Living with Catastrophic Terrorism: Can Science and Technology Make Us Safer?

William Scholwalter Science and Technology Policy Seminar  College of Engineering, University of Illinois, October 8, 2002

Lewis Branscomb, JFK School, Harvard University
Asymmetric Warfare

- Cold War: asymmetry of Soviet ground forces balanced by NATO technology.
- Catastrophic terrorism is the ultimate in asymmetric conflict;
  - Each terrorist threat is in some ways a new conflict.
  - Organized terrorism is the “privatization of war.”
- To what extent can S&T compensate for the asymmetry in terrorism threat?
Offsetting the Terrorists’ Advantage

- US is not structured to deal with a problem that cannot be compartmented
  - into war or civil justice
  - into domestic or foreign
  - into short term or longterm
  - into public or private responsibility

- US technical community is ready to be called on. How can it help? What will the price be for providing that help?
Sources of Vulnerability

- Terrorists did not create them; we did.
- Vulnerability results in part from the proliferation of weapons for terrorists:
  - chemical, biological, and nuclear weapons of mass destruction – products of the military.
  - Explosives and imaginative uses of conventional technologies in communications, transportation and industry – products of the economy.
- It is a consequence of highly efficient and interconnected systems we rely on for key services -- transportation, information, energy, food, finance, and health care.
Five Points about Countering Terrorism

- Only a vigorous S&T effort can make the United States and its allies less vulnerable.
- Weapons of mass destruction are potentially devastating but not most probable threats.
- Reducing vulnerabilities is a highly complex systems problem.
- New policies for federal – industry relations for critical infrastructure are required.
- The proposed Department is needed but will initially be very poorly equipped to deal with S&T for vulnerability reduction.
Public Policy Alternatives to Hardening Society

- **Foreign Policies**
  - Policies to reduce poverty, injustice, authoritarian rule, religious zealotry, are the only long term solutions

- **Domestic Policing**
  - The cheapest, most disturbing, and probably least effective policy is the denial of civil liberties at home in an effort to find the terrorists.

- **Political temptations**
  - "‘War’ on terrorism” can also be used to justify aggressive actions overseas, deflecting public attention from threat of domestic terrorism.
Assessment of progress since 9-11-2001 – LMB opinion

- Almost nothing has been done by the federal government since 9/11/01
  - Of $37.5 B in HSD for FY 2003, only $0.5 B is for R&D.
- Iraq is an expensive and dangerous diversion from the goal of reducing the recruiting and motivation of terrorists.
- Sacrifices of civil liberties on the altar of the search for terrorists in our midst will not make us safer.
- Little progress on defining industry responsibilities and government incentives for hardening
The Academies’ Study

- National Academy of Sciences, National Academy of Engineering, & Institute of Medicine initiated study with own funds after 9/11. Lewis Branscomb and Rick Klausner, co-chairs; 119 expert contributors, 46 reviewers.

- Presented to Congress and White House June 25.


Website: [www.nap.org](http://www.nap.org)

- Download off web (free) books.nap.edu/html/stct/index.html
Can S&T Make Us Safe?

- No.
- Hardening US infrastructure cannot deny terrorists attractive targets; can only make the attacks more difficult and less effective.
- However, S&T provide the only long term solutions to reducing the threat of terrorism, other than public polices to deter or discourage the motive to commit terror attacks.
Critical Infrastructures

- 85% of US Infrastructure systems are owned and run by private firms; not government.
- They are deeply technically interdependent:
  - Domino effects
  - Leads to threat of multiple, simultaneous attacks
- US deregulation has increased vulnerability significantly in some areas.
- What are government/industry responsibilities? How can government motivate industry investment in hardening?
Vulnerabilities and Ways to Reduce Them
Terrorist targets

- Human health and food systems
- Energy systems (power plants and distribution)
- Communications and information services
- Transportation systems (air, sea & land)
- Cities and fixed infrastructure (buildings, water supply, tunnels & bridges, people)
- People and their response to terrorism
Terrorists’ Weapons

- Nuclear and radiological attacks.
- Biological weapons against human and agricultural health systems.
- Military chemical weapons; inflammable, toxic, & explosive chemicals & materials.
- Cyber attacks on telecoms, data or controls.
- Transportation systems used as weapons.

[Red items are “weapons of Mass Destruction”]
Nuclear and Radiological Threats

If terrorists gain acquire 50kg of Highly Enriched Uranium (HEU) they can assemble an inefficient nuclear weapon in a US city.

The United States must induce other countries to cooperate in safeguarding fissile material and blending down stocks of HEU.

Educate the public on limited nature of the radiological threat.
Biological Threats to People and their Food Supply

• Research on pathogenesis of infectious agents & early detection.

• Stockpile Vaccines against known and unknown diseases

• CDC for agriculture & farm animals to protect food supply

• Research on decontamination in human and farm environments
Toxic chemicals, explosive & flammable materials
Toxic Chemicals and Explosive or Flammable Materials

- Some highly lethal chemicals are easily made. Even greater risk from industrial chemicals.
- Create sensor networks to detect and characterize dangerous materials.
- Self analyzing filter systems for buildings.
- Research on olfactory biosensors to reach levels of sensitivity dogs already possess.
- Special efforts to protect food supply.
- Track dangerous chemicals in transit; encrypted electronic identification.
Energy Systems

• Harden electric power grid and enable recovery.
• Vulnerable unique extra-high-voltage transformers.
• Increase security of SCADA systems; encrypt traffic.
• Develop adaptive power grid for rapid recovery
• Improved surveillance of gas pipelines, electric transmission facilities.
First responder communications
Amplify other weapons; denial of service, spurious messages
Attack SCADA systems in critical infrastructures.

There are no fully secure operating systems.
Transportation and Borders

• Sensor networks for inspection
• Data fusion and mining
• Biometrics for personal ID
• Identifying and protecting critical facilities
• Locating and identifying chemical railcars, containers
Cities and Fixed Infrastructure

- Protect Emergency Operations Centers
- Adopt & extend Europe standards for fire and blast
- Make air intakes less accessible; air filters with analysis.
- Equip first responders to detect toxics and Hazmats
- Bridges, dams, tunnels and dikes
- Water supply: contamination and denial
Response of People to Terrorist Threat

- Trusted and knowledgeable people should be trained in advance to provide accurate and trustworthy information quickly and authoritatively.
- Fear and confusion more likely than terror. Main danger: loss of public confidence in those responsible for protection.
- Is government needlessly amplifying the threat, thus doing terrorists psychological job for them?
  - Need for meaningful warning systems.
  - Need for local leadership and resources.
Technology Strategies

- Repair the weakest links in vulnerable systems and infrastructures.
- Use defenses-in-depth (do not rely only on perimeter defenses or firewalls).
- Use “circuit breakers” to isolate and stabilize failing system elements.
- Build security into basic system designs where possible.
- Build flexibility into systems so that they can be modified to address unforeseen threats.
The “system of systems” technical challenge

- Attacks are likely to involve multiple complex systems
  - Multiple critical industrial infrastructures
  - Federal state and local authorities and responders
  - Complex networks of sensors
  - Data fusion and data mining
- Priority setting requires modeling and simulating attack and response, red teaming proposed solutions.
Dual-Use Strategy

- Search for technologies that reduce costs or provide ancillary benefits to civil society to ensure
  - increase likelihood that industry will invest in hardening critical infrastructure;
  - more sustainable effort against terrorist threats
  - integration of HS R&D with rest of societal research and engineering base
How to set S&T priorities?

- Vulnerability and value of the target
- Ability of S&T programs to harden target
- Dual use value of the S&T outcomes
- Value of the target to terrorists
  - Satisfaction of terrorists’ goals
  - Capability of terrorists to attack it
  - Likelihood of success
Terrorists’ Priorities
Which would they choose if they had the capability:
- Spread disease germs among the population?
- Destroy the Statute of Liberty?
- Flood New Orleans?
- Shut down the New York Stock Exchange?

US counter terrorism strategy requires predicting their priorities. This requires better intelligence and understanding of radical Islam.
Gathering intelligence, controlling people and censoring information: What will government do? What will the public tolerate?
Civil Liberties vs Technology

- Sensors may reduce need for personal & package inspections.
- Biometrics
  - much more reliable than drivers license
  - can also be used to intrude on personal privacy
  - Don’t prove “who you are.”
- However, only politics, not science, can avoid the most serious civil liberties threats (eg TIPS)
Keeping Information from Terrorists

- System of military secret classification is not adapted to terrorism threat.
  - A very broad range of basic research information will be needed to counter terror threats.
  - “Sensitive but unclassified” likely to be applied to much university work.
- Science journals already being attacked for publishing science deemed useful to terrorists.
- There are serious, legitimate dilemmas about what should in fact be published.
The USA PATRIOT Act [Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism]

- Expands intrusion on Internet, answering machines and other telecoms.
- Allows searches without probable cause of a crime.
- Allows determination of what web sites a person has visited if “relevant to an ongoing criminal investigation”
- Expands power to make “secret searches”
- Puts CIA in domestic intelligence gathering through cooperation with FBI.
Security and Intelligence on University Campuses

- Much more difficult problem than in Cold War
  - “War” is here: public interest in security lapses at universities will be intense.
  - “Enemy” is ill defined and diverse
  - Threats are extraordinarily diverse
  - “War” is of indefinite duration; victory is undefined.

- Public will expect universities to track students who may be conceived of as threats

- Universities with rules against work for the CIA will find new policies hard to define.
A new US nationalism:
- Self definition by universities as global institutions may be questioned.
- Could experience a significant rupture in foreign student flow and foreign research collaboration.

Political questions of student and faculty loyalty may arise
- Is a new “McCarthy-ism” possible?
Will she be a TIPS Agent? Post Office says “no.” Justice Department says “Join Now!”

See

www.citizencorps.gov/tips.html
Department of Homeland Security

- Neither Administration nor Lieberman bill originally included Undersecretary Technology, but was added to the House bill.
- Dep’t is assembled from the “border” control agencies; none have a strong S&T research, acquisition & deployment experience.
- With all the S&T capability outside the Department, technical progress depends on an effective OHS and OSTP in the White House; neither seems likely.