Integrating Physical and Cyber Security Workforce Needs (P17-20592)

Session 619 Transportation Workforce Needs for Critical Infrastructure Resilience for Physical Security and Related Cyber Security Challenges

Tuesday January 10, 2017 1:30-3:15 PM

Rae Zimmerman
rae.zimmerman@nyu.edu
Professor of Planning and Public Administration
NYU-Wagner School
Transportation Research Board Annual Meeting 2017

NOT FOR DISTRIBUTION OR CITATION

Purposes, Functions and Types of Physical Security Measures

- Purposes in Reducing the Impacts of Natural and Human (intentional and unintentional) Risks, Threats, and Hazards (Garcia 2008, p. 2 - 7)
  - Prevent or deter movement
  - Delay movement
  - Divert movement
  - Detect movement
  - Reduce damage

- Types
  - Active
  - Passive

- Facilities Used
  - Blockages for transportation systems: Barriers, Bollards, Gates, etc.
  - Building design elements
  - Detection: CCTV, etc.
  - Operational controls

Source: Drawn from Garcia, M. L. (2008) The Design and Evaluation of Physical Protection Systems. Second Edition. Amsterdam: Elsevier.

Examples of Types of Physical Security Structures to Prevent Vehicle Movement (Perimeter Protection)

PASSIVE BARRIERS

Planters

Jersey Barriers

Bollards

ACTIVE BARRIERS

Movable wedges

Crash Beams

FEMA (2007) 430, Site and Urban Design for Security: Guidance against Potential Terrorist Attacks Chapter 4, Physical Security Barrier http://www.fema.gov/media-library-data/20130726-1624-20490-0371/430_ch4.pdf; Bollards, p. 4-23; Planters, p. 4-21; Jersey Barriers, p. 4-30. Active Barriers: Movable wedges and crash beams, p. 4-43

Examples of Types of Physical Security Structures to Prevent Vehicular Intrusion on Transportation Structures (Perimeter Protection): Roadways

Bollards

Picture by Rae Zimmerman

Costs

- Passive: $100-$700 (Jersey barriers and bollards are the most expensive)

- Active: $24,000-$160,000 (wedges are the most expensive)

Source: Compiled by Zimmerman and Restrepo from U.S. EPA (undated web site last updated May 2012) Security Product Guides. Passive Security Barriers, originally available at http://cfpub.epa.gov/safewater/watersecurity/guide/productguide.cfm?page=securitybarriers (web site no longer active).

Cyber-Physical Integration

- The security needs are becoming greater on each sides individually
- As the sectors converge, the need for integrating physical and cyber security is growing
- Integrating physical and cyber security technology has been an enormous undertaking primarily in shaping an integrated workforce
- The nature of the workforce, the disciplines they originate from and the skill sets are very different on either side
- Disciplines and skill sets in each of the two areas differ
- The transition to accommodate integrated thinking is challenging

Definition of cyber-physical (from NSF CISE 2012 Vision Statement https://www.nitrd.gov/nitrdgroups/images/6/6a/Cyber_Physical_Systems_(CPS)_Vision_Statement.pdf)

"Cyber Physical Systems (CPS) are smart networked systems with embedded sensors, processors and actuators that are designed to sense and interact with the physical world (including the human users), and support real-time, guaranteed performance in safety-critical applications. In CPS systems, the joint behavior of the "cyber" and "physical" elements of the system is critical - computing, control, sensing and networking can be deeply integrated into every component, and the actions of components and systems must be safe and interoperable."

Physical Security and Cyber Security

Information technologies are integrated with physical structures: ITS Deployment for Transportation, 78 Largest Metros, 1997-2006

- Traffic data collection 16-38%
- Access to service patrols 0-11%; 30-46%
- Centralized control of signalized intersections 47-54%
- Electronic toll collection 36-82%
- Automatic Vehicle Location devices 23-56%
- Electronic fare collection 30-63%
- Electronic surveillance of intersections 5-4%
- Computerized vehicle dispatch 43-81%
- Public dissemination of freeway condition information 12-38%

Source: U.S. DOT. 2008 Status of the Nation's Bridges, Highways, and Transit Conditions & Performance, Washington, DC: U.S. DOT, ITS Deployment Statistics Database, Research and Innovative Technology Administration. Excerpted and summarized from p. 2-18. Percentage range refers to adoption in 1997 and 2006 respectively

Increasing importance of information technologies in the transportation sector

- Increasing deployment of ITS in transportation between 1997 and 2006 (U.S. DOT 2008)

- Innovations in vehicle technologies for both roads and rail have relied increasingly on information technology
  - "Self-Driving" Cars
  - Personal Rapid Transit

- Vehicular Automation
  - Computerized Controls
  - Computerized Vehicle Location Systems
  - Communication Systems with External Connections

Effectiveness of Physical Security Only

Failures: Cases of Breaches of Transportation Physical Security

- July 22, 2014 Two German tourists/artists scale Brooklyn Bridge and replace American Flag with a white flag[1]
- August 24, 2014 A Russian tourist scales the Brooklyn Bridge during the day[1]
- September 2, 2014 Metal screens are placed on the bridge to supplement a gate as a barrier to intrusions[2]
- November 16, 2014 French tourist scales the Brooklyn Bridge, climbing over a barrier[3]
- Earlier Incident: Adhesion of magnetic structures to bridges and other steel structures
- 2016. Nice and Berlin truck attacks. [4]

Successes:

- Sanitation trucks filled with sand are used to prevent truck attacks
- Physical barriers placed along road and rail systems have reduced consequences of natural hazards
  - Flood barriers such as conventional sandbags

Sources: News media coverage
[1]James C. McKinley Jr. (August 25, 2014) Tourist Is Held After Climb on Brooklyn Bridge Cable, New York Times http://www.nytimes.com/2014/08/26/nyregion/tourist-is-held-after-climb-on-brooklyn-bridge-cable.html
[2]M. Morales and P. Shallwani (September 2, 2014) New Barriers Added to Brooklyn Bridge to Block Intruders. Metal Screens May Thwart Unauthorized Climbers After Recent Stunts, Wall Street Journal, http://online.wsj.com/articles/new-barriers-added-to-brooklyn-bridge-to-block-intruders-1409706761
[3]Pervaiz S. (November 17, 2014) French Tourist Charged After Climbing on Brooklyn Bridge, Wall Street Journal http://blogs.wsj.com/metropolis/2014/11/17/french-tourist-charged-after-climbing-on-brooklyn-bridge/;
[4]

Effectiveness of Physical Security with Cyber

Failures: Unintentional Disabling of Transportation Systems from IT Failures

- August 20, 2003. CSX rail shut down from computer system failure (InformationWeek, August 20, 2003)[1]
- May 25, 2006. Amtrak and NJ Transit system disruption from a failed 4 year old computer part that provided power restoration orders (Associated Press, February 23, 2007) [2].
- September 29, 2011. Major disruption of Long Island Railroad occurred due to a lightning strike and the associated failure of a new computer system and programming error (MTA 2011) [3]
- December 25, 2016. Subway power failure at a computerized centralized power system in Manhattan [4]

Successes

- CCTV (mounted on physical rail transit structures) has detected perpetrators, e.g., London train bombers in 2004

Sources:
[1]InformationWeek (August 20, 2003) Computer Virus Brings Down Train Signals http://www.informationweek.com/computer-virus-brings-down-train-signals/d/d-id/1020446?
[2] M. L. Wald (February 23, 2007) New Gear, Not Old, Caused 2006 Amtrak Blackout, New York Times http://www.nytimes.com/2007/02/23/us/24amtrakcnd.html
[3] MTA (October 24, 2011) Preliminary Review September 29, 2011 Lightning Strike at Jamaica http://web.mta.info/supplemental/lirr/images/09-29-2011_LightningStormPR.pdf
[4] A. Newman (December 26, 2016) Subways Hobbled by Underground Fire in Midtown Manhattan, New York Times.

IT/Transport/Energy (not only people)

Interconnections with Communication Technology: Detection Equipment - SCADA, alarms, etc.

- Availability or access to detection equipment
  - Marshall MI incident – 17 hour delay in detecting rupture
- Adequacy of detection equipment
  - Rancho Cordova, CA incident - arrival of a flame ionization detector to detect outdoor leaks took 2 hours and 47 minutes
- Performance of and experience with detection equipment
  - St. Cloud, MN incident – gas monitor was not calibrated leading to unreliability of readings
  - Knoxville, TN incident – SCADA system failed to determine that a release had occurred; SCADA alarms did not sound when there was a pressure drop
  - Carmichael, MS incident – Emergency dispatch and fire department connection was disabled
- Interpretation of detection equipment results
  - Chalk Point, MD incident – operating procedures and flow monitoring practices were inadequate

Communication technologies come in all shapes and sizes . .

Cybersecurity: IT Dependency in Transportation – Vulnerabilities and Unintentional and Intentional IT Disruptions*

Vulnerabilities

- Cyber intrusions typically have to be accompanied with a physical intrusion and at close range
- Potential for intrusions initiated remotely into automatic breaking systems, unlocking of vehicles, and open software-based communication systems (McMillan July 27, 2011; Koscher et al. 2010)
- McAfee (2011, p. 4) identifies the following location for embedded devices: "airbags, the radio, power seats, anti-lock braking system, electronic stability control, autonomous cruise control, communication system, and in-vehicle communication."
- ICF-CERT (2012, 2013, 2014 reporting dates) notes that cyber attacks on transportation systems constitute about 5% of attacks on utilities and manufacturing facilities

Intentional Attacks

- August 2006. Traffic signals were hacked in Los Angeles disrupting traffic (Bernstein and Blanstein 2007)
- August 2011. Hacking of BART system (Newton 2011)

Sources: *Summarized from R. Zimmerman (2012) *Transport, the Environment and Security*, Cheltenham, UK & Northampton, MA: Edward Elgar Publishing, Ltd. Ch 7.
S. Bernstein and A. Blanstein (January 9, 2007) Key signals targeted, officials say http://articles.latimes.com/2007/jan/09/local/me-trafficlights9
Koscher, K., A. Czeskis, F. Roesner, S. Patel, T. Kohno, S. Checkoway, D. McCoy, B. Kantor, D. Anderson, H. Shacham and S. Savage (2010) Experimental security analysis of a modern automobile' 2010 IEEE Symposium on Security and Privacy, available at http://www.autosec.org/pubs/cars-oakland2010.pdf.
McAfee (2011) Caution: Malware ahead', available at http://www.mcafee.com/us/resources/reports/rp-caution-malware-ahead.pdf.
McMillan, R. (2011), '"War texting" lets hackers unlock car doors via SMS NetworkWorld, available at http://www.networkworld.com/news/2011/072711-war-texting-lets-hackers-unlock.html
Casey Newton (August 14, 2011) BART website hacked, customer info leaked http://www.sfgate.com/bayarea/article/BART-website-hacked-customer-info-leaked-2335175.php

Some Warnings and Cautions

Wrong communication involving IT and transportation at least indirectly during or creating another layer of disaster leading to further casualties:

- WTC September 2001 attacks. Some building occupants were told to stay in place as if it was a fire.
- Fukushima. People were told to evacuate to what turned out to be the direction of radiation rather than away from it.
- Mianus Bridge collapse. Evacuation orders were for people to move toward the break.
- Institute WVA. Chemical that escaped was not programmed into the computer so it went undetected.

Then there are cyber attacks . . .

IT/Multiple Infrastructures: Concentration of Cyber Attacks in Critical Infrastructure Sectors

In 2012, ICFCERT reported based on 198 attacks*:

- 41% (82) in the energy sector
- 3% (6) in the nuclear sector
- 15% (29) in the water sector, and
- 3% (5) in the transportation sector

By 2013, based on 256 attacks they reported**:

- 59% (151) in the energy sector
- 3% (8) in the nuclear sector
- 5% (13) in the water sector, and
- 5% (12) in the transportation sector

By 2014, based on 245 attacks they reported***:

- 32% (79) in the energy sector
- 27% (65) in manufacturing
- 3% (8) in the nuclear sector
- 6% (14) in the communications sector
- 6% (14) in the water sector
- 6% (15) in health care, and
- 5% (12) in the transportation sector

*Industrial Control Systems Cyber Emergency Response Team (October/November/December 2012) ICS-CERT Monitor http://ics-cert.us-cert.gov/sites/default/files/ICS-CERT_Monthly_Monitor_Oct-Dec2012_2.pdf p. 5.; **Industrial Control Systems Cyber Emergency Response Team (October-December 2013) ICS-CERT Monitor, p. 1, https://ics-cert.us-cert.gov/sites/default/files/Monitors/ICS-CERT_Monitor_Oct-Dec2013.pdf; ***ICF-CERT Monitor, Jan.-Feb. 2015, p. 1

Synopsis

Do we fight physical security breaches with physical security or with cyber security or both?

- The French response to the use of trucks in Nice was to increase electronic surveillance*
- The U.S. response to both the use of trucks was to fight trucks with trucks, e.g., sand-filled sanitation trucks as barriers during New Year's eve in NYC**

Regardless of the directions taken, new coordination and collaboration among government agencies and hence training will be required.

Sources:
*Noemie Bisserbe and Sam Schechner (November 25, 2016) French Authorities Deploy New Surveillance Powers to Thwart Attack, The Wall Street Journal via the Associated Press.
**Ashley Southall December 29 2016 Garbage Trucks Will Help Protect New York for New Year's Eve, NYT
http://www.nytimes.com/2016/12/29/nyregion/new-york-city-new-years-eve-defense-team.html