EUROPEAN ORGANISATION FOR SECURITY

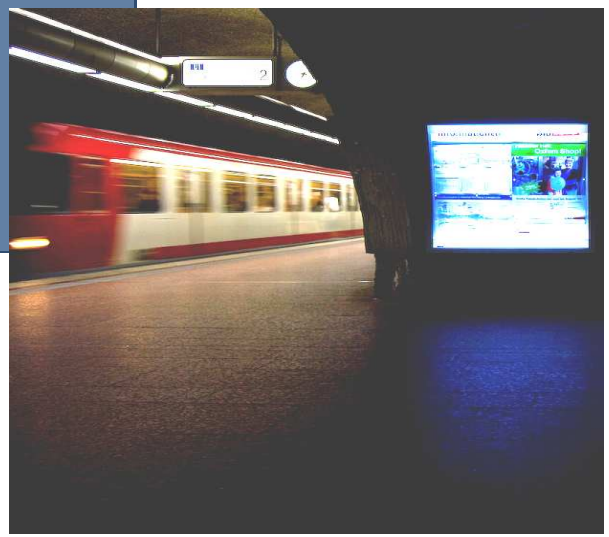
SURFACE TRANSPORT SECURITY WORKING GROUP PRESENTATION TO UNECE

EOS: 31 MEMBERS
12 EUROPEAN COUNTRIES

	USER/OPERATOR & SUPPLY COMPANIES	RESEARCH & NGOs Institutions	EU Sectoral Associations
CIVIL SECURITY & DEFENCE	Alcatel·Lucent, ALTRAN, Atos Origin, Avio, BAE SYSTEMS, bumar, COTECNA, DASSAULT AVIATION, DIEHL, EADS, EDI SOFT, ENGINEERING INGEGNERIA INFORMATICA, FINMECCANICA, FINCANTIERI Cantieri Navali Italiani S.p.A., G4S Group 4 Securicor, Indra, IVECO, Sagem Défense Sécurité SAFRAN Group, SAAB, SIEMENS, smiths detection, ieletron, TELVENT, THALES	CEA, KEMEA, TNO	ASD, CORTE, ERTICO ITS EUROPE
TRANSPORT & ENERGY			
INFORMATION & COMMUNICATION			
FINANCE & SERVICES			
HEALTH / FOOD / WATER			
NUCLEAR / BIO / CHEMICAL			

Overview

- In particular, the Surface Transport Security Working Group focuses on **Subways, Trains and Buses Security**.



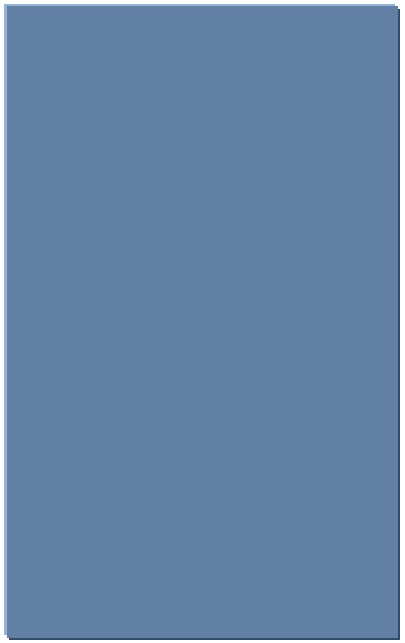
Composition of the Group on Surface Transport

Out of the 31 companies members of EOS, 18 organisations – Users, operators, research organisations and EU Sectoral Associations – are involved in the Working Group on Surface Transport

Why the focus on Subways, Trains and buses?

- Typically security in these transport modes is not given the correct priority.

Complex open systems with large distances between stations



Impression that as security increases so does the disruption to business

Common risk and requirements

- There is commonality between environments both social and commercial.
  - All concerned with moving people from A to B
  - All need to protect revenue
  - All need to provide a secure and safe environment

Common risk and requirements

March 1995 Tokyo subway sarin attack

July 1995 Paris subway bombing

2004 Moscow subway bombing

2004 Madrid train system bombings

2005 London underground and bus bombings

Common risk and requirements

- Risk Analysis– Quantify and understand the risks
- 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 – To be able respond appropriately and manage the result
- Evidence – Post incidence, collect and maintain evidence integrity

Towards an integrated market

- Reduction of costs
- Efficiency
  - In many cases development is being done at sub national level
  - Collection of best practices
  - Economies of scale

Harmonisation

- Need to ensure interoperability.

"Communications from the trains to the London Underground Network Control Centre and the emergency services were inadequate or non-existent on 7 July. As a result, transport and emergency service workers had to run from the trains to the platforms and back again to communicate with their colleagues and supervisors"

Technology from other areas

- Indoor positioning and navigation systems
- Remote vehicle stopping and immobilisation
- Satellite communications can be used to support high data rate transmission such as video to control centres

Need for rationalisation of stakeholders

- No clear leader of owner of transport security.
- Different EU DG's tackling security in general

EOS White Paper on Surface Transport Security

The objectives of the WP are as follow:

- Define what “Transportation Security” means and develop Security and resilience concepts
- Take stock of existing practices, challenges and gaps
- Prepare and develop the market (gather the opinions of EC DGs, MS, Regulators etc…)
- Promote standards at EU level
- Give the industrial vision to the users
- Integrate Security in the business of operators

Methodology:

- White Paper will be developed
- The White Paper is being drafted with Users & Operators
- The WP will be further discussed with users and operators and validated during a workshop organised in 2009.

White Paper's scope

Subway and Surface train (urban) Scoping

- From any event or man made disaster
- Facilitating security into the business model
- Passenger security :- so where can we act from? The moment they enter the station to carrying out the journey
- Station security
- Wagon security
- Securing infrastructure and critical assets (human and physical) entering unauthorised a control centre and interlocking ,stations etc ...
- Access control & Authentication (ticketing)
- Recognition of illegal handling and behaviour
- Tunnel security
- Recognition of critical situations :- intelligence pre-processing and indentifying, monitoring situations automatic systems to highlight situations to the operator.
- Privacy Issues

Bus (urban) scoping

- From any event or man made disaster
- Where is security in bus transportation?
- Facilitating security into the business model
- Passenger security :- so where can we act from? The moment they enter the bus station/bus to carrying out the journey
- Securing infrastructure and critical assets (human and physical) entering unauthorised a control centre etc
- Access control & Authentication (ticketing)
- Recognition of illegal handling and behaviour
- Recognition of critical situations :- intelligence pre-processing and indentifying, monitoring situations automatic systems to highlight situations to the operator.
- Privacy Issues

Meeting Users and Operators

EOS has identified the following Organisations as first interlocutors in the framework of the drafting of the WP:

- European Commission
- UITP (Union internationale des Transports publics)
- CER (Communauté Europeenne du Rail)
- TFL (transport for London)
- Banverket - Swedish National Rail Administration
- RATP
- VDV (Verband Deutscher Verkehrsunternehmen)
- TMB (Transports Metropolitans de Barcelona)
- STIB
- Metro de Lisboa
- Deutsche Bahn
- ACPO
- KLPD
- SNCF/RFF
- Comboios de Portugal/REFER
- RAVE – Rede de Alta Velocidade
- RENFE/ADIF
- Railtrack
- ATOC (association of train operating companies UK)
- Train Italia/RFE (Rete Ferrovaria Italiana)
- UNIFE (The European Rail Industry)
- SNCB (Belgium)
- ALLIANZ (technical team, not the risk profilers)
- RAILPOL
- EMT - Bus Public Transport Madrid

Questionnaire to users and operators

An extensive questionnaire has been drafted by the members.

- **Definition of the Perimeter (organisation/ Funding)**: importance of security, organisation, budget, links with EC, what means security, threats assessment, existing methodology for risk assessment, needs for standards/regulations? etc…
- **How do operators deal with Security? (Security Officer? To whom does he report?):** defined procedures, levels of security throughout the infrastructure, organisation, training? Links with other operators (police, emergency services…), contingency planning and exercises, use of CCTV, standard security architectures? Sharing of best practices together with the other operators? Who are the key players in terms of Security?
- **Efficiency of the existing security systems and procedures?** security criteria and indicators, measurement of the effects of security, existence of key Performance Indicators
- **What are the current needs? What needs to be improved?** Is Screening of passengers for subway viable? Needed? Mobile? Stationary?Are there visible and non visible methods to security? What security concerns are not covered currently? Required improvements on existing security procedures or technology solutions: did you identify security gaps
- **Other?** Insurance

Working Group's next steps: Planning for the next 6 months, 12 months and 3 years

6 months

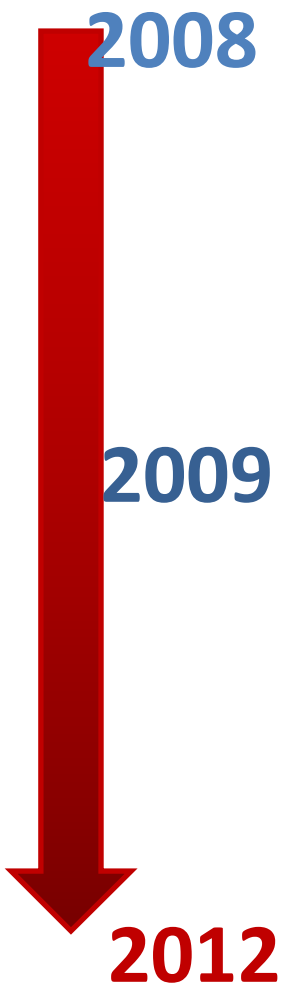
- Draft White paper (version 0) (by Dec 08)
- Workshop with users/operators and possibly EC Beginning 2009
- Operator meetings get in touch with the customers
- Expert Group of EC?
- Strategy for push to market
- Communications

12 months

- White paper V1(after workshop)
- Surface transport security framework definition
- Demonstrations or trails
- Push to Market of solutions
- Communications

3 years

- Implementation and Deployment
- Communications



Recommendations

- Take into consideration mass transit systems
- Support international co-operation (What role for UNECE?)
- UNECE could work with EOS to build links between stakeholders to help them make security a priority in their operations, policy and procurement *Security & Resilience Programme aimed at:*
  - *Common methodology for risk assessment and management*
  - *Common understanding of needed capabilities*
  - *Capacity Building (including technology, legal, social, awareness issues)*
  - *Support to deployment at local level*
  - *Training and support*