Michigan Journal of International Law

Volume 20 | Issue 3

1999

Catastrophic Terrorism- Thinking Fearfully, Acting Legally

Barry Kellman
DePaul University College of Law

CATASTROPHIC TERRORISM—THINKING FEARFULLY, ACTING LEGALLY

*Barry Kellman**

INTRODUCTION

Catastrophic terrorism[1] has incited headlines, *60 Minutes* reports, Presidential addresses, and popular fiction.[2] A most dire threat comes

---

* Professor of Law, DePaul University College of Law.

1. "Catastrophic terrorism" is an intentionally undefined term, reflecting the fact that terrorists who aspire to inflict catastrophic injuries have a long menu of options to employ, and reflecting the conclusion that debates over whether a particular technology is or is not within this category are, essentially, inconclusive. The definition of "catastrophic terrorism," as opposed to conventional terrorism, turns less on what type of device is used than on the magnitude of the effects. Conventional terrorism, plane hijacking, kidnapping, or bombing with conventional explosives causes casualties in the hundreds and does not lead to a wide-scale disruption of commonplace affairs, even within the locale of the event. By contrast, catastrophic terrorism would be capable of, and typically would be intended to, cause casualties in the thousands (or tens of thousands) or cause an extraordinary suspension of civilized order. In general, "catastrophic terrorism" should include the use, by individuals or sub-national groups, of nuclear, chemical, biological, or radiological weapons. Also included should be conventional explosions of nuclear power plants or chemical facilities which release toxic substances over a wide area. Moreover, the term should include various types of cyber-terrorism that cause the breakdown of essential infrastructure such as communications, banking, or air traffic control. *See generally* Ashton Carter, John Deutch, & Philip Zelikow, *Catastrophic Terrorism; Tackling the New Danger*, WASH. Q., Nov.–Dec. 1998, at 80. *See also*, Walter Laqueur, *Postmodern Terrorism*, FOREIGN AFFAIRS, Sept.–Oct. 1996, at 32; and William J. Broad, *Sowing Death: How Japan Germ Terror Alerted World*, N. Y. TIMES, May 26, 1998, at 1.

2. Indeed, the furor over catastrophic terrorism has prompted a counter-reaction of skepticism alleging that the threat has been over-stated and that the response is disproportionate. *See*

from trans-national criminal organizations whose motives are altogether distinguishable from those of States.[3] These organizations would not consider overt war, and deterrence is meaningless. These organizations are seeking to amass pecuniary or political capital, and catastrophic weapons may substantially augment those plans.

The time has come to move beyond howls of alarm to a public discussion of what policies should be adopted or reformed. That discussion should proceed even as crucial questions remain only partially answerable: How realistic is the possibility of catastrophic terrorism? How easy is it to make a catastrophic device that actually works? Why would any person or group want to kill hundreds, thousands, or tens of thousands of innocent victims?

These questions do not have empirical answers, and some skepticism should attend assertions that risks of catastrophic terrorism may be measurable. Assessing risk is difficult because catastrophic terrorism is a low probability threat which, if it occurs, could have exceptionally high casualties. Yet, four points can be offered without serious contradiction. First, technical obstacles to catastrophic terrorism will decline with time. The capabilities for producing lethal devices will spread, and the choke points of human activity will become more concentrated, thereby unfortunately converging the ability to make a lethal weapon with an ability to use it to devastating effect. The necessary ramification is that whatever the technological barriers to accomplishing an act of catastrophic terrorism may or may not be, those barriers will be overcome, sooner or later. Even if the risks are not now realistic, they will be.

Second, after a catastrophic terrorist event actually occurs, legal issues such as protecting civil liberties and constitutional rights may likely be ignored, at least temporarily. Thus, the costs of a catastrophic event must be measured not only in loss of life and property but also in the probable disruption and constriction of due process of law.[4] This assertion directly leads to point three: the costs of a disorganized response to a catastrophic event, in money and in jeopardy to our civil liberties, are likely to exceed overwhelmingly the costs of preventing an event or, if necessary, of executing a well-planned effort to mitigate and remedy the harm done. America will be well-served by careful legal planning, in advance, which appreciates catastrophic terrorism's risks,

---

generally Peter Pringle, *Terrorism: America's Newest War Game*, THE NATION, November 9, 1998, at 11.

3. *See generally* John M. Deutch, *Terrorism; The Possibility of the Use of More Sophisticated Weapons*, FOREIGN POLICY, September 27, 1997, at 10.

4. *See generally* Michael Eisenstadt, *Enhancing Public Preparedness for Chemical and Biological Terrorism*, POLICYWATCH, April 3, 1998.

outlines options to prevent such events while recognizing the legal complexities of that task, and organizes responses in a manner respectful of the rule of law.[5]

Fourth, lawyers have a crucial role, not to hold a grand debate over a single over-arching question, but to clarify and strengthen the legal rules pertaining to preventing catastrophic terrorism, or, if prevention fails, responding to a terrible event. By joining the planning process, lawyers can focus policy analysis so as to harmonize the pursuit of security with the preservation of civil liberties. Inquiry should focus on five issues: (1) Which parts of government can exercise how much authority, and what limits apply to that authority? (2) What should be the military's role in responding to terrorist events? (3) What regulatory controls of materials and technologies may deny access to weapons capabilities? (4) How can the international community, through treaty-making, cooperatively address catastrophic terrorist threats? and (5) How might the private sector cooperate in counter-terrorism, and what protective boundaries should be established for individual privacy and property rights?

I. ORGANIZATION OF THE FEDERAL GOVERNMENT

Senior government officials, including the President, have often warned about the catastrophic terrorism threat, but is the federal government optimally organized to detect and prevent catastrophic terrorist activities? Two somewhat converse issues arise in this context because Americans want to be protected without sacrificing liberty: (1) Are the many relevant agencies of the federal government coordinating their efforts efficiently in order to maximize protection, detection, investigation, and remediation capabilities? and (2) Are appropriate controls in place to forestall over-reaching of authority?

According to recent analyses, current governmental efforts are largely uncoordinated. Relevant federal and state regulators, law enforcement, intelligence, emergency preparedness and management, defense and other communities formulate policies to defend against and

5. As a recent analysis of bioterrorism concluded: The development of a clearly articulated, comprehensive strategy to defend against bioterrorism must be based on an accurate threat assessment, prudent allocation of resources, and respect for the rule of law. If properly implemented and sustained, this approach could help deter terrorists and sponsors of state terrorism who otherwise would consider biological attacks. Conversely, the perception that the United States is poorly prepared to cope with bioterrorism is likely to encourage groups to exploit this strategic vulnerability. James H. Anderson, Ph.D., *Microbes and Mass Casualties: Defending America Against Bioterrorism*, THE HERITAGE FOUNDATION BACKGROUNDER, May 28, 1998, at No. 1182.

respond to threats, but they do so virtually independently. Vital information is not currently shared between government sectors in ways that promote a more complete understanding of catastrophic terrorist risks.[6]

Until 1998, the Department of State coordinated the federal government's international anti-terrorism efforts,[7] reflecting a supposition that terrorism was a "foreign" phenomenon best addressed through diplomatic channels. The World Trade Center and Oklahoma City bombings shattered that supposition, and increasing notoriety of hate groups focused law enforcement attention on domestic terrorism risks. Moreover, at the bureaucratic level, having the State Department in charge meant that there could be confusion among agencies as to who had primary responsibility over certain issues and situations. Clearly, the Attorney General has authority, as the nation's chief law enforcement officer, over any required federal response to domestic terrorism. Elements of the response may require support of the defense, emergency response, intelligence and diplomatic agencies, as well as other agencies within government. Yet under the previous system, FBI activities, obviously the foundation of any domestic anti-terrorism effort,[8] were subject to the authority of the Attorney General while the State Department, a co-equal part of the Executive Branch which was viewed as having less familiarity with the requirements of domestic crime fighting, had policy coordination responsibilities.

Another potential quandary for State Department supervision concerned counter-terrorism's need for rapid and systematic information-sharing among myriad agencies: the Departments of State, Treasury,

---

6. *Id.*

7. *See* Presidential Decision Directive No. 39 (1995).

8. The FBI is the lead agency for combating domestic terrorism and a key supporting agency for combating international terrorism. From fiscal years 1995 to 1998, FBI counter-terrorism resources more than doubled, increasing from about $256 million in FY 1995 to about $581 million in FY 1998. In total, from 1995 to July 31, 1998, the FBI had allocated an estimated $1.6 billion to carry out its counter-terrorism mission; about $609 million is allocated for the FBI's counterterrorism mission in FY 1999. *See* GAO Report, *Combating Terrorism—FBI's Use of Federal Funds for Counterterrorism-Related Activities (FY's 1995–98)*, GAO/GGD 99-7, (1998). The FBI's "counterterrorism" activities include: (1) Preventive and crisis management efforts to detect and investigate terrorism against U.S. persons and property, both in the United Sates and abroad; (2) Forensic and other support functions, and (3) Leadership of joint terrorism task forces and participation in interagency working groups. The FBI manages standing Joint Terrorism Task Forces in 18 cities to facilitate exchanges of intelligence and coordinate activities among law enforcement personnel. The FBI is a member of the Interagency Intelligence Committee on Terrorism that enhances the processing, analysis, and distribution of foreign intelligence information by sharing information on the terrorist activities and assessing indications of terrorist threats. *See* Legal Foundations, The Federal Legal Landscape, Report 2 of 12, Report to the President's Commission on Critical Infrastructure Protection, at 18–19 (1997) (visited March 30, 1999); <http://www.pccip.gov/report_index.html>.

Energy, and Defense, as well as the FBI and FEMA. Moreover, counter-terrorism uniquely requires interaction between domestic law enforcement and international intelligence, and there is a clear need to have required planning capabilities and response authorities available directly to the White House. Placing the State Department between and above the CIA (and other intelligence agencies) and the FBI, and between those agencies and the White House, suggests a less-than-optimal order. Moreover, information-sharing must be coordinated between the entire federal government and state and local governments. Thus, there should be an official in charge of combatting terrorism that is above any specific Executive agency capable or coordinating the federal government's efforts to work uniformly with other nations as well as with state and local governments.

On May 22, 1998, President Clinton announced Presidential Decision Directive 62, establishing the National Coordinator for Security, Infrastructure Protection and Counter-Terrorism within the National Security Council.[9] Richard Clarke was named the first National Coordinator with responsibility to create a "new and systematic approach to fighting the terrorist threat of the next century."[10] Elevating coordination to the NSC clearly enables resolution of many potential problems. As National Coordinator, Clarke has the final word to resolve inter-agency confusion or conflict on an instance-by-instance basis; elevating coordination to the NSC reduces the risk of inappropriately meshing different types of governmental activity having different scopes of authority.[11]

PDD-62 establishes a comprehensive strategy for military preparedness and response, allocating $300 million for chemical-biological defense, and $100 million to provide diagnostic, detection, and protective equipment to local and state agencies. The primary component of this strategy is enhanced communication and coordination among federal and local government as well as international organizations and foreign governments. Clarke has implemented a four-part program: (1) coordinating local agencies; (2) coordinating federal agencies; (3) detecting and intercepting the flow of weapons and equipment that may be

9. *See* Presidential Decision Directive No. 62 (1998) (visited March 30, 1999);<http://www.fas.org/irp/offdocs/pdd-62.htm>.

10. *Id.*

11. On the same day, the President announced PDD-63, Presidential Decision Directive No. 63 (1998) (visited March 30, 1999) <http://www.fas.org/irp/offdocs/pdd-63.htm>., which focuses on enhancing the nation's capability to protect the security and reliability of critical infrastructures. PDD No. 63 defines critical infrastructures as those physical and cyber-based systems that are so vital that their incapacity or destruction would have a traumatic or debilitating impact on the United States. These systems generally include electrical power, gas and oil, telecommunications, banking and finance, transportation, vital government operations, emergency services, and water supply systems.

used by terrorist groups; and (4) disrupting terrorist organizations. Clarke also announced that the government reserves the right to use first strikes in self-defense against terrorist groups.

It may be reasonable to presume that these recent changes are responsive to concerns over the government's capability to coordinate its activities to prevent catastrophic terrorism and to respond if prevention fails. However, serious questions have to be asked about converse concerns: the risk of over-reaching of authority. The new National Coordinator is more an administrator than an advisor, with responsibility to assign roles to 18 federal departments and agencies, including the FBI, CIA, and the Pentagon, and to coordinate the law enforcement efforts of state and local governments. This responsibility includes authority to allocate tasks among governmental agencies and to supervise their budget requests with regard to counter-terrorism.[12]

The NSC was created in 1947 to be the President's chief advisory group on matters of international security; its role is to prepare policies to address foreign threats. Despite its role as a White House foreign policy advisory office, unfortunately, the NSC has a history of having exceeded legal limitations on its mandate. Moreover, the NSC is subject to only minimal congressional or judicial oversight.[13] The predominant check on the NSC is Presidential oversight. In the domain of foreign affairs, the President's authority is greatest, and doctrines of executive privilege are significant; by contrast, legal concerns over civil liberties are somewhat attenuated. There is a concern here that the NSC might intrude on constitutional rights and civil liberties of Americans, and that such intrusion would not be subject to accountability. Iran-Contra suggests that a more elaborate set of legal rules may be appropriate. No aspersions need be cast at Richard Clarke to be concerned that a new Administration might appoint a new National Coordinator who recognizes the absence of limitations on his/her authority and who takes advantage of the public trust.

II. ROLE OF THE MILITARY IN RESPONDING TO TERRORIST EVENTS

Perhaps no issue regarding catastrophic terrorism has raised as much heated controversy as the role of the military and the CIA. In fact, there is not one issue here but many issues intertwined. On these mat-

12. *See* Philip Gold, *Limitations of the NSC*, WASH. TIMES, March 30, 1998, at A19.

13. For a general discussion of pertinent issues, see Jay S. Bybee, *Advising the President: Separation of Powers and the Federal Advisory Committee Act*, 104 YALE L. J. 51 (1994).

ters, the focus should be more normative than descriptive; that is, with regard to catastrophic terrorism, it is less significant what are the rules pertaining to involvement with domestic law enforcement than what those rules should be if an unparalleled cataclysm occurs in America. It may be that, for a variety of reasons, reforms should be propounded to enable the military and the CIA to become more actively involved in specific law enforcement activities. In the context of catastrophic terrorism, involvement of the military and/or the CIA may be the best way to forestall rampant chaos and protect individual rights and property.

The legality of the military's role in carrying out domestic missions has, of course, been extensively litigated and discussed. The Posse Comitatus Act prohibits the military from executing the role of law enforcement; military personnel may not "execute the laws."[14] Four questions are relevant to application of that prohibition. First, is the activity directed at foreign or domestic threats? Traditionally, terrorism has been viewed as a foreign threat, but, as discussed above, that view has given way to a new understanding in recent years. A second question is whether the threat, even if domestic, is a crime or is a matter of national security concern. The problem is to define terrorist activity as either a national security threat or crime. Significantly, threats to critical infrastructure are considered national security threats.[15] The third question is whether the military activity is in response to an emergency or does the context allow for a deliberate law enforcement response; the military can act in response to an emergency.[16] Furthermore, immediate action by military commanders may be allowed when serious conditions resulting from a civil emergency may require action to save lives, to prevent human suffering or to mitigate great property damage, and time does not permit prior approval from higher authorities.

The fourth question arises only if the activity is in response to a criminal threat: is the military acting to assist law enforcement or has it taken the lead role? The military may provide passive assistance that is "merely incidental."[17] Yet, the military may provide intelligence gathered during normal operations to federal, state and local law

14. United States Code, 18 U.S.C. § 1385 (1999).

15. *See generally* M.E. Bowman, *The Military Role in Meeting the Threat of Domestic Terrorism*, 39 NAVAL L. REV. 209 (1990).

16. The Disaster Relief section of the U.S.C.A., provides for the assistance of federal agencies to local authorities in the event of natural or man-made emergencies. 42 U.S.C.A § 5121 (1999). This section requires a request to the President for assistance, through FEMA, and a finding that the event is a bona fide emergency. *See generally* Jim Winthrop, *The Oklahoma City Bombing: Immediate Response Authority and Other Military Assistance to Civil Authority (MACA)*, ARMY LAW., July 1997, at 3.

17. People v. Burden, 411 Mich. 56, 303 N.W.2d 444, 447 (1981).

enforcement officials.[18] The military may also furnish equipment for law enforcement use and may provide for that equipment's maintenance and repair.[19] The military may provide training and advising to law enforcement officials.[20] Finally, military personnel may be used to supplement law enforcement effort at the request of heads of agencies responsible for enforcing federal drug laws, immigration laws, and customs laws.[21]

There are difficulties in applying these standards in the context of catastrophic terrorism because of jurisdictional challenges which are further complicated by the fact that we may not know the source of an attack—domestic or foreign. We may not know the identity or motives of the attacker—individual or group, terrorist, criminal, or government. Nor may we initially know the magnitude of the attack. We may not even know if ours is the only nation experiencing the attack. Can we even pretend to distinguish between a foreign or a domestic threat when the attacker is using the Internet to electronically dismantle key infrastructure sectors?[22]

At the prevention stage, it would seem to be illegal to use the military to infiltrate subversive organizations or to conduct domestic surveillance, but it would seem within the scope of the military's authority to help state and local law enforcement officials as well as private industry to apply systems defense measures. Training, expert advice, operating and maintaining equipment, and transfer of information are not within the Posse Comitatus prohibition. Also permitted are other actions that do not subject civilians to the use of military power that is regulatory, prescriptive, or compulsory. A significant role for the military will be in protecting borders and monitoring customs operations.

Intelligence-gathering raises unique issues. Seemingly not controversial would be gathering intelligence about foreign terrorist activities, but gathering intelligence on foreign-sponsored terrorist activities within the United States is more ambiguous. The CIA does not have police, subpoena, law enforcement, or internal security powers. However, a recent amendment to the National Security Act allows the Intelligence Community to collect information abroad about non-U.S. persons in order to support a U.S. law enforcement or counterintelli-

---

18. *See* 10 U.S.C. § 371(a)(1994). [A's text] This may include operational intelligence such as movements of air and sea traffic, or evidence gathered during criminal investigations conducted within military jurisdiction.

19. *See* 10 U.S.C. § 372 (1997).

20. 10 U.S.C. § 373 (1994).

21. 10 U.S.C. § 374 (1994).

22. *See generally* Allan R. Stein, *The Unexceptional Problem of Jurisdiction in Cyberspace*, 32 INT'L LAW. 1167 (1998).

gence investigation upon request of a U.S. law enforcement agency.[23] If the investigation or gathering of intelligence and counterintelligence is to take place within the United States, the CIA efforts must be coordinated with the FBI. It is worth considering whether the demands of international exchanges of information and mutual legal cooperation suggest an enhanced role for the U.S. intelligence community, and, if so, how that community's activities should be coordinated with domestic law enforcement agencies.[24] Some experts have recently proposed establishment of a new National Terrorism Intelligence Center to deal with these issues.[25]

After a catastrophic terrorist event, the military's role would be decidedly greater. No serious controversy attends the deployment of expert military teams, trained to detect and cope with chemical or biological agents, to respond to a terrorist event, and to help minimize loss of life. Nor does serious controversy attend deployment of Army Corps of Engineers to work with only Federal authorities (e.g. FEMA) to repair infrastructure and alleviate property damage.

The military's role in maintaining civil order if a catastrophic terrorist event were to occur with thousands or even tens of thousands of casualties may be so crucial that doctrines such as posse comitatus may diminish to trifling concerns. If government agencies are totally incapacitated by a terrorist event, the military may step in to provide all government services, including law enforcement, without waiting for specific authorization or instructions from the seat of the government. The military is authorized to aid law enforcement in cases of sudden and unexpected invasion, insurrection, or riot that endangers the public property of the U.S., or in cases of attempted or threatened robbery or interruption of the U.S. mails, or other equal emergency so imminent as to prohibit communication. The protection of life and property in the

---

23. Executive Order No. 12333 specifies the scope of the intelligence activities in which the CIA may engage and limits those activities to the gathering of "foreign intelligence" (information relating to the capabilities, intentions and activities of foreign powers, organizations or persons) and "counterintelligence" (information gathered and activities conducted to protect against espionage, other intelligence activities, sabotage, or assassinations conducted for or on behalf of foreign powers, organizations or persons). Exec. Order No. 12333, 1981 Pub. Papers 1128 (1981), *reprinted in* 50 U.S.C. § 403 (1996). For a discussion of the CIA's Counterterrorist Center, see Vernon Loeb, *Where the CIA Wages Its New World War; Counterterrorist Center Makes Many Arrests, Pursues Bin Laden With Aid of FBI, NSA*, WASH. POST, September 9, 1998, at A1.

24. The Nunn-Lugar-Domenici legislation included in the Department of Defense Authorization for 1997 sets out a comprehensive plan for dealing with terrorist threats from WMD. *President's Report on Government Capabilities to Respond to Terrorist Incidents Involving Weapons of Mass Destruction*, 33 WEEKLY COMP. PRES. DOC. 256 (Feb. 26, 1997).

25. Ashton Carter, John Deutch, & Philip Zelikow, *Catastrophic Terrorism; Tackling the New Danger*, FOREIGN AFFAIRS, Nov.–Dec. 1998, at 80.

wake of a catastrophic terrorist event may require the search and seizure of private property without warrants, arrest and detention, and temporary deprivation of fundamental rights. In any event, there would be few legal remedies for abuses committed by military personnel under these circumstances.

The most difficult issues pertain to investigating responsibility for an event and apprehending suspects. No responsible assertion has been made that the military or CIA should take control of investigating and apprehending domestic criminal suspects. The FBI has the authority to investigate all crimes against the U.S. It is the lead agency in all crimes for which it has concurrent or primary jurisdiction and which involve terrorist activities. The FBI has developed plans to deal with unconventional crisis situations including a Nuclear Terrorism Response Plan, a Chemical/Biological Incident Contingency Plan, the Critical Response Group, and the Hostage Rescue Team. Section 1416 of the 1997 National Defense Authorization Act[26] permits the Secretary of Defense to provide assistance to the Department of Justice in emergency situations involving a biological or chemical weapon. While the statute prohibits the direct participation of military personnel in most cases, it authorizes direct participation in arrest, search and seizure, and intelligence collection when necessary to save human life and civilian authorities are unable to take the required action, as long as the action is otherwise authorized by law.

The Disaster Relief Act[27] authorizes the federal government to provide an orderly and continuing means of assistance to State and local governments in carrying out their responsibilities to alleviate the suffering and damage which result from disasters. Then, through the state and local agencies, assistance may be available to private concerns. In terms of direct aid, the Stafford Act provides funding and other assistance authority only to public entities and facilities and private nonprofit facilities. Accordingly, the Federal Response Plan establishes a framework for mobilizing a coordinated response to catastrophes. The Terrorism Annex has recently been added to the FRP to address incidents involving weapons of mass destruction (WMD). The authority of the military to engage in key asset protection operations has been judicially upheld.[28] Moreover, the military has a recognized role in disaster relief operations, including: battling fires, building levees to protect against flood waters, providing emergency electricity, assisting rescue operations, and debris removal.

---

26. *See* 10 U.S.C.A § 382 (1994).
27. *See* 42 U.S.C.A §§ 5121–5204 (1999).
28. In re Debs, 158 U.S. 564 (1895), *see also* Mitchell v. Harmony, 59 U.S. 115 (1951).

The military's authority would seem, therefore, to be sufficient to address most responsibilities that would befall it in the event of a catastrophic terrorist event. The issue is, however, whether that authority could be abused. Clearly, the military is differently trained than domestic law enforcement officials with implications for the use of force and for the collection of evidence. In an emergency, involvement of the military in maintaining order, sifting through evidence, and helping apprehend culprits could lead to an overreaching of authority, and perhaps a hasty threat to liberty.[29] This possibility is compounded by the coordinating role of the National Security Council, discussed above, which is even less constrained against overreaching. In the chaos that would follow a catastrophe, might the National Security Council authorize military activity that would intrude on American's civil liberties and even on their basic rights to life and liberty? Certainly the risk is improbable, but just as certainly there appear to be few significant legal protections against such a risk and virtually no means of accountability.

Any potential problems concerning the role of the military and the CIA regarding catastrophic terrorism should be worked out in advance and which in a manner which anticipates as many contingencies as possible. Memoranda of Understanding (MOU) between the Department of Justice and the CIA or Department of Defense, separately or with the NSC, should analyze both the myriad types of attacks as well as the distinct phases of involvement, specifying as precisely as possible the respective roles of military and intelligence and providing for a clear transfer of authority as the crisis passes through various stages from the initial emergency to the post-crisis and investigative stages. Since the military's most crucial counter-terrorism role would seem to be in the immediate aftermath of terrorist events, what is meant by an emergency should be circumscribed and the point at which law enforcement agencies should assume authority over situations involving terrorist events should be defined. To the maximum extent consistent with national security concerns, MOUs should be shared with Congress, state and local officials, and the public; if an event occurs, responsible people throughout all sectors of society should know the hierarchy of authority and the rules of engagement.

29. *See* Matthew Carlton Hammond, *Note: The Posse Comitatus Act: A Principle in Need of Renewal*, 75 WASH. U. L. Q. 953, 953 (1997).

III. CONTROL OF PRECURSORS—DENIAL OF ACCESS TO WEAPONS CAPABILITIES

A second set of questions may be addressed to the sufficiency and efficiency of legal regulation of weapons agents and their precursors under domestic law. What legal impediments might complicate a terrorist's ability to produce catastrophic agents? Are monitoring systems in place that raise the likelihood of detecting clandestine production? Are storage systems for such agents securely protected against theft? Can these agents be acquired or is acquisition dependent on legal permission which would, at minimum, provide an ability to trace large-scale purchases? Are systems in place to limit the transportation of significant quantities of dangerous agents?

The regulatory regime applicable to nuclear materials should serve as a model. The entire process of making fissile materials, from mining uranium to processing that ore into fuel, is regulated by federal law. Any attempt to develop a productive capability without proper licenses is manifestly illegal and should trigger a variety of government oversight measures. Creation of a clandestine uranium enrichment facility or a chemical reprocessing plant to recover plutonium from spent fuel would be certainly illegal and virtually impossible. Storage of nuclear materials is extensively regulated, and beating security systems would unquestionably invoke a massive law enforcement response. Possession or acquisition of nuclear materials without a license is illegal, without regard to how the accused intends to use those materials. Finally, transportation of nuclear materials is subject to strict federal standards.

The picture changes considerably with regard to chemical precursors. Many of the substances that might be used to make a chemical weapon are environmentally regulated under the Toxic Substances Control Act (TSCA); the EPA Administrator has authority to prohibit the manufacturing, processing, or distribution in commerce of substances that present an unreasonable risk of injury to health or the environment.[30] Under the Federal Insecticide, Fungicide, and Rodenticide Act (FIFRA), the EPA has comprehensive regulatory authority over many of the substances that could be used to make chemical weapons.[31] Primarily, these environmental statutes regulate the introduction of potentially harmful chemicals into the marketplace; a license is re-

30. 15 U.S.C. § 2605 (1994). The Administrator may also regulate the production of such substances, require that records be maintained, regulate chemical use and distribution, require that manufacturers or processors give notice of risks of injury, and recommend quality control measures. *Id.*

31. 7 U.S.C. §§ 136–136y (1994).

quired, without which marketing is prohibited. For these statutory powers to apply to all chemical weapons agents and serve all relevant purposes, the EPA must regulate those chemicals for anti-terrorism as well as environmental purposes. These environmental laws do not, per se, prohibit the production of these chemicals.

With enactment in December 1998 of the Chemical Weapons Convention Implementation Act (CWCIA),[32] production of chemicals listed in the Chemical Weapons Convention[33] (CWC) is not illegal, although production over stipulated concentrations and quantities triggers reporting obligations, and failure to report or improper reporting is illegal.[34] Unlike most other CWC States Parties, the U.S. has not even enacted a licensing system for "Schedule 1 chemicals" (the chemical weapons agents and precursors most strictly regulated under the CWC).[35] The CWCIA does promulgate severe penalties, including the death penalty, for use of chemical weapons.[36] However, the storage of

---

32. 22 U.S.C.A. §§ 6701–6771 (1998).

33. The Convention on the Prohibition of the Development, Production, Stockpiling and Use of Chemical Weapons and on Their Destruction, Jan. 13, 1993, 32 I.L.M. 800 (entered into force April 29, 1997). As of January 1999, the CWC has over 170 signatory States.

34. Willful failure or refusal to establish or maintain any required record or to submit information to the government or to permit access to any record is illegal. Violators may be required to pay a civil penalty up to $5,000 for each violation. Chemical Weapons Convention Implementation Act [CWCIA] § 501 (a)(1)(B). Anyone knowingly violating these requirements shall also be criminally fined or imprisoned up to one year, or both. CWCIA § 501(b).

35. The lethal Schedule 1 chemicals that present the greatest risk to the CWC's object and purpose may be produced only in limited quantities at specific types of facilities. States Parties may produce Schedule 1 chemicals at only two types of facilities: at a single "small-scale" facility "approved by the State Party" and at "other facilities" that produce only a limited quantity of Schedule 1 chemicals and for only limited purposes. "Production of Schedule 1 chemicals in aggregate quantities not exceeding 10 kg per year may be carried out for protective purposes at one facility outside a single small-scale facility." CWC Verification Annex, pt. VI, (C)(8), (10). Protective purposes are "those purposes directly related to protection against toxic chemicals and to protection against chemical weapons." *Id.* at Art. II, ¶ 9(b). In addition, at facilities approved by the State Party, "[p]roduction of Schedule 1 chemicals in quantities of more than 100 g per year may be carried out for research, medical or pharmaceutical purposes outside a single small scale facility in aggregate quantities not exceeding 10 kg per year per facility." Finally, "[s]ynthesis of Schedule 1 chemicals for research, medical or pharmaceutical purposes, but not for protective purposes, may be carried out at laboratories in aggregate quantities less than 100 g per year per facility." CWC Verification Annex, pt. VI, (C)(11)–(12). "Each State Party, during production . . . shall assign the highest priority to ensuring the safety of people and to protecting the environment." Further, "[e]ach State Party shall conduct such production in accordance with its national standards for safety and emissions." *Id.* at pt VI, (C)(7).

36. The CWCIA adds a new Chapter 11B—Chemical Weapons to Title 18 of the United States Code. It is now unlawful to knowingly "develop, produce, otherwise acquire, transfer directly or indirectly, receive, stockpile, retain, own, possess, or use, or threaten to use, any chemical weapon" or assist or induce anyone else or attempt or conspire to do so. 18 U.S.C.A § 229(a) (1998). A violator will be fined, imprisoned for any term of years, or both;

chemicals is regulated only to the extent of preventing environmentally-threatening releases; security against theft is a matter left to each chemical firm. Sale of hazardous chemicals may come within the scope of various environmental laws and under the CWCIA must be reported, but it is not illegal to sell weapons agents to an unlicensed party. Interstate transport of many chemicals is regulated, but this regulation is not designed to detect movement for terrorist purposes nor are reporting obligations sufficiently comprehensive to trigger law enforcement.[37]

The regulatory system for chemicals is positively encyclopedic when compared to the system that controls deadly biological agents. Under the Biological Weapons Anti-Terrorism Act of 1989, as amended in 1996,[38] use of biological agents to kill or injure is criminalized; knowing possession, transfer, or acquisition of biological agents for use as a weapon is also criminalized.[39] Biological agents are defined broadly to encompass any micro-organism, virus, infectious substance, or biological product, whether created as a result of biotechnology or isolated from nature. Biological agents are also defined as capable of causing: (a) death, disease, or other biological malfunction in a human, an animal, a plant, or another living organism; (b) deterioration of food, water, equipment, supplies, or material of any kind; or (c) deleterious alteration of the environment.[40]

---

if someone dies due to such culpable conduct, the violator will be punished by death or life imprisonment. Also, civil penalties of up to $100,000 per violation may be imposed, and the violator must reimburse the United States for any expenses incurred incident to seizing, transporting, or destroying any property. *Id.* § 229A. Anyone lawfully authorized to deal with chemical weapons pending their destruction or who tries to destroy or seize a chemical weapon in an emergency situation is not thereby culpable. *Id.* § 229 (b).

37. 49 U.S.C.A. § 5103 assigns regulatory authority to define and supervise interstate transport of hazardous materials (including biological and chemical materials). 49 U.S.C.A. § 5301 (1996). For a list of the chemicals/agents that are so regulated, see 49 C.F.R. § 172.101 (1998). For a description of marking requirements for non-bulk transport of hazardous materials, see 49 C.F.R. § 172.301 (1998).

38. 18 U.S.C.A. § 175 (1996). The purpose of this Act is to implement the Biological Weapons Convention and to protect the United States against the threat of biological terrorism.

39. In *U.S v. Baker*, 98 F.3d 330 (8th Cir. 1996), *rehearing and rehearing en banc denied, cert. denied,* 117 S. Ct. 1456, 137 L.Ed.2d 561, the Eight Circuit defined knowledge:

Evidence sustained conviction for knowing possession of ricin, a toxin, for use as a weapon, notwithstanding defendant's statements that he intended to use ricin to kill garden pests and that he did not know who had given it to him; ricin was shown to be extremely toxic, deadly in extremely small quantities, and very difficult to detect, with no known antidote, and to have been popularized as a method of killing people; handwritten note addressed to defendant and found inside coffee can with ricin contained information about dangerousness of contents and precautions to be used in handling it; and defendant admitted to Federal Bureau of Investigation (FBI) that he knew that ricin was dangerous and had to be handled with extreme care.

40. 18 U.S.C. § 178 (1) (A) & (B) (1994).

The statute does not define what constitutes "for use as a weapon," but specifies the alternative. Development, production, transfer, acquisition, retention, or possession of any biological agent, toxin, or delivery system for prophylactic, protective, or other peaceful purpose is legal.[41] The evidentiary showing required to establish that possession is indeed for such legal purposes is unclear and raises difficult legal issues, especially if the suspect is apprehended prior to use. Furthermore, individuals may escape liability if they can show that they were developing antidotes/antibodies against the very organisms they might employ in attack. More significantly, there is a substantially unrestricted market for biological agents so long as it cannot be shown that those agents had no apparent justification for legitimate uses.

No license is needed to obtain many of the agents that have been identified as having ready weapons capabilities. Use of biological materials on humans as well as standards for protection in research facilities are regulated as are packaging standards.[42] Yet, regulation of storage systems is limited to protection against public health-jeopardizing releases and is enforced by OSHA;[43] protection against theft or diversion is wholly ignored. Distribution and transportation of biological agents are astoundingly unregulated; many deadly biological agents can be obtained through the mail. The export of biological agents may only proceed with a license; export control regulations list nearly every biological agent that might be used as a weapon and also specify technology supporting the production of such agents.[44] It is generally prohibited to license these products to countries identified as sponsoring State terrorism, including Cuba, North Korea, Iraq, Iran, Syria, Sudan, and Libya.[45] As to other countries, license applications are considered on a case-by-case basis to determine if permission would contribute to a chemical or biological weapons capability.[46]

In short, the most immediate legal reform to reduce the risk of catastrophic terrorism is comprehensive and effective regulatory controls to govern production, acquisition, and possession of relevant materials and

41. 18 U.S.C. § 175 (B) (1994).

42. 42 U.S.C.A. § 262 (1999) provides requirements for labeling, packaging, containers of biological products, regulated by FDA and HHS.

43. 29 C.F.R. § 1926.25 (1998) deals with OSHA regulation of clean-up following release, disposal of toxic agents. 9 C.F.R. § 114.4 (1998) deals with labeling and storage requirements under USDA. 21 C.F.R. § 864.3250 (1998) specifies containment requirements during transport and storage under HHS.

44. *See* 15 C.F.R. § 742.2 (1998).

45. *See* 15 C.F.R. Pt. 742, Supp. 2 (1998).

46. *See* 15 C.F.R. § 742.2 (1998).

technologies.[47] Although potentially drastic, proposals should be considered to regulate the production and domestic trade of materials and technologies that are essential to catastrophic terrorism. It may be appropriate to institute licensing systems to govern industries that produce or use chemical or biological agents which can be weaponized. The costs of such regulation may be weighty and would tend to fall on legitimate commercial enterprises; mechanisms to both minimize and to spread that burden through sensitive and cooperative policies that affect the private sector (discussed below) must therefore be considered. At minimum, new legislation is needed to track the domestic distribution of chemical and biological agents and to criminalize possession except by commercial or research entities.

A regulatory system over the production, possession, and use of catastrophic agents must be braced by a criminal justice system that strictly punishes offenders. All violations, including but not limited to actual attacks, should be treated as severe crimes, regardless of where they originated or the purpose of the attack. The Biological Weapons Anti-Terrorism Act provides for significant penalties for use, attempt, threat, or conspiracy to use biological weapons.[48] However, current Sentencing Guidelines do not adequately address the severity of consequential damages arising from mere possession of deadly agents; a possibility exists of disproportionately light sentences.[49] Notably, Larry Wayne Harris received only 5 months probation for ordering bubonic plague by mail, after he plead guilty for mail fraud. When he subsequently was accused of possession of anthrax, he did not receive jail time for the offense because all he had was a harmless animal vaccine, but he later served time for having violated his probation from the bubonic plague.[50] The Sentencing Commission should consider expanding

47. *U.S. Counterterrorism Policy:* Hearing of the Senate Judiciary Committee, Capital Hill Hearing with Defense Department Personnel, September 3, 1998 (testimony by FBI director, Louis Freeh).

48. 18 U.S.C. § 175 (1998) provides for a fine or for imprisonment for life or any term of years or both.

49. *See* Legal Foundations, Adequacy of Criminal Law and Procedure, Report 7 of 12, Report to the President's Commission on Critical Infrastructure Protection, (1997) (visited March 30, 1999);<http://www.pccip.gov/report_index.html>.

50. Robert Roth, *Harris Pleads Guilty, Is Free; Anthrax Case*, COLUMBUS DISPATCH, March 25, 1998, at 01A; *Anthrax Suspect's Parole Extended*, FACTS ON FILE WORLD NEWS DIGEST, October 15, 1998, at 730 E3. *See generally Time to Tighten Bioterrorism Laws; Criminals Won't Wait Around for Congress to Take Action on Proposed Five-Year Plan*, FULTON CTY. DAILY REPT., July 23, 1998. Earlier this year, the Nevada Senate, where Harris was arrested, approved a bill making it a felony to use or threaten to use anthrax and other biological weapons. Sean Whaley, *Senate Passes Bill That Would Make Using Biological Weapons a Felony*, LAS VEGAS REV.-JOURNAL, February 13, 1999, at 6B.

coverage of its Guidelines to better address the implications of possession of biological and chemical agents.

IV. International Non-Proliferation Conventions

Ultimately, catastrophic terrorism is a global threat, and counter-terrorism efforts must be global to have any serious chance of success. Negotiation of multilateral conventions is therefore essential to establish standards of behavior as well as cooperative mechanisms to control deadly agents and investigate potential threats. Unfortunately, current negotiations are mired in antiquated non-proliferation concepts that are substantially unresponsive to catastrophic terrorist threats.

Non-proliferation efforts focus on States on the premise that deployment of weapons of mass destruction in military arsenals will lead to their use in armed conflict with catastrophic consequences. Certainly, States' deployment of weapons have encouraged adversary States to deploy similar weapons, fueling arms races. In order to prevent proliferation of catastrophic weapons, critical materials and technologies in the process of making those weapons (choke points) are identified, and entities that are involved with those choke points are monitored by imposing reporting requirements and, perhaps, on-site inspections to verify that they are not involved in illicit weapons activities. Since making weapons for militarily significant purposes demands an enormous commitment of resources, strict verification of critical materials and technologies enables international officials to detect military programs.

Verification is not foolproof, but, at minimum, the costs of a clandestine weapons program become exorbitant. Most States know that pursuit of a clandestine weapons program entails massive expenditures and that the probability of detection is high. Detection of a program carries seriously adverse political ramifications of condemnation and perhaps sanctions. At minimum, an adversary State may respond with a military buildup of its own. Accordingly, most States refrain from developing a prohibited weapons capability.

Closely related is the fact that most States do not want a prohibited weapons capability; the motive to obtain such weapons is driven, in part, by the perception that their neighbors and adversaries are acquiring them and will therefore be able to threaten destruction. Verified non-proliferation commitments serve to break this cycle by providing evidence that other States are fulfilling their obligations and by confirming that prohibited activities are not taking place. Most States gain confidence that their security does not require catastrophic weapons, and the incentive to develop them diminishes, thereby further strengthening the

international prohibitory norm. Even though not 100% effective, non-proliferation efforts make sense: they enable the international community to focus on the handful of proliferating States with the assurance that nearly all the world is not, in fact, threatening to develop a clandestine capability.[51]

The question that must be asked is whether this non-proliferation construct applies to the threat of catastrophic terrorism—that is, does it reduce the risk that sub-national actors will gain the capability to produce/obtain terror-significant quantities of weapons, and does it pose a realistic potential for detecting such activity? Non-proliferation verification will go far toward proving that legitimate activities are indeed legitimate, but verification will not do much to uncover illicit catastrophic weapons activities undertaken either by a pariah State or a sub-national criminal organization. Non-proliferation is not built for that purpose, and therefore will not have that capability. Even under the most fortuitous circumstances, strengthened international conventions will enable everyone to know that commercial facilities in the overwhelming majority of States are definitely not engaged in weapons-related activities; we will not know, however, about the few isolated and disguised sites where mass death is concocted.

The capability to make lethal chemical or biological agents is so ubiquitous that to concentrate verification measures where production capability is demonstrable verges on the absurd. If lethal agents can be made virtually anywhere, then why would anyone intending to produce catastrophic devices make use of a facility that is monitored because of its sizeable production of biological, pharmaceutical, or chemical agents? Put simply, if catastrophic agents can be produced anywhere, what is gained by verifying that legitimate enterprises are not engaged in illegal activity? That information tells us nothing about where terrorists are producing lethal agents clandestinely, which is the most needed information.

The patently obvious fact is that a group of moderately trained technicians using commonplace equipment can brew sufficient agents to kill thousands, and any currently-considered weapons control verification system will be unaware until the consequences are apparent. Terrorists or criminals can, without difficulty, gain access to powerful agents of mass death. If those agents can be put to remunerative or attention-enhancing use, then a control system to verify that those agents are not part of States' military capabilities is inapposite.

---

51. *See* Barry Kellman, *International Consensus and States Non-Parties*, *in* VOLUME III, ARMS CONTROL AND DISARMAMENT LAW (Julie Dahlitz, ed., 1996).

A far-reaching international law enforcement effort is needed to investigate suspicious activity and apprehend miscreants.[52] Multilateral negotiations to develop that effort, not re-configuring non-proliferation modalities, should focus on at least seven objectives.

A. *Criminalizing Possession of Weapons Agents*

First, handling precursor agents or undertaking activities relevant to developing a catastrophic terrorist threat should be defined as an international crime, excepting authorized activities pursuant to a license. Activity that constitutes an international crime affects world peace and security or significantly offends the basic values of humanity; accordingly, powerful international law modalities apply to those crimes. Currently, there is no unified international convention on terrorism.[53] Unfortunately, the international legal response to terrorism does not address adequately trans-national catastrophic terrorism, and its treatment as an international crime could be reinforced. There are gaps in coverage, and existing modalities of cooperation fall far short of the integrated international regime that should be established.[54] Nations should assume a corollary obligation to treat the same behavior as crime under domestic law. Uniform enactment of clear and strict penalties, the jurisdictional scope of the law, and the law's application to corporate conduct could undermine the stability of criminal organizations.

Recently, the United Nations General Assembly adopted the International Convention for the Suppression of Terrorist Bombings making it an international crime to bomb a public or government place or a transportation system or an infrastructure facility with the intent to cause death, injury, or destruction.[55] The Convention also criminalizes attempt, conspiracy, or assistance to others to accomplish a prohibited

---

52. *See generally* M. Cherif Bassiouni, *A Comprehensive Strategic Approach on International Cooperation for the Prevention, Control and Suppression of International and Transnational Criminality*, 15 NOVA L. REV. 353 (1991).

53. The international legal response to terrorism has been limited to prohibiting terrorist conduct, preventing preparations for discrete terrorist offenses, and promoting interstate cooperation in the investigation, extradition and/or prosecution of offenders. *See* John F. Murphy, *Cooperative International Arrangements: Prevention of Nuclear Terrorism and the Extradition and Prosecution of Terrorists*, *in* PREVENTING NUCLEAR TERRORISM 368–70 (Paul Levanthal & Yonah Alexander eds., 1987).

54. *See* Barry Kellman & David S. Gualtieri, *Barricading the Nuclear Window—A Legal Regime to Curtail Nuclear Smuggling*, 1996 U. ILL. L. REV. 667, 667 (1996).

55. *International Convention for the Suppression of Terrorist Bombings*, G.A. Res. 52/164, U.N. GAOR, 52nd Sess., Agenda Item 152, U.N. Doc. A/RES/52/164 (1998) [hereinafter Terrorist Bombing Convention]. The Convention will enter into force thirty days after the deposit of the twenty-second instrument of ratification. Terrorist Bombing Convention, art. 22.

act. Each State Party must criminalize these offenses under its domestic law; such acts may not be justified "by considerations of a political, philosophical, ideological, racial, ethnic, religious or other similar nature and are punished by penalties consistent with their grave nature."[56] Significantly, each State Party must investigate facts pertaining to alleged offenses, and, if appropriate, ensure that person's prosecution or extradition.[57] Further provisions specify legal assistance requirements, obligations to extradite, and procedural rights of accused offenders. Notably, no offense within the meaning of the Convention may be viewed as a political offense.[58]

A group of experts led by Harvard biologist Matthew Meselson advocates a convention that would make the production of biological weapons an international crime, prosecutable anywhere.[59] This proposal marks a significant advance in treatment of catastrophic terrorism, but it is limited in two important respects: 1) it applies only to biological weapons terrorism and not the full range of activities that could inflict catastrophic harm; and 2) it does not specify the full range of legal modalities that States should adopt to enforce its proscriptions.

B. *Preventing Diversion of Weapons Materials*

The international community should implement measures to protect against unlawful diversion of weapons materials. These measures, similar to those discussed above in the domestic context, should apply to the storage and transportation of these materials and could entail extensive reporting obligations whenever such material is sold or moved. In regard to nuclear materials, the Convention on the Physical Protection of Nuclear Materials[60] obligates each State Party to take appropriate steps within the framework of its national law to protect nuclear civilian (but not military) material to minimize the risk of unauthorized removal or sabotage of nuclear materials. This Convention has substantial gaps and limitations;[61] more important, no comparable obligations whatsoever apply to chemical or biological materials.

---

56. *Id.*, art. 5.

57. *Id.*, art. 7(2).

58. *Id.*, art. 11.

59. *See* Carter, Deutch, & Zelikow, *supra* note 1, at 80.

60. Convention on the Physical Protection of Nuclear Material, Mar. 3, 1980, 18 I.L.M. 1419 (entered into force Feb. 8, 1987). The treaty is codified in the United States at 18 U.S.C. § 831 (1994) and 22 U.S.C. § 4831 (1994).

61. Barry Kellman & David S. Gualtieri, *Barricading the Nuclear Window—A Legal Regime to Curtail Nuclear Smuggling*, 1996 U. ILL. L. REV. 667, 701–704, 714–717 (1996).

C. *Coordinating National Police Forces*

Perhaps most important, mechanisms should be established to coordinate activities among States' police forces and officials of relevant agencies. Special computer linkages could afford investigators instant access to information about suspicious activity in other States. Institutional barriers to rapid communication and cooperation should be erased; a new trans-national agency or office could be established to coordinate investigations and responses. Because a State's unilateral conduct of law enforcement measures within another State would transgress international law and heighten diplomatic tensions, most governments demand that law enforcement actions be conducted by local police authorities. Thus it is crucial to strengthen international police capabilities pursuant to a convention that regularizes interactions among police in the field and overcomes the unpredictability and inadequacies inherent in domestic enforcement techniques.[62]

D. *Controlling and Tracing Transportation Networks*

Transportation networks should be strictly controlled with capabilities to follow relevant materials and equipment. Currently, legitimately produced nuclear, chemical, or biological material that is smuggled or stolen cannot be traced to a specific source. The inability to trace material complicates law enforcement investigations of criminal organizations responsible for diversion. An international database should be prepared on catastrophic agents to enable law enforcement officials to have a common baseline of information.[63] If possible, these agents could be tagged or marked so that they could be traced back to their source if later uncovered during an investigation.

E. *Preventing Trans-border Movement of Catastrophic Agents*

Improved border controls and customs enforcement could help stanch catastrophic terrorism by preventing the movement of dangerous

---

62. Interpol is regarded as the premier motivator for international police cooperation. It provides a formal association for police worldwide which helps establish personal relationships vital for speedy cooperation and cutting through red tape. Interpol also helps local police to stay abreast of new enforcement tools and techniques through internationally disseminated notices. *See generally* Mary Jo Grotenroch, *Interpol's Role in International Law Enforcement*, *in* LEGAL RESPONSES TO INTERNATIONAL TERRORISM 375 (M. Cherif Bassiouni ed., 1988).

63. The International Atomic Energy Agency maintains a database on nuclear material, although tagging systems are not as effective as technology would permit. *See generally* Steve Fetter, *Nuclear Archeology: Verifying Declarations of Fissile-Material Reduction*, 3 SCI. & GLOBAL SECURITY 236 (1993). No analogous systems exist for chemical or biological agents.

items and persons from sites where weapons may be produced or acquired to sites where terrorists want to inflict harm. Customs authorities must have efficient means to communicate with intelligence agencies, and customs posts must be equipped with adequate detection systems. Strengthening of the Customs Co-operation Council (CCC) may be one step toward accomplishing this objective.[64]

F. *Obligating Mutual Legal Assistance and Cooperation*

Underlying all other steps, the international community should impose an obligation on States to enact expedited mutual legal assistance and penal cooperation among agents and officials in investigations of suspected terrorist activities and provide evidence for use in subsequent prosecutions. These laws should formalize evidence sharing procedures and obviate the cost, inconvenience, and other difficulties of cross-jurisdictional cooperative investigations. The proposed biological terrorism treaty, mentioned above, obligates States to extradite suspects or prosecute them, but there is no requirement for the various other modalities of legal assistance. Currently, a wide variety of treaties apply to mutual assistance and penal cooperation in different, and sometimes overlapping, contexts. A unified convention would help rationalize coordination among States. Most important, a convention should clarify that the political offense exception to extradition must not apply to catastrophic terrorists.[65]

G. *Harmonizing Municipal Legal Regimes*

An international convention should establish uniform standards for a variety of domestic laws. Domestic law enforcement officials should be authorized to seize miscreants' assets both for use in subsequent prosecutions and to deter anyone from pursuing terrorist activities for pecuniary gain. Law enforcement officials should be able to track bank records and to overcome complex money laundering schemes.[66] In addition, if there are concerns that government officials have been corrupted by criminal activities, new laws should be specified for enactment to

---

64. *See* David McClean, INTERNATIONAL JUDICIAL ASSISTANCE 126–27 (1992).

65. *See generally* Bruce Zagaris, *Developments in International Judicial Assistance and Related Matters*, 18 DENV. J. INT'L L. & POL'Y 339 (1990); and William M. Hannay, *The Legislative Approach to the Political Offense Exception*, *in* LEGAL RESPONSES TO INTERNATIONAL TERRORISM, *supra* note 65, at 116.

66. *See* United Nations Economic and Social Council, *National Legislation and Its Adequacy to Deal with the Various Forms of Organized Transnational Crime; Appropriate Guidelines for Legislative and Other Measures to be Taken at the National Level*, U.N. Doc. E/CONF.88/3 (1994).

authorize investigations and to punish severely those who have breached the public trust. Moreover, those responsible for combatting terrorism activities should be adequately paid to reduce the temptation of corruption.

V. COOPERATION WITH THE PRIVATE SECTOR

The private sector, which contains many attractive and vulnerable terrorist targets, must join government counter-terrorism efforts in order to maximize the success of those efforts. Unquestionably, the interaction of the private and public sectors raises legal issues that must be carefully resolved. How inclined private enterprises are to cooperate with the government depends, in part, on whether systems can be devised to share sensitive information in a manner that neither raises potential liabilities nor risks devaluation of that information.[67] If law reforms are not instituted to obviate relevant concerns, then tactics to prevent catastrophic terrorism may fall victim to pettier but more immediate misgivings over business interests.

Cooperation among competing enterprises may be helpful in developing prevention systems and detection technologies that might be helpful in the fight against catastrophic terrorism. Especially in regard to the threat of cyber-terrorism, inter-enterprise cooperation and information sharing may be necessary as electronic and information systems link vulnerabilities.[68] Since such cooperation could render enterprises vulnerable to antitrust exposure, statutory exemptions to antitrust liability for cooperative counter-terrorism should be considered. Guidance from the Department of Justice Antitrust Division or the Federal Trade Commission that clarifies the standards for communicating information relevant to counter-terrorism could alleviate apprehension among private sector entities.

An effective counter-terrorism information sharing program involves dissemination of information back to private interests after it has been collected and analyzed by the government. Private sector participants may be reluctant to share sensitive information if there are not appropriate protection mechanisms to ensure that the information is not used by competitors, who presumably participate in the same program.

---

67. *See* Information-Sharing Models, A "Legal Foundations" Special Study, Report to the President's Commission on Critical Infrastructure Protection (1997) (visited March 30, 1999);<http://www.pccip.gov/report_index.html>.

68. *See* Legal Foundations, Legal Impediments to Information Sharing, Report 10 of 12, Report to the President's Commission on Critical Infrastructure Protection, (1997), (visited March 30, 1999); <http://www.pccip.gov/report_index.html>.

The same technologies that are used in catastrophic weaponry also have important commercial applications. The risk that confidential business information (CBI) might be lost could impede cooperation of relevant businesses. Without adequate CBI protection, a perilous situation could develop where a private company would have to choose between obstructing counter-terrorism cooperation and losing valuable business information.[69] Trade secrets are protected by Federal law from theft and unauthorized disclosure.[70] More specific provisions should be considered to address unique issues concerning relevant counter-terrorism information and to ensure that appropriate agencies have instituted adequate procedures to prevent diversion or loss.

One specific problem related to trade secret disclosure concerns is dealt with in 5 U.S.C. § 552.[71] This section makes information in the possession of the federal government available to the public on request. Potential participants in an information sharing mechanism may require assurances that their sensitive information will remain confidential despite a FOIA request to obtain that information from the government. Information need not be disclosed if Congress enacts a specific exemption for that type of information. To strengthen counter-terrorism efforts, promulgation of such an exemption may be appropriate.

Different issues pertain to information sharing with foreign corporations. Many agencies employ national security guidelines for sharing sensitive information with foreign corporations, but each agency employs different criteria for determining what information may not be shared and for what percentage of foreign ownership is a bar to sharing.[72] Developing uniform federal guidelines specifically tailored to counter-terrorism could alleviate unnecessary inter-agency confusion.[73]

A key sector of private enterprise will be security specialists. These sensitive duties are being performed by individuals whose qualifications, methods, and accountability are unregulated. One approach could be government licensing of private security specialists that would spec-

---

69. *See generally* Barry Kellman, et al., *Disarmament and Disclosure: How Arms Control Verification Can Proceed Without Threatening Confidential Business Information*, 36 HARV. INT'L L.J. 71 (1995).

70. 18 U.S.C. § 1905 (1994)(disclosure of confidential information generally).

71. 5 U.S.C. § 552 (1994).

72. Executive Order No. 12968, 60 Fed. Reg. 40245 at § 2.6 (1995) provides that classified information may be disclosed to foreign individuals, governments, or international organizations where compelling reasons exist in furtherance of agency mission. This must be done according to carefully defined guidelines. Executive Order No. 12333 provides for cooperation between the intelligence community and foreign intelligence systems. It makes no provision for information-sharing between private entities and foreign organizations or governments. Exec. Order No. 12333, *supra* note 25.

73. *See* Legal Impediments to Information Sharing, *supra* note 71, at Report 10.

ify qualifications for obtaining a license, levels of insurance required, standards of practice, and conditions that allow for limited information sharing. Professional licensing could facilitate responsible growth of the profession by ensuring that trained, qualified and fully insured personnel are available to perform these sensitive duties. Professional licensing could also accelerate the establishment of much-needed industry standards and best practices, and can even serve the interests of privacy by making practitioners more accountable. The licensing body might also facilitate the passing of relevant information in the interests of government and private parties, while meeting clients' needs for confidentiality and control over routine investigations.[74]

The most serious legal issues concerning private sector anti-terrorism efforts have to do with providing assistance in tracking potential terrorists by furnishing information about employees to law enforcement officials. Employees arguably pose the most immediate and credible threat to the nation's critical infrastructures. While the federal government guards itself through authority to conduct background investigations in screening employees for sensitive positions, issue security clearances, and conduct periodic reinvestigations,[75] private employers who produce critical materials and technologies or who operate critical infrastructures do not have the same authority to screen applicants for certain highly critical positions, or to re-investigate current employees prior to placement in such positions.[76]

In many states, private employers do not have access to criminal history information, are prohibited from requesting or using criminal, financial or employment information, and may incur tort liability for revealing unfavorable employment history.[77] These restrictions result from legitimate concerns over privacy, fair employment, rehabilitation, and related questions. Existing laws that hinder an employer from obtaining, with the consent of the applicant or employee, certain job-related background information may need to be reconsidered in light of catastrophic concerns. At minimum, measures should be considered to achieve an appropriate balance between security

74. *See* Legal Foundations, Studies and Conclusions, Report 1 of 12, Report to the President's Commission on Critical Infrastructure Protection, (1997) (visited March 30, 1999); <http://www.pccip.gov/report_index.html>.

75. Civil Service Investigations, Exec. Order No. 10450, *codified in* the Civil Service Act of 1883, 5 U.S.C. § 3301 (1997).

76. 5 U.S.C. § 552a(d) (1994), provides that the employment records of Federal employees cannot be shared with other employers without the involvement of the employee.

77. *See generally* Robert Adler & Ellen Pierce, *Encouraging Employers to Abandon Their "No Comment" Policies Regarding Job References: A Reform Proposal*, 53 WASH. & LEE L. REV. 1381 (1996).

requirements of conducting employee background investigations with individual employees' interests in personal privacy.[78] Broader use could be made of the National Criminal Information Center (NCIC) which serves as a clearinghouse of information about the criminal records of prospective employees.[79]

A closely-related issue concerns the legality of using polygraphs. Federal law currently prohibits private employers from requiring or even asking employees to submit to polygraph examinations except under very narrow and carefully described circumstances involving an investigation into employee wrongdoing.[80] A second narrow exception exists for employers in certain security professions—so that security companies, such as those that provide armored car services or alarm system installation services to specially enumerated businesses, can periodically polygraph their employees (again, subject to carefully defined conditions and circumstances). Arguably, the same rationale that militates in favor of having this exception available for providers of physical security services should apply with equal force to provides of information security services. Congress could narrowly expand existing exemptions to the Employee Polygraph Protection Act (EPPA) to include within the scope of its exemptions those who are in the business of providing information security services.[81]

---

78. *See generally* Privacy Laws and the Employer-Employee Relationship, A "Legal Foundations" study, Report 9 of 12, Report to the President's Commission on Critical Infrastructure Protection (1997), <http://www.pccip.gov/report_index.html>.

79. Under 28 U.S.C. § 534 (1997), the Attorney General is required to establish information on the criminal backgrounds of certain persons for purposes of identification. 28 C.F.R. § 20.31 provides that the FBI administer the NCIC. Criminal Justice Information Systems, 28 C.F.R. § 20.31 (1998). The information can be shared with government agencies or with employees in sensitive industries. This clearinghouse tends to be very passive, only disseminating information as it is requested by prospective employers. The clearinghouse is not capable of alerting the law enforcement community or of monitoring the movements of criminal suspects. States participate voluntarily in the program, and the FBI makes information in the database available to employers who are banks, state and local governments, registered securities exchanges or nuclear power providers. States are free to create their own clearinghouses if they choose not to participate in the NCIC. *See generally* 28 C.F.R. § 20.1–20.38 (1998).

80. The Employee Polygraph Protection Chapter, 29 U.S.C. § 2001.

81. 29 U.S.C. §§ 2001–2009 (1998). These exemptions include all government employees as well as various DOD, DOE, intelligence community and FBI contractors and their employees. 29 U.S.C. § 2006e (1998). Another exception applies to employers who provide physical security-related services for protection of facilities having a significant impact on health of safety, including electric power plants, public water supply systems, public transportation, and protection of currency, securities, commodities, or proprietary information. 29 U.S.C. § 2006(e)(1) (1998). Chemical companies, producers and handlers of biological agents, and provides of telecommunications services are not included in the list of protected facilities.

CONCLUSION

Catastrophic terrorist threats have received far more attention than have the legal rules that are appropriate to a response. This suggests either that officials planning responses to terrorism are callous about those responses' legal implications or that answers are being formulated without overt public discussion involving the larger legal community. In either event, the very real risks of catastrophic terrorism are being compounded, unnecessarily, by the risk that a crisis will evoke an inefficient and/or repressive reaction.

Official supervisory authority is vested in the National Security Council, conferring an unprecedented administrative role for a policy advisory arm of the White House. The benefits of coordination are significant, and the risks of over-reaching may not be currently probable. Yet, the absence of legal safeguards should be addressed lest a precedent of NSC involvement in domestic law enforcement become customary. Somewhat related is the lack of defined rules applying to military roles, both in preventing catastrophic terrorism and responding to an event. The military has important expertise to contribute to counter-terrorism, and a truly catastrophic event might rent the social fabric sufficiently to welcome disciplined troops. But it would seem cavalier to be wholly quiescent about the possibility of an NSC, limited only by the President, exercising supervising authority over troops deployed in the United States. As these concerns can be appropriately addressed through overt adoption of policies specifying the roles of various agencies, including accountability processes, the prolonged absence of such policies tends to energize apprehension.

Materials and technologies relevant to production of biological and chemical agents that pose catastrophic dangers are inadequately regulated. For historical reasons, these substances are easily obtained, produced, and traded, and legal accountability for activity short of actual use is scant. The law's treatment of nuclear materials provides a dramatic contrast, and Congress should consider adopting analogous licensing and monitoring systems for other precursor substances. Internationally, biological and chemical weapons capabilities are even less restricted. But instead of developing sophisticated law enforcement modalities to stanch the production and trade of these capabilities, the international community is focusing verification techniques on commercial sectors as if the primary threat came from States in a military context. There should be discussion, domestically and internationally, about intelligence sharing, cooperative policing, transportation and borders controls, and uniform criminalization. Ignoring the need for

international collaboration is smug isolationism; diverting attention in traditional non-proliferation directions is to turn a blind eye to the fact that the threats have changed. Answers that avoid the need for enhanced law enforcement are folly.

Amidst all these issues is a concern for civil liberties: can we have our security and our autonomy too? The importance of harmonizing public needs with private rights is underlined by the imperative of engaging the private sector in counter-terrorism measures. Threats of antitrust charges or losses of confidential information will alienate the private enterprises whose participation is most critical. Security specialists, who will be the first line of defense, should be held to modest standards; a licensing system may be appropriate. Most challenging will be the task of balancing personal privacy rights with the need to know background information about employees who have access to critical materials, equipment, or infrastructure.

None of these issues is beyond straightforward resolution which makes the paucity of that resolution all the more troubling and, at worst feeds suspicions that rights are being infringed. The legal community, by overtly addressing these issues, can thus serve a dual purpose: by balancing competing interests and enacting those balances into law; and by expounding, in public view, that catastrophic terrorism's threat will neither be ignored nor made a justification for magnification of government restraints on our liberties. There is much constructive work to be done and, perhaps, so little time.