grand solution, preferring to shape "bricks" that strengthen existing structures, consider the very different technical challenges presented by nuclear, biological, chemical, and cyber threats, and provide a foundation for future adaptation and future building.

Organizing for Success

The threat of catastrophic terrorism typifies the new sort of security problem the United States must confront in the post Cold War world. It is transnational, defying ready classification as foreign or domestic, either in origin, participants, or materials. As the World Trade Center incident demonstrated, one group can combine U.S. citizens with resident aliens and foreign nationals, operating in and out of American territory over long periods of time.

The greatest danger may arise if the threat falls into one of the crevasses in our government's field of overlapping jurisdictions, such as the divide between terrorism that is "foreign" or "domestic;" or terrorism that has "state" or "non-state" sponsors; or terrorism that is classified as a problem for "law enforcement" or one of "national security." The law enforcement/national security divide is especially significant, carved deeply into the topography of American government.

The national security paradigm fosters aggressive, proactive intelligence gathering, presuming the threat before it arises, planning preventive action against suspected targets, and taking anticipatory action. The law enforcement paradigm fosters reactions to information voluntarily provided, post-facto arrests, trials governed by rules of evidence, and general protection for the rights of citizens.

We start with a concept for an overall end-to-end strategy. This has at least four elements: (1) intelligence and warning; (2) prevention and deterrence; (3) crisis and consequence management; and (4) a process for coordinated acquisition of needed materials, equipment, and technology. Throughout, there must be clear guidance about what our institutions should be able to do and definition of the roles and missions of involved agencies at all levels of government.

In an address at the U.S. Naval Academy, President Clinton announced on May 22, 1998, that we must approach the new terrorist challenges of the 21st century "with the same rigor and determination we applied to the toughest security challenges of this century." To that end he signed Presidential Decision Directive (PDD) 62 and appointed a National Coordinator for Security, Infrastructure Protection, and Counterterrorism to "bring the full force of all our resources to bear swiftly and effectively." The National Coordinator and PDD-62, like the predecessor PDD-39, look to "lead agencies" on one or another issue to "identify a program plan with goals and specific milestones." The National Coordinator will produce an annual "Security Preparedness Report," offer budget advice, and lead in the development of guidelines for crisis management.[3]

We welcome the presidential determination to address the danger of catastrophic terrorism and see no harm in the designation of a responsible White House aide. But we suggest a different emphasis when it comes to solving the difficult problems of shared powers and overlapping authorities.

We place no faith in czars. An unidentified, incautious administration official explained to reporters that "when money was going to the war on drugs, we created a drug czar. Now money is going to counterterrorism, and so we'll have a czar for that, except this one will have real power."[4] A national coordinator may be necessary, but is certainly not sufficient. For better or worse, however, "real power" resides in the executive departments and companies that actually have people, equipment, money, and the capacity to do things. This report thus focuses on building such capabilities, rather than dwelling on coordination at the apex.

"In form," Richard Neustadt explained long ago, "all Presidents are leaders nowadays. In fact this guarantees no more than that they will be clerks. Everybody now expects the man inside the White House to do something about everything. ... But such acceptance ... merely signifies that other men have found it practically impossible to do their jobs without assurance of initiatives from him. ... They find his actions useful in their business. ... A President, these days, is an invaluable clerk. His services are in demand all over Washington. His influence, however, is a very different matter."[5]

Well before the idea of a terrorism czar had been conceived, James Q. Wilson had noticed that "whenever a political crisis draws attention to the fact that authority in our government is widely shared, the cry is heard for a 'czar' to 'knock heads together' and 'lead' the assault on AIDS, drug abuse, pollution, or defense procurement abuses. Our form of government, to say nothing of our political culture, does not lend itself to czars...."[6]

Also, most of the expensive functional capabilities that must be brought together to cope with the danger of catastrophic terrorism are capabilities that are needed for other purposes, too, from reconnaissance satellites to National Guardsmen. Unifying these capabilities exclusively for one challenge will not work in practice. The people making decisions about using these capabilities against terrorists should be the same people who must consider the other missions and who can weigh and reconcile competing demands.

Experience from World War II (such as that of the British Chiefs of Staff Committee or the U.S. Office of War Mobilization) through the Cold War to the present, including the current system of security policymaking the British have devised (after long trial and error) for Northern Ireland, instead counsels us toward a different approach.[7] One or another executive agency may be in the lead, but the key is to give responsibility (and accountability) to the people who are in charge of the relevant people and machines; create unglamorous but effective systems for shared decision-making that combine civil, military, and intelligence judgments up and down the chain of command; fashion entities that integrate planning and operational activity at the working level; and focus on the tasks of building up the institutional capacities to do new things. There must be exercises of the entire system to highlight defensive needs, before an incident happens. We turn now to the first crucial task: intelligence and warning.

Intelligence and Warning

Since 1945 the United States has given intense attention to any potentially hostile entity that might deliver weapons of mass destruction against its territory or its allies. The intelligence objectives were straightforward: orientation toward governments and monitoring of weapons development, testing, and deployment. The intelligence task for catastrophic terrorism is complicated by non-state actors, concealed weapons development, and unconventional deployments. In cyber attacks, the delivery of weapons can be entirely electronic.

So the intelligence job is much harder. It is not impossible. The would-be terrorists have problems, too. If states are involved, the organizations tend either to be large and leaky, or small and feckless. If no state is involved, the group may be small, feckless, and pathological, too. These realities form the opportunities for intelligence successes. Even the most formidable Irish terrorist groups took years of experience to acquire their level of professionalism and, for all their skills and training, suffered frequent setbacks in their underground war against British intelligence. Perhaps the most serious recent attempt to carry out an act of catastrophic terrorism was an expertly planned effort to destroy, with a series of simultaneous bomb explosions, the entire electrical power supply for metropolitan London. The attempt was thwarted and British security forces arrested the terrorists.

The U.S. government should seek to have the legal authorities and the capability to monitor—physically and electronically—*any* group and their potential state sponsors that *might* justifiably be considered to have a motive and capability to use weapons of mass destruction. The U.S. government should be able to do all that can reasonably be done to detect any use or deployment of such weapons anywhere in the world, by utilizing remote sensing technology and by strengthening and evaluating worldwide sources of information. These would include clandestine collection, open sources such as foreign newspapers and journals or the Internet, and would include better-organized exchanges with key allies and other like-minded states.

Nearly a year before its attack on the Tokyo subway system, the Aum Shinrikyo group had already used the nerve gas, Sarin, in attacks on civilians. Although known to the Japanese news media, the U.S. government did not know. Not only did Washington not know what Japanese law enforcement agencies knew, it is likely that centralized Japanese law enforcement agencies did not know what other local organizations in Japan knew about this prior and well documented use of chemical weapons.

Today the U.S. intelligence community lacks a place to perform "all-source" planning for collecting information, where the

possible yields from efforts in overhead reconnaissance, electronic surveillance, clandestine agents, law enforcement databases and informants, and reports from foreign governments, can be sifted and organized for maximum complementary effect. The national security agencies can be proactive. Domestic law enforcement officials understandably are not proactive about intelligence collection but focus their efforts from informants or other collection to investigate suspected criminal actions with the objective of criminal prosecution. Civil liberties properly discourage them from going out and looking for criminals before they have evidence of crime.

On the other hand, domestic law enforcement has many techniques for gathering data, including lawful wiretaps and grand jury investigations. Much of the yield from these efforts is, in turn, closed off to the national security community by law or regulation, to safeguard constitutional rights.[8]

We believe the U.S. needs a new institution to gather intelligence on terrorism, with particular attention to the threat of catastrophic terrorism. We call this new institution a *National Terrorism Intelligence Center*. This Center would be responsible for collection management, analysis, dissemination of information, and warning of suspected catastrophic terrorist acts. The Center would need the statutory authority to:

- monitor and provide warning of terrorist threats to relevant agencies of the U.S. government, supporting defense or intelligence operations, as well as law enforcement;

- set integrated collection requirements for gathering information for all the intelligence agencies or bureaus of the U.S. government;

- receive and store all lawfully collected, relevant information from any government agency, including law enforcement wiretaps and grand jury information;

- analyze all forms of relevant information to produce integrated reports that could be disseminated to any agency that needed them, while restricting dissemination of underlying domestic wiretap and grand jury information;

- review planned collection and intelligence programs of all agencies directed toward terrorist targets to determine the adequacy and balance among these efforts in preparation of the President's proposed budget;

- facilitate international cooperation in counterterrorism intelligence, including the bilateral efforts of individual agencies;

- not manage operational activities or take on the task of general intelligence about the proliferation of weapons of mass destruction (now coordinated in the Director of Central Intelligence Nonproliferation Center);

- be exempt from motions for pretrial discovery in the trials of indicted criminals.[9]

Since this Center would have constant access to considerable domestic law enforcement information, we believe it should *not* be located at the Central Intelligence Agency. The highly successful Director of Central Intelligence Counterterrorism Center established in the mid-1980s has a narrower mandate than the National Center that we propose and it would be incorporated into the new National Center. Instead we recommend the National Center be located in the FBI. However, the Center, in our conception, would be responsible to an operating committee, chaired by the Director of Central Intelligence and including the Director of the FBI, the Deputy Secretary of Defense, the Deputy Attorney General, the Deputy Secretary of State, and the Deputy National Security Adviser. The budget would be included within the National Foreign Intelligence Program, which already provides support for the FBI's National Security Division. Unresolved disputes would go to the National Security Council. The director of the Center would come alternately from FBI and CIA. The major intelligence organizations would all be required to provide a specified number of professionals to the Center, and this number would be exempt from agency personnel ceilings.

The concept of this Center attempts to combine the proactive intelligence gathering approach of the national security agencies, which are not legally constrained in deciding when they may investigate a possible crime, with the investigative resources of law enforcement agencies. We must have an entity that can utilize our formidable but disparate national security and law enforcement resources to analyze transnational problems. This combination should be permitted, consistent with public trust, only in a National Center that has no powers of arrest and prosecution and that establishes a certain distance from the traditional defense and intelligence agencies. The Center would also be subject to oversight from existing institutions, like the federal judiciary, the President's Foreign Intelligence Advisory Board and the select intelligence committees of the Congress.

There are precedents for creating novel interagency operating institutions that work—the National Reconnaissance Office and the reformed Counterintelligence Center offer relevant illustrations. We are not anxious to create new government institutions. But the problems in information sharing about terrorism are not just products of petty bureaucratic jealousy. They stem from a real question: how do we reconcile the practices of foreign intelligence work with the restrictions that properly limit domestic law enforcement? We believe our proposal offers a possible answer.

Prevention and Deterrence

There are several measures that we believe will contribute to prevention and deterrence of catastrophic terrorism. We suggest three measures here—an international legal initiative to make any development or possession of weapons of mass destruction a universal crime, a National Information Assurance Institute, and stronger federal support to strategic risk analysis of the catastrophic terrorism problem.

Outlawing Terror Weapons

Prevention is intertwined with the concept of deterrence. The U.S. has finally developed a sound, firm, and increasingly credible declaratory policy that criminalizes terrorist activity and supports sanctions, or even the use of force, to thwart an attack or respond. We also believe that the United States must work with other countries to extend the prohibitions against development or possession of weapons of mass destruction. Matthew Meselson and others have recently proposed a convention that would make any individual intentionally involved in biological weapons work liable as an international criminal, prosecutable anywhere, as is the case for pirates or airplane hijackers.[10] Defensive work against biological warfare agents would of course be permitted.

There are already international treaties in which governments promise to restrain their weapons developments—the nuclear Non-Proliferation Treaty, the Biological Weapons Convention, and the Chemical Weapons Convention are the most notable examples. Governments breaking such a treaty violate international law. We are pressing a different idea. Prohibited weapon development would become a universal crime, opening the way to prosecution and extradition of individual offenders wherever they may be found, around the world. This idea utilizes the power of national criminal law against people, not the power of international law against governments. It builds on analogous developments in the law of piracy, treaties declaring the criminality of airplane hijacking, crimes of maritime navigation, theft of nuclear materials, and crimes against diplomats.

We are concerned about the actions of governments, too. Over time, we hope the burden of proof in demonstrating compliance with international conventions must also shift away from those alleging noncompliance to those states or groups whose compliance is in doubt. International norms should adapt so that such states are obliged to reassure those who are worried and to take reasonable measures to prove they are not secretly developing weapons of mass destruction. Failure to supply such proof, or prosecute the criminals living in their borders, should entitle worried nations to take all necessary actions for their self-defense.

National Information Assurance Institute

Cyber-terrorism is a special problem, where private sector cooperation is vital, but elusive. The President's Commission on Critical Infrastructure Protection (often called the Marsh Commission) stressed that industry was reluctant to deal with these problems on its own because the solutions cost money, the risk is unclear, and they fear heavy-handed government

action. On the other hand, although the FBI has created a National Infrastructure Protection Center, which can help identify sites that need help, we do not think FBI, with all its operational duties, is the place to build a bridge with the private sector or harness the significant resources and expertise found on the cyber problem within the Department of Defense. So we propose a *National Information Assurance Institute*, based within the private, nonprofit sector, that could serve as a kind of industry laboratory with a central focus on cyber protection. Placed in the private sector, the institute would not itself own the infrastructure or be part of the government, but it could deal with both sides. It implements the Marsh Commission's recommendation, seeking a way for industry to organize itself better to deal with this problem as part of a public-private partnership.

For industry, this institute could become:

- a clearinghouse for sharing information assurance techniques and technology;
- a developer of common techniques and technology for information assurance;
- a trusted repository of proprietary information that poses no competitive threat;
- a single point of contact with the law enforcement, national security, and other agencies of the federal government;
- a resource for training and familiarization of industry personnel with technical best practice and government concerns, policies, and regulations.

For government, this institute could become:

- a channel for sharing sensitive intelligence about threats to information infrastructure;
- a center of technical excellence for developing and improving technology and techniques for protecting critical infrastructure;
- a unified government-industry forum for coordinating federal policy, regulation, and other actions affecting infrastructure providers.

We envision that the institute would be established as a not-for-profit research organization by a group of concerned private companies, universities, and existing not-for-profit laboratories. The institute would be governed by a board of directors drawn from the private sector and academia.

The institute staff could be supplemented by detailees drawn from both industry and government. Industry affiliates would not only include the manufacturers and maintainers of information systems, but also service vendors, their trade associations, and the major companies and trade associations from the power, telecommunications, banking, transportation, oil and gas, water and sewer, and emergency service sectors (including multinational companies, with appropriate protection for circulation of U.S.-only classified information).

This new institute could perform information assurance assessments for industry on a confidential basis. Industry representatives would be educated and trained on technical best practice, threats, and government policies. The institute would receive contracts from government. The institute could sponsor and conduct research on security assessment tools, intrusion detection, recovery, and restoration. As it identifies and develops industry standard best practices, and evaluates the vulnerability of commercial products, we prefer to rely where possible on informal private sector enforcement of these ideas in the marketplace (through insurance rating, for example), rather than formal government regulation. The institute could also perform incident evaluations, create a monitoring center for information assurance, provide on-call assistance, and help industry develop contingency plans for failure.

Risk Analysis

Other than more general policies to keep America's enemies to a minimum and to prevent anyone from acquiring weapons of mass destruction who does not already possess them, efforts to prevent catastrophic terrorism turn on the interdiction of people and materials and on deterring attacks. A serious U.S. government effort would include development of the capacity to use remote sensing technology to detect, at least from close range, any distinctive and measurable physical properties of nuclear, biological, and chemical weapons or their less commonplace precursor materials and the distribution of this technology in a form that can be used in the field. Aided by international agreements among supplier nations, materials that can be used in weapons of mass destruction would be marked or tagged wherever possible, to enhance detection or post facto identification.

Moreover, the United States should seek to ascertain the identity of every person and the contents of all freight entering its territory or its installations overseas. Though we know this goal obviously cannot be attained in the immediate future, it is a legitimate objective for the long-term. Even imperfect measures can still create the perception, among would-be terrorists, that they or their precious weapon material might run a significant risk of being intercepted. But systematic interdiction efforts require shrewder analysis of where more resources can make a difference.

The allocation of inspection and protective instruments by the government should be guided by risk analysis. This form of analysis is well known to engineers who may analyze a dangerous system to find the key sequences of errors that can lead not just to failure, but to catastrophic failure. Those are the sequences that then command disproportionate engineering attention (to add redundant switches, for example). Not all worries merit equal concern. Engineers refer to a "balanced" design as one where all the components have been designed to be as good as the whole system needs, neither better nor worse.

The role of risk analysis, or strategic analysis for risk control, is to analyze threats and define risks in a natural way (avoiding the temptation to define them in terms of existing agency boundaries or capabilities), to commission further data gathering and analysis to assess relative significance, and then to subdivide acute risks into actionable components where resources can make a difference.[11] A systemic approach is needed that encompasses broad area surveillance; specific threat identification; targeted surveillance and warning; prevention, protection, deterrence, interdiction and covert action; consequence management; forensic analysis of a site to determine responsibility, punitive action, and learning lessons.

Analysis, for instance, shows that international border crossings are an important bottleneck in the worldwide movement of criminals. The United States, rather than just looking after the verifiability of its own passports, should organize resources focused on such bottlenecks throughout the world. We can imagine, for instance, a system created, with American funding, to insure that every country's passports are computer readable, that every passport control officer has such a reader, and that every reader is linked to a database that can validate the status of the document, or indicate the need for further inquiries. The database need not invade the internal files of any government. As is already the case in the private sector, third entities can be created to perform the clearinghouse role, using data supplied by participating governments. Naturally, terrorists could still use documents of non-participating countries, but those would attract just the suspicion such travelers seek to avoid.

Government agencies can do many things reasonably well, but strategic risk analysis is not one of them. We recommend establishing a center for catastrophic terrorism risk analysis, offering a substantial multi-year contract, executed by the FBI, to a not-for-profit research center to perform this sort of analysis, devise and evaluate exercises and tests, and develop concepts of operations for countering catastrophic terrorism. Early in the nuclear era the RAND Corporation played an important part in helping the government think about a new set of security concerns. The Department of Defense has made a start by establishing an advanced concepts office in the newly formed Defense Threat Reduction Agency. But risk analysis will require a national, not just a DOD, focus.

Crisis and Consequence Management

Crisis management for catastrophic terrorism should include the capacity to employ appropriate force and specialized capabilities in any part of the world, endeavoring to minimize collateral damage, and to thwart a possible attack using weapons of mass destruction. Crisis management would include urgent protective efforts, employing every resource at the disposal of federal, state, and local governments. The U.S. government should also acquire capacities and plans for forensic

investigation of the site of an attack in order to collect evidence and identify those responsible for further action.

Consequence management is a capacity to deal with the aftermath of an attack. The United States, at all levels of government, must develop the ability to respond effectively within hours, if not minutes, to any use of a weapon of mass destruction—nuclear, biological, chemical, or cyber—against American targets with appropriate and specific measures to mitigate casualties and damage. This is a large order. The needed capabilities include emergency medical care, distributions of protective gear or medications (including vaccines for those not yet exposed to the pathogen[12]), evacuations, and area quarantines, among other measures. Since these capabilities would need to be on a large scale, extensive preparations are needed to ready them in central locations, be able to mobilize them on sudden notice, be able to transport them where needed, and expect local authorities and caregivers to be ready to receive and use them. The United States must also have emergency plans readied, including redundant or alternative control systems, for sustaining the operation of infrastructure that provides the necessities of life, if this infrastructure comes under attack.

The present system for handling terrorist emergencies is based on the FBI or—if overseas—on initiatives by State Department representatives or local military commanders. If an acute threat emerges in the United States, local authorities are expected to alert the local FBI office. The FBI's special agent in charge would then organize intergovernmental response through activation of a strategic intelligence center in Washington, and a joint operations center and joint public affairs effort in the local area. If there were a WMD threat, the FBI could call on its Weapons of Mass Destruction Operations Unit, which has "Domestic Guidelines" to coordinate with other agencies and, in particular, seek Pentagon assistance.

There is ample legal authority to seek military aid in dealing with such a crisis on U.S. soil. FBI can call upon an existing, though rather small-scale, interdepartmental Domestic Emergency Support Team (or, overseas, a Foreign Emergency Support Team). FBI has its own Hazardous Materials Response Unit. More military assistance would likely come, not from a joint interservice command, but from the Army's Chemical and Biological Defense Command. If the attack occurred, consequence management would be organized by the Federal Emergency Management Agency (FEMA) under what is called the "Federal Response Plan."

This structure is adequate for responding to ordinary terrorist threats or attacks, or perhaps even small scares related to weapons of mass destruction, as in February 1998 when FBI learned that two suspects in Las Vegas, one of whom had earlier been convicted for fraudulently obtaining bubonic plague virus, might be in possession of some anthrax. The crisis response went well, including coordination with limited Defense Department resources. The suspects turned out not to have any anthrax.

However, if some agency of the U.S. government learned that a large scale WMD attack might actually be imminent, threatening tens of thousands of lives, we expect that this structure for responding would almost instantly be pushed aside. The White House would immediately become involved and would seek to use every bit of power at America's disposal in order to avert or contain the attack. The operational command structure would need to be capable of directing everything from CIA covert actions to strikes by bombers or missiles, be able to set up interdiction involving ground, sea, and air forces, and be able to mobilize and move thousands of soldiers (active duty, ready reserve, and National Guard) and thousands of tons of freight (in various emergency supplies and support for deployed units). Nor can any of these actions happen quickly unless plans have already been drawn up and units designated to carry them out, with repeated training and exercises to create a readiness to bring the plans to life. In this situation, the Defense Department's capabilities would immediately become paramount. The FBI does not command such resources and does not plan to command them.

So what is needed is a *two-tier* structure for response, one for ordinary terrorist incidents that can be managed by federal law enforcement with interagency help, and a second structure readied for the contingency of truly catastrophic terrorist attack. The United States has set up unified combatant commands to prepare for remote but extremely serious contingencies of regional aggression, like U.S. Central Command's response to Iraq's 1990 invasion of Kuwait. The United States must also develop a structure that is ready to respond to this new, perhaps even more likely, contingency of the future.

Rather than create a new combatant command, we suggest instead two new offices, one set up within the Office of the Secretary of Defense, and the other created within the existing combatant command, U.S. Atlantic Command, that is already responsible for the security of the American homeland with operational responsibility for the majority of the U.S. armed forces. Our working titles for these offices are *Catastrophic Terrorism Response Offices*, or CTROs. The new offices

would build a capability centered in the federal government but including state and local authorities along with relevant parts of the private sector to respond, once authorized to act by the President and the Secretary of Defense, to validated terrorist threats that would cause massive loss of life (measured in the thousands, i.e., significantly larger than the attack on the federal building in Oklahoma City) or otherwise jeopardize the operation of American government or critical infrastructure necessary to public health or the functioning of the economy. Obviously, the President and his advisors would face a difficult judgment to determine when this threshold has been met, but such judgments are required in other areas of national security policy and they can be made here.

The CTROs would plan and organize for a U.S. response to catastrophic terrorism by all elements of the U.S. government.

They would:

- assess intelligence and warning information in order to alert the National Command Authority of catastrophic terrorist threats;

- set requirements for, among other things, the collection and analysis of intelligence carried out by the proposed National Counterterrorism Intelligence Center;

- define needed resources and assure that resources, procedures, and trained personnel are available at the federal, state, and local level to respond to validated catastrophic threats;

- sponsor training and exercises involving federal, state, and local authorities for responding to catastrophic terrorist attacks;

- task operations by other organizations once activated by the President through the Secretary of Defense (with actual operations being undertaken by line organizations, whether covert actions by the CIA or military operations through the Joint Chiefs of Staff or law enforcement actions by the FBI);

- coordinate international preparedness to join in a multinational response against catastrophic terrorist threats.

The two CTROs should have the legal responsibility to achieve overall U.S. government readiness to respond to catastrophic terrorist threats when asked to do so by the President, acting through the Secretary of Defense. The defense secretary would be the executive agent for both offices and for their budget program, so that the CTROs can program elements in the DOD program budgeting system and have the job of submitting a consolidated catastrophic terrorism response program to the White House for inclusion in the President's proposed budget. The Congress pointed toward such a goal in the Defense Against Weapons of Mass Destruction Act of 1996 (more commonly known as the Nunn-Lugar-Domenici Amendment, or Nunn-Lugar II) which mandated that DOD train civilian emergency personnel at all levels of government and establish rapid terrorism response teams. Our idea broadens the scope of the initiative and suggests a way to give it a stronger, and more operational, institutional base.[13]

The Department of Defense would play a strong, supporting role, not the leading one. It has resources and capabilities in dealing with biological and chemical weapons. Its resources would be needed either for crisis or for consequence management, but only as part of a larger national effort.

Why two offices, rather than one? The CTRO centered in the Office of the Secretary of Defense should concentrate on planning and preparedness for preemptive and/or retaliatory strikes, utilizing covert action or the uniformed armed forces. It should draw additional staff from and involve a relatively narrow set of agencies: the Joint Staff, CIA, and FBI. This is a highly secret, delicate activity now done only in an ad hoc manner between CIA and JCS and never with the FBI. But the second office must be prepared to handle a much broader range of activities that affect prevention, containment, and management of the consequences of a catastrophic attack. The number of agencies involved must also be inclusive. This consequence management function must draw on the resources of the National Guard, FEMA, the Department of Health and Human Services, and other federal, state and local agencies. This is a much larger orchestra that we think can be well

prepared and conducted, if activated in an emergency, by an integrated structure like U.S. Atlantic Command.

Neither of these new offices need be very large. Their jobs are planning and preparation, not day-to-day intelligence gathering, law enforcement, or combat operations. Yet the work they do will be invaluable, should the crisis ever come.

Acquisition

A national policy must include a concept for buying what is needed. The government is already ordering everything from vaccines to new research, but nearly two dozen agencies have their own separate shopping lists and ways of doing business. All these budget requests eventually arrive in Congress, where the lack of overall acquisition planning creates new difficult choices for the affected committees and budget competition on the Hill. In November 1997 a conference report accompanying appropriations for the Department of Justice correctly warned that "additional emphasis is needed to coordinate efforts among the many participating departments and agencies that have personnel, resources, and expertise to contribute" to the counterterrorism mission.[14]

We urge the creation of a coordinated, broadly focused, budget program that will plan, coordinate, and track all R & D and acquisition projects intended to improve counterterrorism capabilities, both conventional and unconventional, defensive and offensive, domestic and foreign, including field testing of new operational capabilities. This national counterterrorism acquisition program would be based on a government-wide five-year plan to develop and acquire the needed technology and operational skills. Examples include improved detectors of special materials (like radioactive substances), forensic investigation tools, automated tracking and analysis systems, and improved protective clothing or equipment.

The Clinton administration has already started a significant effort to acquire stockpiles of vaccines, antidotes, and antibiotics, adding to such a program already underway for the U.S. armed forces. Resources are needed for storage, transportation, and shipment of such medications. There is a further need for renewed research into defense against biological weapons, including adaptation to genetic alteration of deadly pathogens in order to defy available vaccines or antidotes. Improved detection devices need to be complemented by specialized laboratories, set up around the country, that can rapidly analyze substances or validate field identifications.

Attorney General Janet Reno warned Congress of the extraordinary acquisition requirements that would be created by a serious policy to cope with the threat of catastrophic terrorism. In April 1998 she explained that "we may need to develop an approach which will permit the government to accelerate the normal procurement procedures to quickly identify and deploy new technologies and substances needed to thwart terrorist threats and respond to terrorist acts. These procedures would be used not only to purchase medications and other needed tools, but also, in some instances, to borrow medications or tools from, or to enter into effective partnerships with, both academia and industry."[15] To us, this statement is a call for an interdepartmental acquisition program that draws on Defense Department expertise. Despite its limitations, the Defense Department still has the best track record in the government for successful sponsorship of technological development and rapid, large-scale procurement.

This proposed acquisition program would be quite separate from other, also worthwhile, acquisition programs for cooperative threat reduction (like the Nunn-Lugar programs for the former Soviet Union), efforts to counter narcotics trafficking or organized crime, and nonproliferation activities; its focus would be counterterrorism. An effective interdepartmental committee system is needed for this acquisition program to be successful.

We suggest a *National Counter-Terrorism Acquisition Council* that would be chaired by the undersecretary of defense for acquisition and technology. Such an acquisition council should include representatives from other departments, including top subcabinet officials from Justice, Energy, Treasury, State, and Health and Human Services, as well as the deputy director of FBI, the deputy director of CIA for science and technology, and the director of the Federal Emergency Management Agency.

This acquisition council would need to oversee the field-testing and evaluation of new capabilities with participation of several concerned agencies. Some agencies might worry about Defense usurpation of their procurement decisions. Instead we think it is just these agencies that should want a national program. Defense will already be acquiring vast quantities of

equipment for its own needs. Suppliers will naturally configure themselves around this demand. Civilian agencies need a way to be sure that their particular requirements are also taken into account.

We suggest that the Defense Department establish an initial program with more than $100 million to fund the development of some technology ideas that would offer benefits across the government. Where appropriate, the acquisition council would designate lead agency responsibilities. The acquisition council can also facilitate easier sharing of technology, tactics, and material from one agency to another. Further, this council can provide a point of contact for international program and technology sharing with other nations. It can provide government-wide procedures controlling access to especially sensitive projects within the national counterterrorism program. Although the program would be executed by various departments, the acquisition council would still be held responsible for monitoring the progress of each program element and should be expected to report annually on progress to both the President and to the Congress.[16]

Conclusion

Our group's deliberations started from the premise that catastrophic terrorism poses a first-order threat to our nation's future. We then asked, in effect: if we had a serious national policy to deal with this threat, what would our government be organized and able to do? In 1940 and 1941 the U.S. government imagined what kind of forces it would have in order to wage a global war. The answers were so far beyond existing reality that we can imagine all the wry smiles and shaking heads that must have been seen in Washington offices as the planning papers made their rounds. Similar cycles occurred in the Cold War. For example, the notion of an intelligence system founded on photographic surveillance from the upper atmosphere, or outer space, seemed outrageously far-fetched in 1954, when the U-2 program was born. The films and cameras alone seemed to be an overwhelming hurdle. A few years later the U-2s were flying; six years later satellites were doing the job. Similar stories can be told about the strange and remarkable history of intercontinental missile guidance or about how the U.S. and its allies developed the capability to move more than a half-million troops and thousands of armored fighting vehicles and their supporting infrastructure to the Persian Gulf within a few months, from both Europe and North America.

Our government can deal with new challenges. But first we must imagine success. Then we must organize ourselves to attain it.

Notes

1. For a careful, dispassionate evaluation, see Richard A. Falkenrath, Robert D. Newman & Bradley Thayer, *America's Achilles Heel: Nuclear, Biological, Chemical Terrorism and Covert Attack* (Cambridge: MIT Press, 1998). On the increasingly fragile and interconnected infrastructure and on the cyber threat, see also the Report of the President's Commission on Critical Infrastructure Protection (also known as the Marsh Commission, for its chairman), *Critical Foundations: Protecting America's Infrastructures*, Washington, DC, October 1997.

2. The most detailed and credible threat scenarios, based on close analysis of specific vulnerabilities, should not be published at all. These would be indispensable but quite sensitive documents to be prepared by relatively small groups of knowledgeable officials and expert consultants.

3. Address by President Clinton, May 22, 1998; White House Fact Sheet on PDD-62; all distributed by the White House Press Office.

4. Roberto Suro & Dana Priest, "Plan to Overhaul Anti-Terrorism Strategy Would Boost NSC's Role," *Washington Post*, March 24, 1998, p. A7; see also M.J. Zuckerman, "Anti-terror 'czar' to coordinate $7B effort," *USA Today*, May 4, 1998, p. 1A.

5. Richard E. Neustadt, *Presidential Power and the Modern Presidents: The Politics of Leadership from Roosevelt to Reagan* (New York: Free Press, 5th ed., 1990), p. 7.

6. James Q. Wilson, *Bureaucracy: What Government Agencies Do and Why They Do It* (New York: Basic Books, 1989), pp. 271-72.

7. See Maurice Matloff, *Strategic Planning for Coalition Warfare, 1943-1944* (Washington: U.S. Army, 1959); John Ehrman, *Grand Strategy: August 1943-September 1944* (London: HMSO, 1956); Herman M. Somers, *Presidential Agency: The Office of War Mobilization and Reconversion* (Cambridge: Harvard University Press, 1950). On the Northern Ireland example, see Philip Zelikow, "Policing Northern Ireland (A): A Question of Primacy," and "Policing Northern Ireland (B): A Question of Balance," Kennedy School of Government Case Program, Harvard University, 1994.

8. Philip Heymann has been especially helpful to us in understanding the legal capabilities and limits affecting counterterrorist investigations. For his survey of the legal and policy dilemmas associated with countering terrorism, see Philip B. Heymann*, Terrorism and America: A Commonsense Strategy for a Democratic Society* (Cambridge: MIT Press, 1998).

9. These motions seek to find whether the police or prosecutors have any information, not already disclosed, that may tend to show the innocence of the defendant. Even if statutes are amended, under our proposal the arresting agency and prosecutor's office would remain subject to such discovery motions, which the Supreme Court considers an aspect of constitutionally mandated due process of law. Since the Center would not itself carry out law enforcement operations or make prosecutorial decisions, it should be exempted from such discovery, although any information it chooses to provide to police or prosecutors would then be discoverable under the procedures specified in the current Classified Information Protection Act.

10. For a summary, see Philip Heymann, Matthew Meselson & Richard Zeckhauser, "Criminalize the Traffic in Terror Weapons," *Washington Post*, April 15, 1998, p. A19; a detailed copy of the proposal is available from Meselson. Development of biological weapons is distinguishable from the necessary work to develop defenses against such weapons.

11. We are especially indebted to Malcolm Sparrow for his thinking on this subject, which we have abridged.

12. Vaccines *may* be useful after exposure to anthrax, however, and smallpox (for different reasons).

13. The FBI has also been given funds for training local "first responders" to an emergency. FBI must be involved in the effort, but based on training plans that fully integrate what Defense and other federal agencies can and are doing. These useful but fragmentary efforts indicate the case for an office like the one we suggest.

14. Conference Report 105-405 for FY 1998 Appropriations to the Departments of Commerce, Justice, State, the Judiciary, and Related Agencies, November 13, 1997.

15. Statement of Attorney General Reno, Hearings of the Senate Judiciary Subcommittee on Technology, Terrorism and Government Information and the Select Committee on Intelligence, "The Threat of Chemical and Biological Weapons," April 22, 1998.

16. A useful analogy for such an acquisition program, on a smaller scale, is the Technical Support Working Group, which develops counterterrorism equipment for use by all agencies of the federal government and for state and local law enforcement, principally with DOD funding. This program concentrates on traditional counterterrorism acquisition, as in robots for municipal bomb disposal squads. One person we talked to told us: "This thing works because it is so small that it flies under the radar of Congress. If you grow it larger, you're going to need a policy to go with it."

About the Authors

The Honorable Ashton B. Carter

Ash Carter is Ford Foundation Professor of Science and International Affairs at Harvard University's John F. Kennedy School of Government and Co-Director, with William J. Perry, of the Stanford-Harvard Preventive Defense Project.

From 1993-1996 Carter served as Assistant Secretary of Defense for International Security Policy, where he was responsible for national security policy concerning the states of the former Soviet Union (including their nuclear weapons and other weapons of mass destruction), arms control, countering proliferation worldwide, and oversight of the U.S. nuclear arsenal and missile defense programs; he also chaired NATO's High Level Group. He was twice awarded the Department of Defense Distinguished Service Medal, the highest award given by the Pentagon. Carter continues to serve DOD as an adviser to the Secretary of Defense and as a member of both DOD's Defense Policy Board and Defense Science Board, and DOD's Threat Reduction Advisory Council.

Before his government service, Carter was director of the Center for Science and International Affairs in the Kennedy School of Government at Harvard University and chairman of the editorial board of *International Security*. Carter received bachelor's degrees in physics and in medieval history from Yale University and a doctorate in theoretical physics from Oxford University, where he was a Rhodes Scholar.

In addition to authoring numerous scientific publications and government studies, Carter was an author and editor of a number of books, most recently *Preventive Defense: An American Security Strategy for the 21st Century* (with William J. Perry). Carter's current research focuses on the Preventive Defense Project, which designs and promotes security policies aimed at preventing the emergence of major new threats to the United States.

Carter is a Senior Partner of Global Technology Partners, LLC, and a member of the Advisory Board of MIT Lincoln Laboratories, the Draper Laboratory Corporation, and the Board of Directors of Mitretek Systems, Inc. He is a consultant to Goldman Sachs and the MITRE Corporation on international affairs and technology matters, a Member of the Council on Foreign Relations, and a Fellow of the American Academy of Arts and Sciences.

The Honorable John M. Deutch

Dr. John Deutch has served in significant government and academic posts throughout his career. In May 1995, he was sworn in as Director of Central Intelligence following a unanimous vote in the Senate, and he served as DCI until December 1996. In this position, he was head of the Intelligence Community (all foreign intelligence agencies of the United States) and directed the Central Intelligence Agency. From March 1994 to May 1995, he served as the Deputy Secretary of Defense. From March 1993 to March 1994, Dr. Deutch served as Under Secretary of Defense for Acquisitions and Technology. From 1977 to 1980, Dr. Deutch served in a number of positions for the U.S. Department of Energy: Director of Energy Research, Acting Assistant Secretary for Energy Technology, and Undersecretary of the Department.

Dr. Deutch has served on many commissions during several presidential administrations, and he has received fellowships and honors from the American Academy of Arts and Sciences (1978), Alfred P. Sloan (Research Fellow 1967-69), and John Simon Guggenheim (Memorial Fellow 1974-1975). Public Service Medals have been awarded him from the Department of Energy (1980), the Department of State (1980), the Department of Defense (1994), the Department of the Army (1995), the Department of the Navy (1995), the Department of the Air Force (1995), and the Coast Guard (1995). He also received the Central Intelligence Distinguished Intelligence Medal (1996) and the Intelligence Community Distinguished Intelligence Medal (1996).

Dr. Deutch has been a member of the faculty of the Massachusetts Institute of Technology from 1970 to present, where he has served as Chairman of the Department of Chemistry, Dean of Science and Provost. Currently, Dr. Deutch is an MIT Institute Professor.

Dr. Deutch earned a BA in history and economics from Amherst College, and both a BS in chemical engineering and a Ph.D. in physical chemistry from MIT. He holds honorary degrees from Amherst College, University of Lowell and Northeastern University. Dr. Deutch serves as director for the following publicly held companies: Ariad Pharmaceutical, Citicorp, CMS Energy, Cummins, Raytheon, and Schlumberger Ltd.

Philip D. Zelikow

Philip Zelikow is Director of the Miller Center of Public Affairs and White Burkett Miller Professor of History at the University of Virginia. He has taught at Harvard University, and he served as a career diplomat in the Department of State and on the staff of the National Security Council.

His books include *The Kennedy Tapes: Inside the White House During the Cuban Missile Crisis* (with Ernest May, Harvard UP), *Germany Unified and Europe Transformed: A Study in Statecraft* (with Condoleezza Rice, Harvard UP), and the forthcoming rewritten edition of *Essence of Decision: Explaining the Cuban Missile Crisis* (with Graham Allison, Longman). He has also written a study of intelligence policy for the Twentieth Century Fund, published as *In From the Cold.*

A member of the Department of State's Historical Advisory Committee, a former consultant to the Office of the Secretary of Defense, and a participant in Harvard's Intelligence and Policy Project, Zelikow is also the deputy director of the Aspen Strategy Group, a program of the Aspen Institute. He holds a doctorate from the Fletcher School and a law degree from the University of Houston.

About Visions of Governance for the Twenty-First Century

The Imperative for Change

Momentous social and economic forces are reshaping democratic governance around the world. Current political rhetoric insists that the era of big government is over—but what will take its place?

The answer is not at all obvious. While some national governments are getting smaller, they are not necessarily getting less powerful. Information technology, which has allowed industry to do more with less, is opening up the same opportunities for governments, while bringing with it new threats to their traditional roles and functions. The increasing number and authority of supranational organizations is countered by trends toward devolution in the United States and Europe. Non-profit and even for-profit entities are taking on tasks once thought of as the sole province of government. Markets are being created and used to produce public as well as private goods.

All of this is taking place amidst a loss of confidence on the part of citizens with their governments. This unhappiness transcends partisanship and economic well-being. It is as if, on some level, the public knows that its government is simply out of step with the times.

Dean Joseph Nye believes it is a critical part of the Kennedy School's mission to address the precipitous decline in confidence in public institutions, by identifying and illuminating some of the most important trends affecting governments, and by creating a public conversation with citizens and policy makers about appropriate responses to changing realities and expectations of government. This imperative is not an artifact of the millennium. In fact, were public trust in government high, change could be incremental. What is needed now, however, is new ways of thinking about governance.

Growing Mistrust in Government

The first year of the Visions Project focused on generating a critical mass of intellectual activity among a core group of Harvard faculty around the issue of trust in government, which resulted in the publication in October 1997 of Why People Don't Trust Government. The book was the culmination of over a year of inquiry into the scope and performance of government (actual and perceived) and the possible causes of citizens' dissatisfaction with it.

The Project is continuing this investigation of declining trust in government with both a study of anomalies in the evidence, such as high levels of confidence in the military, and an international comparative study of public trust in government (Critical Citizens, forthcoming in the spring of 1999).

New Ways of Thinking about Governance

The Project is focusing its attentions on several new areas of inquiry:

- **New paradigms for national security policy**. The Catastrophic Terrorism Study Group will recommend a comprehensive program of responses by the U.S. government to the danger of large-scale, catastrophic terrorism.

- **The future direction of social policy**. Is it possible to bring the productive and innovative power of markets to traditional questions of social welfare? "Who's Responsible? Renegotiating the Social Contract" will evaluate the central question of alternatives to traditional government activism in various areas of social policy.

- **How governments can manage and measure their performance to better serve their citizens.** A series of Executive Session and Practitioner Forums on Performance Management will seek to engage and invest political decision makers in a management movement which offers the possibility of a new kind of democratic accountability.

- **How information technologies are changing the realities and expectations of governments.** The explosive growth of information as a resource and of computer networks as a medium is at once evident everywhere and yet very little understood. The Visions Project has begun a continuing effort to understand the multiplicitous changes being wrought by information technologies in order to focus attention on maximizing their benefits and minimizing their costs to society.

Visions Project Director Elaine Kamarck will weave these themes together in a book which will raise significant questions that are central to democratic governments. Will a more effective capacity to fight global crime and global terrorism be compatible with our deeply held beliefs that we should protect the privacy of our citizens from internal spying? Can a system which attempts to meet a variety of social needs through market mechanisms and via non-governmental organizations really guarantee equality of treatment? Can innovative governmental organizations also be accountable to elected officials and to the public?

These are momentous questions, and they illustrate why large-scale social and governmental change does not happen overnight. Our challenge is to find the value in change, and that will require new visions of governance for the 21st century.

About the Stanford-Harvard Preventive Defense Project

The Preventive Defense Project is a joint venture between Stanford University and Harvard University. Preventive Defense is a concept of defense strategy for America in the post-Cold War era. The premise of Preventive Defense is that the absence of an imminent, major, traditional military threat to American security presents today's national security leaders with an unaccustomed challenge and opportunity: to prevent new Cold War-scale threats to U.S. security from emerging in the future. While the United States defense establishment must continue to deter regional conflicts in the Persian Gulf and the Korean Peninsula, as well as keep the peace and provide humanitarian relief in selected instances, its highest priority is to contribute to forestalling developments that could directly threaten the survival and vital interests of American citizens.

The Preventive Defense Project will initially concentrate on forging productive security partnerships with Russia and its neighbors, dealing with the lethal legacy of Cold War weapons of mass destruction, engaging an awakening China, and countering proliferation of weapons of mass destruction and catastrophic terrorism. The Project seeks to contribute to these objectives through the invention of new policy approaches reflecting Preventive Defense, intensive personal interaction with defense and military leaders around the world, and through the establishment of highly informed, non-governmental track two initiatives that explore new possibilities for international agreement.

Current Preventive Defense Project initiatives include:

- **Describing Preventive Defense.** In a forthcoming book, the Project's leaders will explain the concept to a wider audience, drawing on their experience in the Pentagon and making recommendations for the future of American security policy.

• **Russia.** The Project is pursuing a number of activities designed to support Russian foreign and defense policy leaders in developing a post-Soviet security identity that matches Russia's interests to the interests of international stability. These initiatives include assisting Russian military reform and the development of national security decision-making processes, furthering NATO-Russia relations, encouraging the development of mutually beneficial relations with the other Newly Independent States of the former Soviet Union, and charting a course for nuclear arms reduction after START II ratification.

• **Other Newly Independent States (NIS) of the former Soviet Union.** Expanded military-to-military contacts and economic opportunities are key to the continued security and stability of the NIS. The Project is pursuing initiatives with Ukraine, the Central Asian states, and the Caucasus countries, including the Caspian Sea region.

• **Eliminating the lethal legacy of the Cold War.** Through such innovations as the Nunn-Lugar program, the United States intervened to promote nuclear safety and non-proliferation in the early years after the breakup of the Soviet Union. Much was accomplished in the first post-Cold War era, but changing politics in Russia and the United States have caused their cooperation in controlling "loose nukes" to bog down and progress in chemical and biological weapons dismantlement to falter. Nunn-Lugar and arms control require "reinvention" if they are to continue in the second post-Cold War era. The Project seeks to contribute fundamental new ideas to that reinvention.

• **China.** Through research and intensive track two dialogue with Chinese defense and military leaders, the Project will concentrate on defining the specific content of the U.S. policy of engagement with China.

• **Countering the proliferation of weapons of mass destruction (WMD).** The glimmers of trouble to come provided by Iraq's WMD programs during and since the Gulf War show that proliferation has moved from a diplomatic problem to a direct military threat. DOD, therefore, needs to strengthen its Counter-proliferation Initiative, which is designed to contribute both to proliferation prevention and to the capabilities of U.S. forces to counter WMD in regional conflict. The Project seeks to define organizational and technical responses by DOD to this growing threat.

• **Organizing to combat catastrophic terrorism.** The Project convened the Catastrophic Terrorism Study Group, which is a collaboration of faculty from Harvard University, the Massachusetts Institute of Technology, Stanford University, and the University of Virginia and is co-chaired by Ashton B. Carter and John M. Deutch. The Study Group is identifying appropriate responses by the United States government to the dangers of catastrophic terrorism.

The Preventive Defense Project is a multi-year effort supported by the Carnegie Corporation of New York, the John D. and Catherine T. MacArthur Foundation, and private sources. The Project's Co-Directors are former Secretary of Defense William J. Perry and former Assistant Secretary of Defense for International Security Policy Ashton B. Carter. Former Chairman of the Joint Chiefs of Staff General (ret.) John M. Shalikashvili and former Deputy Assistant Secretary of Defense for Russia, Ukraine and Eurasia Elizabeth Sherwood-Randall serve as Senior Advisors. Additional contributors to the Project include: member of President Clinton's Foreign Intelligence Advisory Board Robert J. Hermann and former Deputy Secretary of Defense John P. White.

Institute for International Studies

Stanford University

The Institute for International Studies (IIS) seeks solutions to real-world, international problems that affect international security, the global environment, and international political economy. IIS creates a dynamic environment in which to address these critical issues by bringing experts from a variety of disciplines within Stanford University together with long- and short-term visitors from other academic, government, and corporate institutions. At any given time, over 150 scholars are engaged in policy studies within the Institute's federation of research centers.

Center for International Security and Cooperation

Stanford University

The Center for International Security and Cooperation (CISAC), part of Stanford University's Institute for International Studies, is a multidisciplinary community dedicated to research and training in the field of international security. The center brings together scholars, policymakers, scientists, area specialists, members of the business community and other experts to examine a wide range of international security issues.

Belfer Center for Science and International Affairs

Harvard University

The Belfer Center for Science and International Affairs (BCSIA) is the hub of the John F. Kennedy School of Government's research, teaching, and training in international security affairs, environmental and resource issues, and science and technology policy. The center's mission is to provide leadership in advancing policy-relevant knowledge about the most important challenges of international security and other critical issues where science, technology, and international affairs intersect. BCSIA's leadership begins with the recognition of science and technology as driving forces transforming threats and opportunities in international affairs. The center integrates insights of social scientists, natural scientists, technologists, and practitioners with experience in government, diplomacy, the military, and business to address critical issues.

Publications of the Preventive Defense Project

NATO After Madrid: Looking to the Future

The Content of U.S. Engagement with China

Fulfilling the Promise: Building an Enduring Security Partnership Between Ukraine and NATO

Reforming the Department of Defense: The Revolution in Business Affairs

The NATO-Russia Relationship

Catastrophic Terrorism: Elements of a National Policy

Printed copies of this publication are available upon request.

Terrorism is not a new phenomenon. But today's terrorists, be they international cults like Aum Shinrikyo or individual nihilists like the Unabomber, act on a greater variety of motives than ever before. More ominously, terrorists may gain access to weapons of mass destruction, including nuclear devices, germ dispensers, poison gas weapons, and even computer viruses. Also new is the world's dependence on a nearly invisible and fragile network for distributing energy and information.Â Such an act of catastrophic terrorism would be a watershed event in American history. It could involve loss of life and property unprecedented in. Loading, please wait Responding to Terrorism: Is the New Department of Homeland Security the Answer? National Center for Digital Government Lewis Branscomb, Harvard University Situation calls for new approach to policy research & design ï® ï® ï® ï® ï® New problems, poor fit to government experience and structure. Even to ways of thinking about roles of government. High stakes, high levels of uncertainty.Â Catastrophic terrorism is the ultimate in asymmetric conflict; ï® ï® ï® ï® Now the asymmetry is reversed. Each terrorist threat is in some ways a new conflict.Â Use â€œcircuit breakersâ€ to isolate and stabilize failing system elements (soft failure modes). Build security and flexibility into basic designs Design systems for real people, behaving as they can be predicted to behave. Catastrophic terrorism: elements of a national policy. Imagining the Transforming Event. We find terrorism when individuals or groups, rather than governments, seek to attain their objectives by means of the terror induced by violent attacks upon civilians.Â When governments act in concert with private individuals or groups, the United States government may call it war, or state-sponsored terrorism, and retaliate against both the individuals and the governments. Whatever the label, terrorism is not a new phenomenon in national or international life, although terrorists may be animated by a greater variety of motives than ever before, from international cults like Aum Shinrikyo to the individual nihilism of the Unabomber.