Security aspects in the construction and maintenance of infrastructures of the inland transport sector

Richard Harris
Director Intelligent Transport Systems
Faber Maunsell - AECOM

Security Principles

– Deterrence – Keep the bad guys out; make it easier for them to go elsewhere

– Detection – If they do get in, make sure you know about it

– Assessment – Once something happens, know what is unfolding

– Response – Be able respond appropriately and manage the result

Major events

- March 1995 Tokyo subway sarin attack
- July 1995 Paris subway bombing
- February 2004 Moscow subway bombing
- March 2004 Madrid train system bombings
- July 2005 London underground and bus bombings

Infrastructure Security Challenges

- Transportation systems, by their nature, invite public access
- Roadways and rail systems are spread across the landscape
- Distances can make response times long
- Information networks (CCTV, alarm reporting) can be expensive because of distances

Vulnerable Points

- Rail Stations and Railways
  - Open to public access
  - Busy/Crowded
    - Small explosive device can have big impact
    - Difficult to monitor for terrorist activity
    - Difficult to screen passengers
  - Can have economic impact with loss of public confidence

Vulnerable Points

- Roadways, Bridges and Tunnels
  - Open to public access
  - Traffic gridlock can present an inviting target
  - Maintenance points give access to critical areas
  - Vehicle borne explosives are difficult to detect

Best Practices

- Rail Stations
  - Work with police and emergency response staff to design around security concept of operations
  - Use pedestrian modeling to eliminate choke points in passenger flow
  - Use CCTV to monitor interior and exterior
  - Use intrusion alarm on all entries to non-public spaces
  - Place police or emergency response assets and accommodations at key points

Best Practices

- Roadways, Bridges and Tunnels
  - Work with police and emergency response staff to design around security concept of operations
  - Use CCTV to monitor traffic flows and unusual behavior
  - Use intrusion alarm on all entries to non-public spaces
  - Incorporate automatic toll collection equipment into the security system
  - Use lighting to deter criminal activity

Best Practices

- Use technology
- Share technology
- Collect data and share information

Best Practices

- Communications is Imperative
  - Information is critical
  - Communication of alarms, unusual events or suspicious activity must be instant
  - Communications in the management of event response saves lives and minimizes damage
  - Communication Systems must be part of any design

Best Practices

- Communications is a Vulnerability
  - Information must be kept close
  - Design drawings are a terrorists best asset
  - Safeguarding security designs may require different procurement methods in the public sector
  - Procedures for handling security sensitive information before, during and after design and construction are a must

Ministerial Conference on International Transport Security

- Sharing best practice
- Promoting international cooperation R&D, technology, detecting and monitoring
- Encourage government cooperation with stakeholders
- Encourage creation of international working group

- Australia, Canada, China, France, Germany, Indonesia, Italy, Japan, Malaysia, Republic of Korea, Russian Federation, Singapore, UK, USA.

UNECE Role

- Road Transport Infrastructure, European agreement on main international traffic arteries TRANS/SC.1/2002/3 April 2003
- European agreement on main international railway lines ECE/TRANS/63 May 1985
- European agreement on important international combined transport lines and related installations ECE/TRANS/88/rev.3
- European agreement on main inland waterways of international importance ECE/TRANS/120
- Basis for future agreement on levels of service and equipment?

UNECE Role?

- Lead or support international cooperation
- Supplement existing agreements
- Identify priority facilities
- Stipulate recommended security measures