United Nations ECE/TRANS/SC.2/2018/2

Economic and Social Council

Distr.: General
4 September 2018

Original: English

Economic Commission for Europe

Inland Transport Committee

Working Party on Rail Transport

Seventy-second session
Geneva, 21-23 November 2018
Item 5 of the provisional agenda
Rail security

Workshop on Rail Security and the Observatory

Submitted by the secretariat

I. Background

1. Rail security has been on the agenda of the Working Party on Rail Transport for a number of years with the Inland Transport Committee highlighting the importance of this work on a number of occasions (for example in ECE/TRANS/208, para. 91). Over the years the work has extended into the creation of an online Rail Security Observatory that provides member States with access to key rail security information through the sharing of best practice. Following on from the workshop held in 2013 on this subject, the Working Party agreed at its seventy-first session to organise a further workshop to be held in 2018 to update member States on recent developments in the field. This document provides a summary of the outcomes of this workshop as well as an update on the Rail Security Observatory.

II. Workshop on Rail Security (ITF Annual Summit in Leipzig, Germany, 23 May 2018)

2. In collaboration with the International Transport Forum (ITF) and the International Union of Railways (UIC), UNECE organised a workshop on rail security at the 2018 ITF Annual Summit in Leipzig, Germany on 23 May 2018. Tying in with the general theme of the ITF Annual Summit of Safety and Security in Transport the workshop brought together over 30 industry experts and professionals to discuss key issues affecting security in passenger and freight rail transport as well as issues relating to the secure management of infrastructure. The workshop also reviewed steps aimed at improving cyber security in the railways and looked to the future for developing a more secure railway.

The workshop was divided into three main sessions:

- Rail security and the passenger interface
- Rail security and freight
- Rail security implications for infrastructure.

3. These three main sessions were then followed by discussions and conclusions for the workshop.

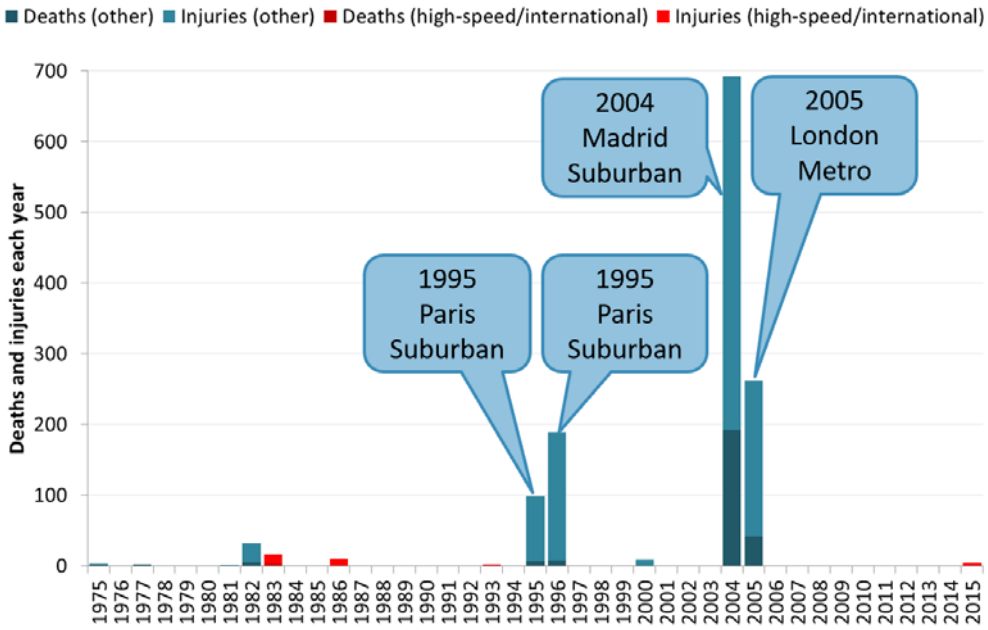
A. Attendance Rail security and the passenger interface

4. A common theme throughout the passenger session presentations and discussion was the need to enhance coordination and cooperation in rail security and how this needs to be addressed mainly for international traffic. National barriers are creating a disconnection between different regimes which could create gaps in security. As one of the speakers stated, "…member States that individually do all the right things leave gaps between them". The need for some form of common legislative and regulatory framework was also highlighted by one of the railway operators present that asked whether vandalism is defined the same in all countries and where you draw the line between vandalism and terrorism.

B. European Union Study on security for high-speed international rail services

5. At the European Union (EU) level, a study on options for the security of European high-speed and international rail services was undertaken in 2016, for international passenger services (where the train crosses at least one border of a EU member State and where the service carries passengers between stations located in different states) and high-speed services (provided by high-speed rolling stock, including tilting trains, that travel at least 200 km/h for at least part of the service; the use of high-speed infrastructure being not always necessary). This study showed that terrorism is rare and focused on metros and suburban lines (figure below).

Deaths and injuries in terrorist attacks*



6. There is, of course, no publicly available data on terrorist incidents that have been averted thanks to local police interventions so there is no way of measuring threat levels to the railways. Table 1 below sets out the average cost of security incidents on the railways. This table shows that terrorism accounts for a small proportion of those costs. However, these costs relate primarily to ex post costs rather than prevention which may be significantly higher due to the number of events averted.

The identified cost per security failure

Security failure	*Average cost, all rail services*	*Average cost, high speed and international*
Vandalism and graffiti	€280 million	€30 million
Metal and cable theft	€70 million	€7 million
Terrorism	€20 million	€0.2 million
Other violent crime	No estimates found, but may be very large	
Other non-violent crime	No estimates found, but may be very large	
Total identified	**€370 million**	**€37.2 million**
Annual passenger numbers	9,200 million	300 million
Identified cost per passenger	**4.0¢**	**12.4¢**
Terrorism cost per passenger	**0.2¢**	**0.7¢**

* Source: Steer Davies Gleave.

7. Building on the data and results the following recommendations were developed:

- Reporting and monitoring:
    - the European Commission should establish a Union-wide framework for reporting and monitoring data on the security of high speed and international services
- Design of trains and stations for added security: The Commission, international and national bodies, prepare guidance on:
    - design of station access and egress, to improve security at stations used by high speed and international services; and
    - standards for blast-resistance on trains and at stations.
- Risk assessment and contingency planning: member States be required to ensure that bodies involved in the operation of high speed and international rail services introduce Security Management Systems (SMSs) including:
    - protocols for the exchange of information between relevant agencies responsible for the security of such services;
    - the recording of vulnerabilities on trains, at stations and elsewhere on railway networks; and
    - documented contingency planning and incident recovery processes.
- Monitoring and awareness of security risks: The Commission, in collaboration with relevant bodies, prepares common mandatory standards for CCTV on trains and stations:
    - as a minimum, covering requirements for recording capability; and
    - optionally, for facial recognition and real-time monitoring;
    - member States should be required to identify responsibilities for undertaking CCTV monitoring activity.

8. Since this study, an open public consultation on rail security and a targeted survey have been carried out. Based on the outcome of these consultations, the envisaged actions are on the EU side are:

- Understand the threat to rail passengers and staff (collect and share information on rail security incidents and counter-measures, implement an EU common methodology for assessing risk, involve passengers and staff with raising security awareness);
- Ensure an adequate response to the threat (reinforce cooperation between the police and railway companies, make an inventory of best/good practices, develop risk management plans for rail);
- Ensure consistency of mitigation measures in member States (staff scrutiny and training, improve station and train security design, wider use of security technologies and customized security processes); and
- Set up a coordination mechanism to address transborder effects (ensure consistency of controls, set up a European railway security coordination body with focal points from the Member States, organize common security exercises).

9. It was acknowledged that there is a need for increased collaboration with law enforcement bodies within countries, but also between countries. This implies setting clear roles for the different stakeholders-operators, infrastructure managers and law enforcement, when dealing with security threats.

It also means increased data sharing for security purposes with law enforcement. Nonetheless, there is a balance to strike between personal privacy and data sharing agreements. Furthermore, there is a difference to be made between commercial data with detailed profiles of users and security wise useful and more easily sharable information.

C. Other aspects addressed during the passenger session

10. In its presentation, COLPOFER explained the level of cooperation that already exists within the European Union between railway related police forces as well as the different types of devices that are used to protect passengers and railway assets in stations and beyond. COLPOFER mentioned that a key issue is ensuring passenger awareness and shared a number of their awareness campaigns underway in Italy. As a conclusion, COLPOFER mentioned that the key aspects of railway security remain ensuring: appropriate training, information sharing, continuous improvement and collaboration between the entities involved.

11. UIC presented the ongoing projects from its Security Division on establishing a Network of Quick Responders and developing a Security Hub. The latter is a private Web Platform accessible to UIC Members and other eligible stakeholders, containing a database featuring many consistently compiled and arranged security measures and data searchable through a structured search function allowing easy and intuitive searches and different possible approaches. End-users can submit comments, share data, statistics or operational experiences about each measure and submit questions to the UIC Network of Quick Responders directly from the Security Hub interface.

D. Rail security and freight

12. The session on freight started by stressing the need to have “soft” integration measures between different world regions. While in the air sector there are common international security regulations, the same does not happen for rail. The Eurasian rail bridge between East Asia and Europe was given as an example where there are “hardware” links, but no regulatory or standards harmonization in relation to rail security for the freight sector.

13. The North American case was provided as an example where there are a number of different challenges. There is good cooperation between authorities across borders and a system which is technically integrated. However, from the point of view of business and the regulatory environment there remain other critical security challenges related to border crossings. Kansas City Southern de Mexico explained this by showing how they: “…face two types of security challenges from criminal groups, first what they want to put in the trains, second what they want to take from the trains”. Drug trafficking, illegal immigration and people trafficking belong to the first group of threats. Dealing with illegal immigration is a particularly controversial topic and one where there is not much the rail operators can do by themselves. Organized crime employing women and children to steal elements from the rail infrastructure is another common security threat. It should be stressed that even while faced with this array of issues rail is still the most secure transport mode in Mexico. To face these threats different means and tools are mobilized by the railway companies, recently drones have been introduced for monitoring and surveillance with positive results. But beyond anything that the rail companies can do themselves, the critical factor is cooperation with the authorities and law enforcement.

14. The discussion also touched in more detail on the procedures associated with border crossing and customs for freight movements. The World Customs Organisation argued that one aspect that would greatly facilitate customs procedures is the acceptance by customs of commercial documents as transit declarations without the need of additional bureaucracy (assuming the commercial issued documents contain the necessary information, such as goods description). Another example provided was the Electronic Customs seal, a radio frequency identification (RFID) or global positioning system (GPS) based technology may contribute to improve security against theft and diversion of cargo and illegal goods such as narcotics and weapon. This lead to a discussion on the balance needed between the costs of employing extra equipment and regulations imposed by security concerns and the competitiveness of private businesses (as is the case of many freight operators). Moreover, the costs of added security are not only purely monetary, they also imply a reduction in capacity and seamless movement of goods and people by rail. To overcome this contradiction, new security measures should, as much as possible, simplify existing procedures and requirements. Some examples were provided on how security and efficiency can be improved with cooperation between authorities of different countries.

15. Discussions also emphasised (through the OTIF presentation) the electronic interface and how ensuring its security is of paramount importance as well as possible solutions to improve the security of rail freight (DB Schenker).

E. Rail security implications for infrastructure

16. The third session of the Workshop on Rail Security covered infrastructure security. This aspect should be addressed as an element of quality of service, supporting the various activities of the rail sector. A priority (beyond avoiding the already known and diagnosed attacks) should be developing cybersecurity further. This is an area where work and improvement is particularly needed due to the speed of technological/digital development. In fact, the growing drive towards digitalisation creates opportunities for new activities and important efficiency improvements, but it also creates new threats which need to be addressed in an effective way. The shift towards intermodal transports needs IT management systems capable of connecting different layers and entities. This interconnection exposes new potential weak spots in such systems. A consortium of 6 partners from 5 countries tackles, through the CYRail project, the challenges of cybersecurity in the railway sector. The goals of this project are to:

- Perform a cyber security assessment of the Railway systems
- Deliver a taxonomy of threats targeting rail management and control systems
- Assess and select innovative rail management systems attack detection techniques
- Specify Countermeasures and Mitigation strategies for improved quality levels
- Achieve Security by Design, by selecting a development framework and specifying Protection Profiles with Evaluation of Assurance Levels.

17. In addition, discussions in this section focused on specific aspects of possible solutions for infrastructure with a particular focus on closed circuit television and similar solutions and their role in ensuring increased security.

F. Workshop conclusions

18. Workshop participants reiterated the importance of continued discussions on rail security as no definitive solutions have been found and threats to passengers, freight, and infrastructure remain. The participants agreed that cooperation between competent authorities at a national and international level remains the most important aspect that needs to be pursued further to ensure that vigilance remains high and rail security threats are minimised.

19. It was agreed that the use of modern technology and new practices in staff training reduce the risk of rail security related events occurring and that railways, where possible, should seek to invest in this going forward. In addition, the emergence of cybersecurity threats and the increasing reliance of the railways on electronic based systems has created a new security threat that needs to be put on a par with other security threats such as terrorism and cargo theft.

20. Participants welcomed efforts by international organisations to facilitate information sharing and cooperation through workshops such as this as well as other initiatives including online information sharing and asked that such initiatives continue going forward.

III. Rail security observatory

21. To support the efforts of member States and rail transport organizations, and to improve the cooperation among the different stakeholders and elaborate common definitions on rail security, the Working Party considered two actions towards facilitation of the above mentioned issues: (a) development of an electronic space allowing to share information and knowledge, creation of an on-line library and, possibly, sharing of good practices in different fields, and (b) development of definitions on rail security with the participation of all interested stakeholders working within the above electronic space.

22. The electronic space allowing to share information and knowledge is available to all member States and rail transport organization who request access. The users can upload documents related to various rail security themes, and search for information uploaded by the other users by combining keywords and various filters. To date, the secretariat has created access to the electronic space for 19 users.

23. Following the seventy-first session of the Working Party, and in conjunction with the workshop mentioned in section II of this document, a further update of the observatory was made with further documentation uploaded and an additional section added providing recent news items relating to rail security that may be of interest to focal points.

IV. Next steps

24. The Working Party may wish to decide next steps in its work in relation to rail security.