Making the Nation Safer

The Role of Science and Technology in Countering Terrorism

NRC Committee on Science and Technology for Countering Terrorism

Lew Branscomb and Rick Klausner, co-chairs

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

Ed Lazowska
Department of Computer Science & Engineering
University of Washington

Panels / chapters

- Nuclear and radiological threats
- Human and agricultural health systems
- Toxic chemicals and explosive materials
- Information technology
- Energy systems
- Transportation systems
- Cities and fixed infrastructure
- The response of people to terrorism
- Complex and interdependent systems

NRC Committee on Science and Technology for Countering Terrorism

Information Technology Panel

John Hennessy and Dave Patterson, co-chairs

Steve Bellovin, Earl Boebert, Dave Borth, William Brinkman, John Cioffi, Bruce Croft, Bill Crowell, Jeff Jaffe, Butler Lampson, Ed Lazowska, Dave Liddle, Tom Mitchell, Don Norman, Jeanette Wing

More interest than any other topic at the 6/25 Hill briefing of the report

IT (the nation's computer and communication system) is:

- A critical infrastructure in and of itself
- A major component of other elements of our critical infrastructure, such as the energy and transportation systems
  - Thus, a weapon and/or point of attack against other targets
- A major element in the prevention, detection, and mitigation of terrorist attacks

Four major elements

- The Internet
- The telecommunications infrastructure
- Embedded / real-time computing (e.g., avionics, SCADA (Supervisory Control And Data Acquisition) systems)
- Dedicated computing devices (e.g., desktop systems)

Threats associated with our IT infrastructure

- The target may be the IT itself
- The target may be another of our society's infrastructures, with IT used ...
  - To launch the attack
  - To exacerbate the attack
  - To interfere with attempts to achieve a timely and effective response to the attack
- Widespread destruction is not required for effectiveness
  - Loss of confidence may suffice – e.g., crash a single fly-by-wire aircraft

Example: Supervisory Control and Data Acquisition (SCADA) systems

⌘ An information system attack could result in irreversible physical damage

⌘ Characteristics:

- Control *and* monitoring
- Minimal attention to security
- COTS components
- Increasingly large-scale, integrated, and distributed
- Information regarding vulnerabilities is readily available

Modes of attack

- Through the wires
- Physical destruction of IT assets
- Compromising trusted insiders

Short-term recommendations

- Increase the security of emergency response agencies' communications systems
- Promote the use of best practices in information and network security
- Ensure that a mechanism exists for providing authoritative IT support to federal, state, and local agencies that have immediate responsibilities for responding to a terrorist attack

Long-term recommendations

- **Research in**
  - Information and network security
  - New IT for emergency response (C3I – command, control, communications, and information)
  - New IT for detection, remediation, and attribution of attacks (information fusion)

Information and network security

- Authentication, detection, and identification
- Containment
- Recovery
- New security models (beyond "perimiter")
- Cross-cutting
  - Reducing buggy code, reducing configuration errors, auditing functionality, managing functionality/security tradeoffs, security metrics, intelligence gathering, field studies of security
- *People!*

IT and C3I for emergency response

- Ad hoc interoperability
- Emergency management of communications capacity
- Security of rapidly deployed ad hoc networks
- Information management and decision support tools
- Communications with the public during an emergency
- Emergency sensor deployment
- Precise location identification
- Managing the physical IT infrastructure
- Characterizing the functionality of regional networks for emergency responders

Information fusion

- Data mining
- Data integration
- Language technologies
- Image and video processing
- Evidence combination
- Privacy and confidentiality

If you want to know what happened ...

⌘ Read the book!

⊡ http://books.nap.edu/html/stct/