Confederation of European Security Services

Position Paper

Study on options for the Security of European high-speed and international rail services commissioned by DG MOVE

March 2017

The Confederation of European Security Services (CoESS) welcomes the opportunity to comment on the study on options for the Security of European high-speed and international rail services commissioned by DG MOVE and presented at the LANDSEC Committee.

As an introduction and general observation, CoESS members hold the view that the study is well documented, complete and accurate and that the methodology is appropriate.

CoESS member companies have a long experience and much expertise in offering security services in train stations, for high-speed trains or regular trains. This paper seeks to add value to the data and information gathered in the study by offering a description of general principles and best practice in train station security.

General principles:

As the study recommends, there is a need for a **better understanding of the threat(s)**, and this requires:

- Resources to be dedicated to **intelligence gathering** in the Member States, in such a way that allows for anticipation of threats rather than post-event response;
- An **open channel of communication** between intelligence services of Member States across the EU, and possibly beyond;
- A 2-way open channel of communication for **private security companies and relevant law enforcement** and/or intelligence authorities, so that:
    - This can support investigation of criminal cases;
    - (Private) security agents know what to look for as being "suspect" or "unusual" – for those attacks that are being planned, it is a well-known fact that criminals will go on reconnaissance, take notes & pictures, do a dry run, etc.
    - Any observation of unusual behaviour can be reported to the adequate authorities in a swift manner.
    - Observations can be used in analyses, changes in trends and the overall threat

Jan Bogemansstraat | rue Jan Bogemans 249 | B-1780 Wemmel Belgium
T +32 2 462 07 76 | F +32 2 460 14 31
chantal@coess.eu | coess.org

picture;

- If the level of threat is heightened, private security companies should be part of the priority stakeholders to inform;

Barriers:

- The **legal framework in place** in the Member States generally does not support this 2-way channel. This can create frustration when PSCs provide information to the police, and little or no information is returned, because PSCs don't have a license to receive or handle sensitive information from the police or intelligence services. In order to achieve the objective of effective cooperation, it is therefore important that this issue is addressed, so that a clear framework can be established for the exchange of relevant information between PSCs and law enforcement / intelligence agencies.
- The **security industry handles classified information** for a number of clients, and undertakes assignments in locations where there is a statutory duty of confidentiality.

Security measures should be **risk-based, proportional and therefore adapted to the location** – this has been emphasised by many participants in the conference on transport security organised by the Commission in November 2016;

Security in train stations, as is the case for most transport infrastructure, involves **multiple stakeholders**. **Smooth cooperation and communication** between all stakeholders is therefore a key factor for a successful security policy and operation. If security is to be taken seriously, it can only be within a **dynamic process (Plan Do Check Act mode), where security - as well as safety - is considered as a chain**, within which each stakeholder knows its mission, duties, role and responsibilities, understands uses and supports smooth and effective processes, and communication follows a clear and efficient path so that security can be improved in a constant way.

Likewise, creating a **security culture**, not only within the **staff** of all **stakeholder** organisations, but also with **users**, is a winning strategy in anticipating both security and safety issues. The principle of "if you see something, say something", awareness campaigns and messages for both staff and users, need to be repeated on a regular basis to keep them alert to possible dangers and informed on how / to whom issues should be reported. **Hot lines** are being created in a number of countries to this end. In a medium to long term, a single telephone number or application for the whole of the EU could be foreseen, or at least a number that is valid on the same train line even if it crosses borders. In emergency situations, people will act in "automatic pilot", and for this reasons **"automatisms" need to be created**.

Jan Bogemansstraat | rue Jan Bogemans 249 | B-1780 Wemmel Belgium
T +32 2 462 07 76 | F +32 2 460 14 31
chantal@coess.eu | coess.org

Last but not least, these general recommendations, as well as the specific recommendations and best practice are based on the assumption that, when selecting private security companies to perform missions in any of type environment, **cost is not the only criteria of choice**. Regretfully, we observe that this is still rarely the case, and quality hardly comes into account for selecting private security providers. There are even cases of procurement (public and private) where the cost of the contract is lower than the collective bargaining minimum salary. As a Social Partner of UNI Europa, and member of the EU Undeclared Work Platform, CoESS feels the need to flag such practices as unacceptable and a clear encouragement to undeclared work. CoESS and UNI Europa have published a manual – entitled **"Buying Quality Private Security Services"** with financial support of the European Commission, which guides buyers of private security services through the **quality criteria to look for**. The guide can be downloaded in 14 languages on the securebestvalue.org website http://www.securebestvalue.org

Specific recommendations:

Based on the locations and the risk assessment, a **different and proportional "mix" of measures** needs to be put in place, which will include security by design, physical security, technology and guarding.

- **Security by design** and / or **physical security**, for example:
    - For Hostile Vehicle Mitigation:
        - Concrete blocks
        - Art that blocks
        - Gabions
        - Bollards
        - Fences
        - Anything that can make it difficult for a vehicle to get close to what you want to protect.
    - Hostile person mitigation:
        - Perimeter protection
        - Fences
- **Staff**:
    - Procedures for hiring and background checks, especially for the staff having access to certain sensitive locations;
    - A safety / security at work policy in place, which enables early detection of insider threats;
    - Regular training / information campaigns to make all staff feel responsible for safety and security.

Jan Bogemansstraat | rue Jan Bogemans 249 | B-1780 Wemmel Belgium
T +32 2 462 07 76 | F +32 2 460 14 31
chantal@coess.eu | coess.org

- **Procedures**
  - **Synergies** exist, and should be fully exploited, **between logistics, health and safety and security procedures**. Logistics enable knowing who/what should be where and when, and therefore can be used as source of information and baseline to identify irregularities. Limiting access to some areas has benefits from health and safety as well as security perspectives. These are just a couple of examples to highlight the interest of looking for these synergies and making the information smooth and available to those who need it, when they need it.
- **Technology and Guarding**
  - **Continuous patrols** in departure and arrival zones
  - Periodical control of **lockers** (left luggage);
  - Special attention in **ticket offices** and **toilets areas**, especially with crowds;
  - Close control of **regular station population** that may be perceived by the general public as potentially bothersome or engaged in unlawful activity (e.g. beggars, drug-addicts and well-known pickpockets);
  - **Fast intervention** in case of arguments to escalation to fights;
  - **Access control** for sensitive areas of the stations and trains;
  - **CCTV** – we expect fast increase in the number of face recognition and/or detection behaviour cameras;
  - If the location is under a particular high threat, **X-ray equipment** for luggage and **Walk Through Metal Detectors** can also be used.

  The above measures have to be based on **operational procedures** and supported by a **CCTV controlled from a Control Room** operated by security specialists duly qualified for the duties to be performed.

CoESS and its members are at the Commission's disposal to provide the Commission for any further information or more detailed examples of best practice.

Catherine PIANA
Director General

CoESS acts as the voice of the private security industry, covering 23 countries in Europe, of which 19 in the EU, representing 2 million licensed guards, over 45,000 companies and generating a turnover of €41M+.

The private security services provide a wide range of services, both for private and public clients, ranging from Ministry/EU Institutions buildings to nuclear plants, airports, critical infrastructure facilities, inter-modal transport hubs, public transport stations and areas, national governmental agencies and institutions (such as asylum seekers centres, public hospitals, universities, etc.).

Jan Bogemansstraat | rue Jan Bogemans 249 | B-1780 Wemmel Belgium
T +32 2 462 07 76 | F +32 2 460 14 31
chantal@coess.eu | coess.org