Catastrophic Terrorism:
How Technology can Reduce Vulnerability

Lewis M. Branscomb, Harvard University
National Academy of Sciences
National Academy of Engineering
Institute of Medicine

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, 2002.
- Published book entitled: *Making America Safer: The Role of Science and Technology in Countering Terrorism* August 2, National Academies Press [2101 Constitution Ave NW, Lockbox 285, Washington DC 20055.] Website: www.nap.org
- Download off web (free) books.nap.edu/html/stct/index.html

Safety and Security: Natural and Deliberate Disasters

- Some features of natural (or accidental) and deliberate disasters are common
  - First responders and emergency management
  - Making critical infrastructure and cities robust against wind, water and earthquakes.
- Some features of high consequence terrorism are unique
  - Use of elements of civil infrastructure as weapons
  - Weapons of mass destruction (WMD) used against civil populations
  - Absence of prior experience; unpredictable threats
- Governments must attempt to minimize both threats.

High Consequence Terrorism

- Terrorism is a very old threat to established societies – most often tactical with political objectives.
- **Tactical terror weapons** are usually guns or explosives; civil justice system deals with them.
- **High consequence weapons** are WMD or weapons from the civil economy itself.
- Aum Shinrikyo and Al Qaeda attacks set a new standard for level of intended destruction –
  - "high consequence terrorism" is defined by social, economic and political response elicited as well as total damage.

Terrorist's advantages

- Their actions are unpredictable, since their objectives, are largely idiosyncratic and obscure.
- Terrorist cells may be in covert residence within the societies they plan to attack.
- Terrorists may be very patient. Those defending against terrorism must be alert at all times, despite the apparent absence of visible terrorist activity. Natural disasters may give some warning.
- Finally, terrorists may enjoy the sponsorship and assistance of a rogue state with access to WMD.

Advantages of industrial societies threatened by terrorists

- Global intelligence services and military presence of cooperating nations may keep the terror networks off balance,
- Military action, or the threat of it, may discourage rogue states from supporting the terrorists.
- Technological and organizational skills may allow threatened states to deny some attacks, make others less consequential.

Terrorism will Threaten Market Democracies Indefinitely

- Our competitive economy creates vulnerabilities to high consequence terrorism (and to accidents and human error).
- A long-term plan to restructure critical infrastructure can reduce the temptation that vulnerability creates and increase safety.
- Open societies are the most vulnerable to terrorism because they tolerate dissent.
- Defenses against natural and man-made disaster much not sacrifice the values of a free society.

Sources of vulnerability of Cities and Critical Infrastructure

Private sector facilities and services are the targets

- Most physical facility targets are corporate or privately owned.
  - buildings where large numbers of people aggregate
  - critical infrastructure.
- Many critical infrastructure vulnerabilities result from bad design or poor decisions, should be remedied.
- Firms are reluctant to invest in hardening and resiliency because risk/return from terrorism cannot be computed.
- Government funded S&T programs must be conducted in cooperation with private sector.

Ecological Economics

Mechanisms through which efficiency is maximized may threaten resilience to catastrophic terrorism include:

- Single point failures: costs of redundancy are high and risks are assumed to be low.
- Excessive concentration of assets in quest for scale economies.
- Dependence on other critical infrastructure systems to leverage scale economies.

Terrorist targets (examples)

- Potential single point failures
  - UHV transformers in electric power distribution
- Critical control systems
  - SCADA software and Internet communications.
- Emergency Operations Centers and other critical infrastructure
  - Depend on communications and data networks..
  - May be vulnerable to EMP, cyber and other preemptive attacks
- Large numbers of people concentrated in highly complex, fragile facilities in cities.
- Large numbers of people widely dispersed.
  - Attacked with biological pathogens or toxic chemicals
  - Delivered through processed food, letter mail, currency, newspapers….

Sources of Terrorist Weapons and Means of Delivery

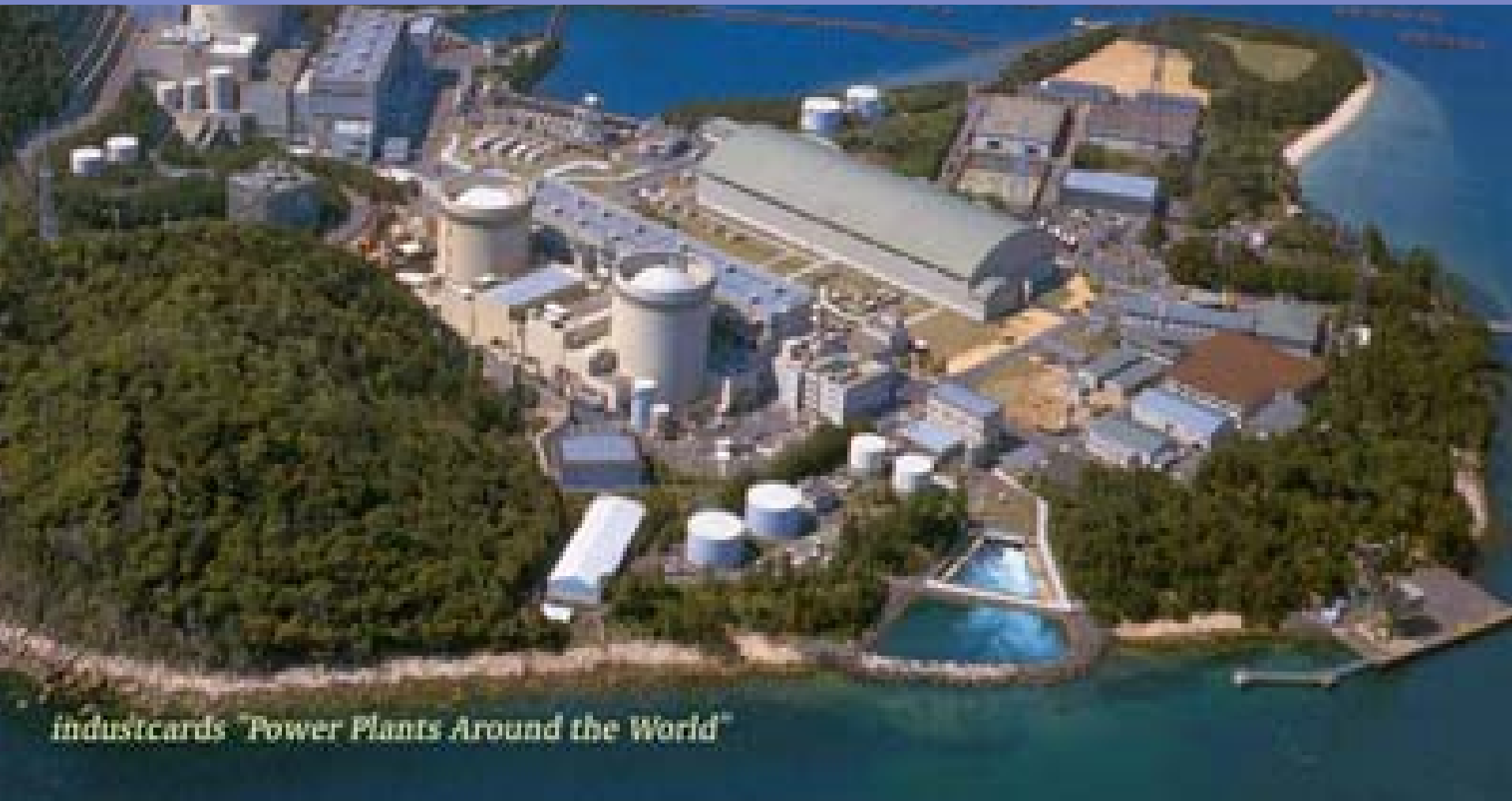
with Examples of Technical Fixes

Terrorist's choice of weapons

- Terrorists would prefer WMD if available
  - [for example from rogue states].
- Many weapons may be available to terrorists from highly efficient, market economies
  - Ammonium Nitrate fertilizer and fuel oil
  - Chlorine shipments to water supplies
  - Fully fuelled large civil air transports
  - Radioactivity from nuclear power plants; toxic chemicals from certain chemical plants.
- Terrorists might use a second weapon to enhance the effect of the first
  - Example: Cyber or Radiation weapons used as consequence amplifiers of a chemical or explosive attack

Nuclear and Radiological Threats

Strengthen international cooperation to deter nuclear weapons proliferation. Protect HEU (and Pu) at the source to prevent creation of crude fission weapons. Inform public about radiological threats to avoid panic.

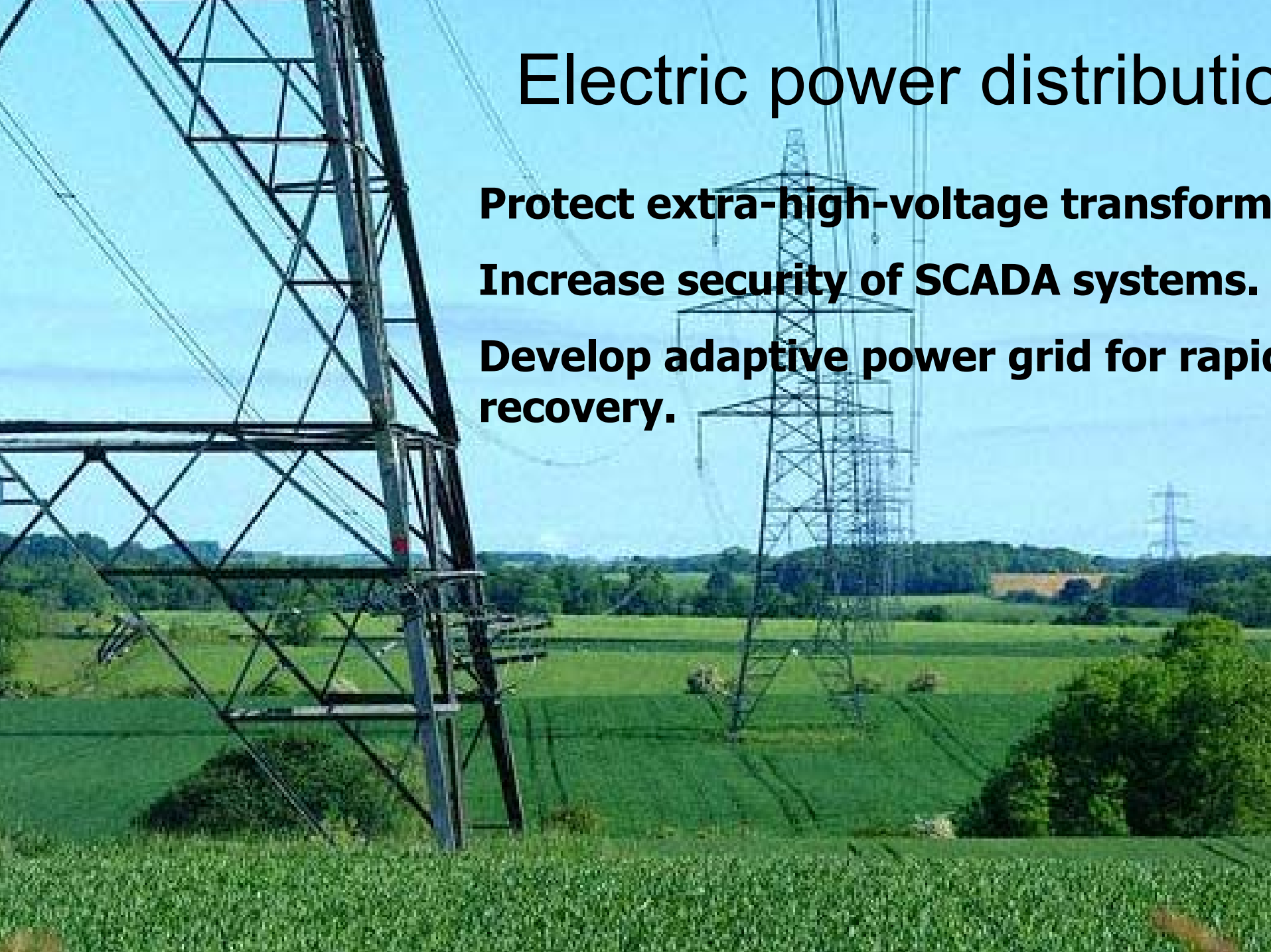


Biological Threats to People and their Food Supply

- Create high speed detection of pathogens, analyze their origins and develop vaccines.
- Create rapid, low cost inspection and identification for pathogens and toxics in agriculture and processed foods.

CHEMICALS

- Track dangerous industrial chemicals in transit; encrypted electronic location and identification.
- Sensor networks to detect and characterize explosives and other dangerous materials.



Electric power distributio

Protect extra-high-voltage transform

Increase security of SCADA systems.

Develop adaptive power grid for rapi recovery.

CYBER & EMP ATTACKS

Interoperable, effective first responder and EOC communications.

Secure computer networks and SCADA systems

Authenticated, secure, and robust command and control communications

Data mining and decision support software

Transportation and Borders

- Sensor networks for inspection
- Biometrics for personal ID.
- Identifying and protecting critical facilities.
- Locating and identifying contents of chemical railcars, containers.

Cities and Fixed Infrastructure

- Protect Emergency Operations Centers.
- Adopt & extend standards for fire and blast in very tall buildings.
- Make air intakes less accessible; improved air filters with analysis.
- Equip first responders to detect toxics and Hazmats.
- Protect bridges, dams, tunnels and dikes.
- Water supply: contamination and denial.

Technical Strategies

- Repair the single point failures in vulnerable systems.
- Use defenses-in-depth (no single firewalls).
- Use “circuit breakers” to isolate and stabilize failing system elements.
- Build security and flexibility into basic system designs where possible.
- Design usable and effective systems for typical first responders (fire, police and medical).
- Focus priority attention on the “system of systems” technical challenge.

Possible projects among universities & national laboratories

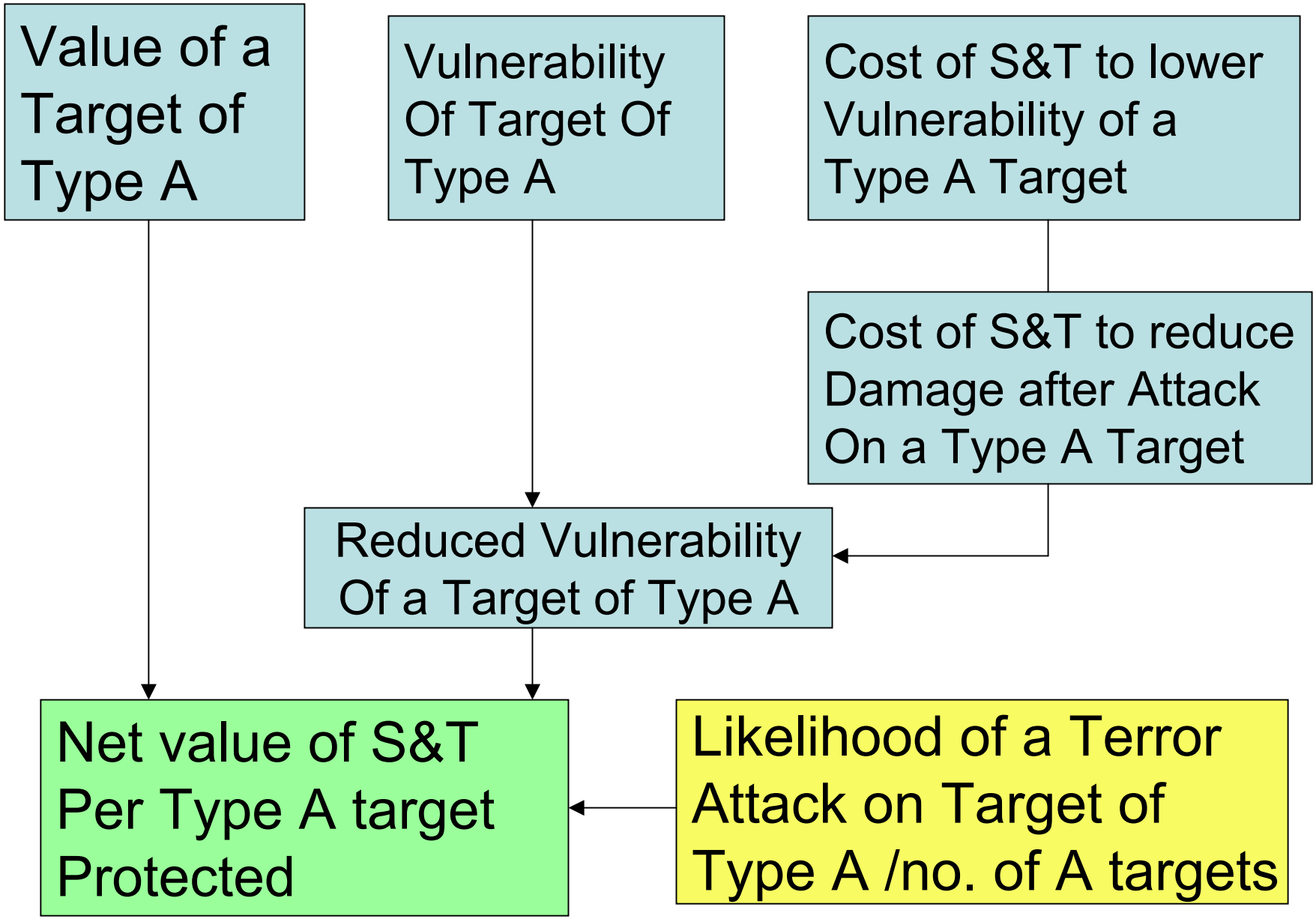
- Pathological organisms, toxic chemicals: detect, identify, evaluate, and respond to threats
- Computer and network security, message authentication, protection of SCADA software
- Sensors and data management from sensor networks, data mining, decision models;
- Border controls: biometrics and data mining
- Risk analysis, economic returns from dual use investment in hardening critical infrastructure in the private sector.
- Roots of terrorism, motivation and behavior of terrorists

System of Systems Analysis, Modeling, Simulation, Evaluation

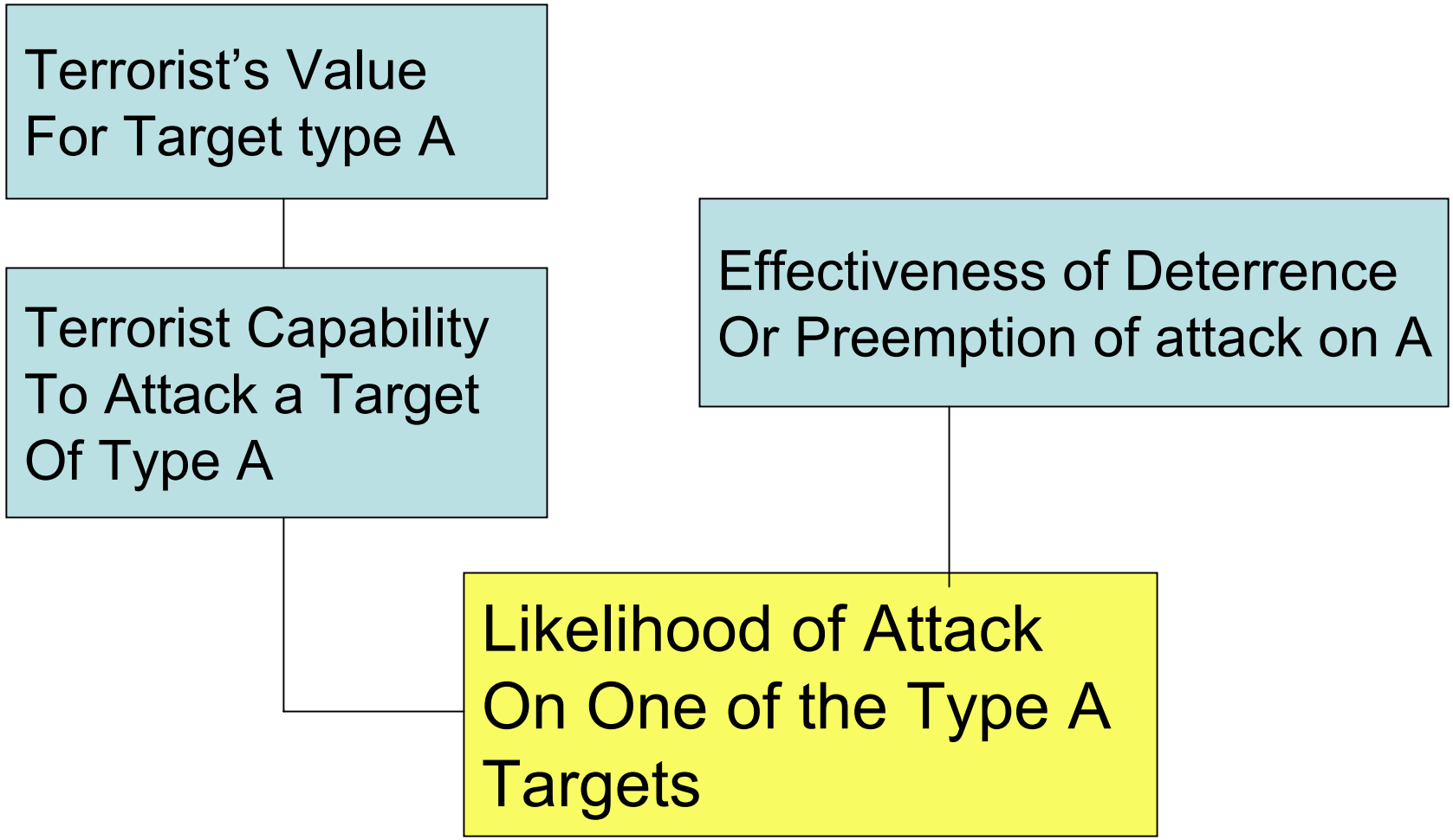
- Testing proposed system solutions
  - As designed through modeling and simulation
  - As deployed through red team testing
- Analyzing linked critical Infrastructures and the effect of attacks on one propagating to others.
- Integrated studies of metropolitan areas
  - Analysis of cities must combine effects of all critical infrastructures, the city's infrastructure, emergency management and organization, and public behavior.

- Setting counter-terrorism priorities requires predicting their priorities.
- This requires better intelligence and understanding of radical Islam and other ideologies.

Value of S&T to Protect a Target of Type A



Likelihood of Terrorist Attack on a Target of Type A



Only he knows Al Qaeda Priorities and Capabilities

Public Panic:
How Officials and the Press Should Provide Public Information

Response of People to Terrorist Attack

Credible experts needed to provide accurate and trustworthy information to the public.

Is USA government needlessly amplifying the threat, thus doing terrorists psychological job for them?

Public Information: Officials, Experts and News Media

- Two objectives of Terrorism
  - Public loss of confidence in government leaders
  - Panic in the face of threats they do not understand
- Civilian experts are often trusted when politicians are not.
- Media and Officials need to engage Experts in public education before the attack.
  - Most important: public understanding of the right response to Radiation Dispersal weapons.

Are Investments to Protect Cities & Critical Infrastructure Sustainable?

- To what extent can firms and owners be expected to invest in hardening?
- Are there "dual benefit" – social and economic -- technical strategies that can reduce costs?
- How similar are the requirements of protection from man-made and natural disasters?
- Will international collaboration help to reduce cost burden and expand benefits?
- Will there be an international market for hardening technologies?

Examples of civil benefits from investments to increase resilience

- Improved Public Health Services for both
  - the normal health needs of communities
  - faster response to natural threats such as SARS.
- Less frequent contamination of the food supply.
- More reliable electric power and other services.
- Safer chemical and energy industries.
- Defense against hackers and virus attacks.
- Better tracking & billing of goods in transit.
- Reduced risk to fire, police and emergency health professionals.

A civilian benefit strategy for hardening industry

- To increase likelihood that industry will invest in hardening critical infrastructure;
- To create a more sustainable public commitment to the costs and inconveniences of national efforts against terrorist threats;
- To integrate homeland security R&D with rest of societal research and engineering base to ensure a fully national effort for both civil economy and homeland security.

Trans-national character of the threat

- Terrorist threats from “safe havens”:
  - cyber attacks,
  - food contamination,
  - shipments of weapons in international freight.
- International services – air and sea transportation, telecommunications, global financial transactions.
- Economic damage spills over to the world economy.
- Fairness and effectiveness of border controls.
  - Agreed standards for biometrics
- Possible rogue nation support for terrorist groups
  - Agreed strategy on nuclear weapons non-proliferation.

Case for US-Japan Cooperation in Counter Terrorism S&T

- We face similar vulnerabilities and threats.
- We enjoy similarly sophisticated S&T
- Our science, services, and economies are closely linked.
- Both countries can enhance their security through technology systems applied to disasters that occur in the civil sector.
- We can reduce the cost and increase the effectiveness of civil security both through S&T collaboration and through comparing outcomes of pursuing different approaches.

References

- *Making the Nation Safer: the Role of Science and Technology in Making the Nation Safer* – The National Academies, Washington DC 2002.

  http://books.nap.edu/hml/stct/index.html

- Lewis M. Branscomb, “Protecting Civil Society from Terrorism: The Search for a Sustainable Strategy” *Technology and Society*, 2004 in press.

Summary

- Roots of terrorism must be addressed internationally.
- Traffic in WMD must be controlled.
- Terrorist weapons may be fashioned from the target economy itself.
- Incentives for private investments in hardening critical infrastructure and urban targets must be devised.
- Protection of critical infrastructure must be accomplished through strategies maximizing civil benefits.
- Hardening infrastructure is complex *systems* problem.
- A degree of cooperation among nations, industries, cities and government unknown in prior experience is required.
- For the protections against terrorism to be sustainable impacts on civil freedoms must be resisted.