steer davies gleave

Study on options for the security of European high-speed and international rail services

Final Report
December 2016

European Commission

Our ref: 22894101
Client ref:
MOVE/A4/SER/2015/637

steer davies gleave

Study on options for the security of European high-speed and international rail services

Final Report
December 2016

European Commission

Our ref: 22894101
Client ref:
MOVE/A4/SER/2015/637

Prepared by:

Steer Davies Gleave
28-32 Upper Ground
London SE1 9PD

+44 20 7910 5000
www.steerdaviesgleave.com

Prepared for:

European Commission
Directorate-General for Mobility and Transport, MOVE A4
Rue de Mot 28
B-1040 Brussels
Belgium

Contents

Figures

Tables

Appendices

Executive Summary

Introduction

In August 2015, an individual boarded a high-speed Thalys train with a number of concealed weapons, and an incident ensued in which four passengers were injured. Following the incident, the European Commission (the Commission) was tasked with examining the impacts of possible initiatives for improving rail transport security in the European Union. As part of this work, the Commission asked Steer Davies Gleave to undertake a study of the options for implementing appropriate and proportionate security measures, at a Union-wide level, to improve the security of high-speed and international rail services. The study covers security of these services as a whole, including on infrastructure, stations and trains.

High-speed and international rail services

For the purposes of this study, we sought to identify the number of rail services within Europe that can be classified as:

- high-speed rail services (according to the existing EU definition of high speed);
- international rail services, of all speeds, that cross both internal Member State borders and also external borders to non EU Member States; and
- combined high-speed and international rail services.

Our principal sources of data on rail services were as follows:

- We used Eurostat data on international services as a control total of passenger numbers.
- We used the European Rail Timetable January 2016, as a consistent source of the rail services which should in principle be operating during 2016.
- We used our own desk research, particularly on the websites of Railway Undertakings (RUs) and Infrastructure Managers (IMs).

We concluded that accurate data was available in only limited areas, such as the number of Member States with international rail services, and the number of stations served by high-speed services (which RUs often show on a clear "promotional" map). Our estimates of the number of services relevant for the study currently operating within the European Union, together with the associated demand, are shown below.

Estimates of scale of high-speed and international rail services (summary)

Data	EU total	International	International high-speed (>260 km/h)	International high-speed (>210 km/h)	High-Speed (>260 km/h)	High-Speed (>210 km/h)
Passenger numbers per year	9,200 billion	78 million EU 14 million CH+NO 4 million other	Order of 40 million	Order of 45 million	Order of 200 million	Order of 225 million
Services each way per typical weekday		650 intra-EU 50 to CH+NO 20 to others	Order of 300 intra-EU	Order of 350 intra-EU	Order of 5,000	Order of 6,000
Stations served	26,000 (estimate)	1,000 in EU 100 outside EU	Order of 200	Order of 220	400	500
Station calls per typical weekday		6,500 in EU 500 in CH+NO 200 in others	Order of 3,000	Order of 3,400	Order of 15,000	Order of 18,000

Source: Steer Davies Gleave analysis

Stakeholder consultation

We interviewed and/or received a written submission from 68 stakeholders from 21 Member States, including transport ministries, regulators with security responsibilities, rail operators, infrastructure managers and a number of pan-European organisations representing different stakeholder groups. Their responses suggested wide variation across Member States in their perceptions of the security threat, approach to the assessment of risk and adoption of different interventions for improving rail security.

Assessment of the current situation

We investigated and documented the current security situation on high-speed and international rail services operating in Europe. This included two key strands of work: investigation of data defining the current level of high-speed and international rail services, and collection of information on current rail security arrangements across the European Union. Security relates to interventions intended to reduce the frequency and impact of terrorist acts as well as a wide range of other types of crime affecting rail infrastructure, stations and trains.

We agreed with the Commission that, for the purposes of this study, security should be defined to include the following types of crime on high-speed and international rail services:

- violent crime, in particular terrorism;
- non-violent crime involving damage to railway infrastructure and rolling stock such as metal and cable theft and graffiti; and
- other non-violent other crimes affecting passengers and staff such as endangering safety, obstruction, trespass and luggage theft.

Crime on the railway is already being addressed by a wide range of activities which can be described as security interventions. At the most basic level, as with most public and private property and buildings, these include provisions such as fences, gates, walls, doors, locks, lights, staff and patrols.

We have not been able to estimate the total scale and cost of all types of crime on high-speed and international rail services. However, on the basis of the limited data available, the total quantifiable annual cost of security failures on EU's rail networks is €370 million or more, of which almost €40 million arises on, or affects, high-speed and international services. The largest quantifiable element relates to vandalism and graffiti. At the same time, we note that the impacts of individual terrorist attacks can be very substantial, but it is not possible to predict their scale and frequency with any confidence.

Problem definition

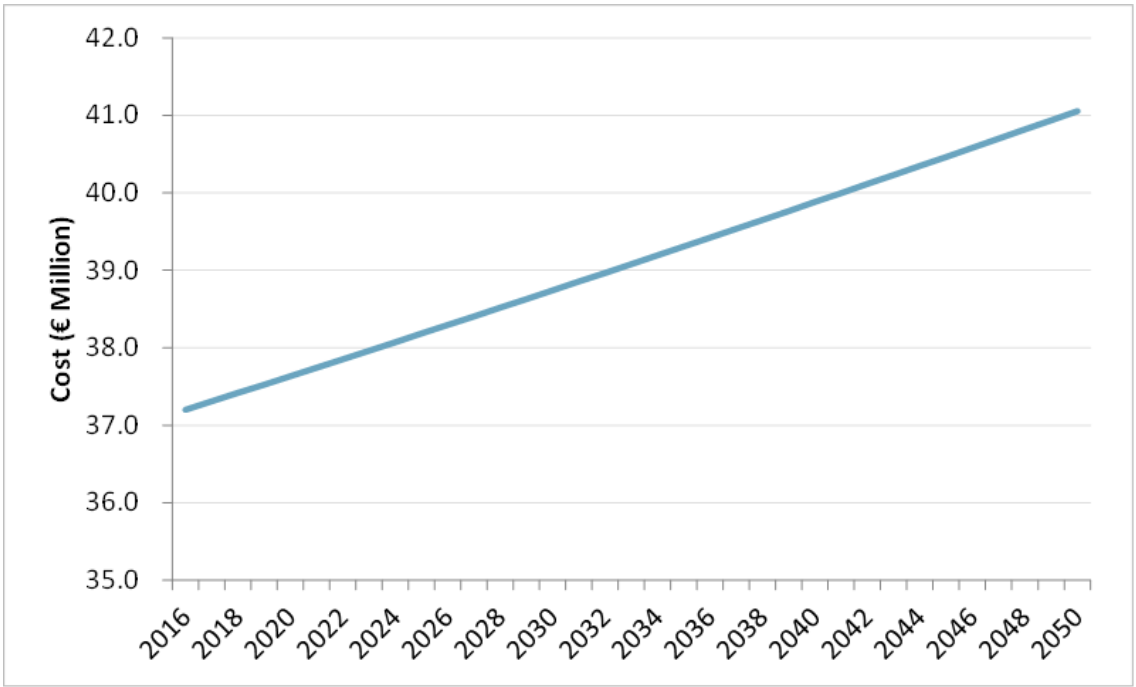
Based on responses from the stakeholder consultation and evidence gathered from a review of academic and industry literature, we sought to define the problem arising in relation to rail security across the European Union. More specifically, we investigated its scale, causes and extent to which it is likely to persist in the absence of EU intervention. We developed a problem tree (illustrating underlying root causes and problem drivers as well as the links between them) supported, as far as possible, by evidence and quantification of the scale of the problem.

Our analysis indicates that this problem can be linked to:

- an insufficient understanding of the security threat, broadly defined to include both violent and non-violent crime, partly an inevitable result of the infrequency of certain types of security incident (particularly terrorist attacks) but also due to inadequate reporting and sharing of data;
- an inadequate response to the threat to the EU rail network as a whole, reflecting an understandable focus on specific threats arising at the national level (which vary significantly between Member States) and weak incentives to address ill-defined and poorly understood threats (particularly in the face of strong commercial pressures within rail undertakings and infrastructure managers across Europe);
- different approaches to the mitigation of security risks among rail industry decision-makers in different Member States, driven partly by cultural differences but, more importantly, by the application of inconsistent methodologies for assessing risk; and
- fragmentation of, and gaps in, security arrangements and responsibilities at both the national and EU level, a result of failures to coordinate security measures on international services and accentuated by the growth of the international rail network.

We also estimated how the costs of security failures might evolve over time on the assumption that threat levels as well as the number and scale of security failures (including terrorist attacks, theft of railway assets and vandalism) remained constant. The increase in costs shown in the figure below reflects the impact of both casualties among passengers and staff and service disruption, whether due to violent or non-violent crime, on a growing European economy. For the purposes of the impact assessment, it represents an element of the baseline against which the incremental impacts of options for improving rail security can be calculated.

Evolution of costs of security failures



Source: Steer Davies Gleave analysis based on estimated costs of security failures and application of OECD long term GDP growth forecasts

In defining the baseline position, we also considered how threat levels might evolve over time and their impact on demand for international and high speed services. We have assumed that

threat levels for individual Member States currently defined by the UK Foreign Office remain broadly constant over time, and that these are consistent with demand growth derived using growth rates from the PRIMES-TREMOVE transport model.

Definition of objectives

From our definition of the problem we derived a number of objectives to support the development of options for intervention. These included a general objective and specific objectives aligned with different aspects of the problem. Our general objective captured the need "to reduce the risk and impact of criminal acts on the European rail network", recognising both the prevention and mitigation dimensions of the security issue. Our specific objectives are aligned with different aspects of the problem and are reproduced below.

Rationale for specific objectives

Problem drivers	Specific objective	Rationale/comment
Insufficient understanding of the threat	**Shared EU understanding** Ensure relevant stakeholders have a more thorough and shared understanding of the security threat across the EU.	While the problem is partly the result of underlying data limitations, more could be done to ensure that rail industry and other stakeholders across the EU share a better understanding of the threat.
Inadequate response to the threat	**Reflect EU-wide benefits** Ensure that the response to the threat adopted by the industry takes full account of the economic and social benefits of security interventions across the EU.	There is a need to address externalities, in the form of security benefits that are not taken into account in commercial decision-making. At the same time, the economic and social benefits of security interventions need to be fully considered by public sector decision-makers determining investment priorities.
Different approaches to mitigation in Member States	**Consistent risk assessment** Ensure that mitigation of the security threat in different Member States is based on a consistent assessment of underlying risks.	While the specific security interventions adopted in different Member States will vary according to circumstances, it is important that common risks are assessed using the best methodologies available to the industry.
Fragmentation and gaps in security coordination	**Holistic and coordinated approach** Ensure that the security threat to high-speed and international rail services is addressed in a holistic and coordinated manner.	Mitigation measures should be applied consistently and coherently to an entire service or group of services, so that measures employed on one part of a journey cannot be circumvented or undermined by perpetrator actions taken on another part.

Source: Steer Davies Gleave analysis

Policy options

We identified and sifted a number of possible security interventions, combined these into policy measures and then assembled three overall policy options for assessment. We rejected one of the security interventions suggested in our Terms of Reference, nominative ticketing, and the more restricted intervention of passenger identity checks. Either intervention would raise both practical difficulties for operators and barriers to travel for passengers.

The nature of the security issue, the problem drivers, and the specific objectives, means that policy options are not mutually exclusive. In particular, no single measure, except closure of all high-speed and international rail services, could eliminate all theft, vandalism, graffiti, crime and terrorism associated with them. This means that:

- Any one specific objective might best be addressed by a number of policy measures.
- Any one policy measure might contribute to addressing a number of specific objectives.

We adopted an approach of packaging the policy measures into the following distinct options, with progressively greater degrees of intervention:

- Option 1: a minimal package, designed to make at least some contribution to addressing each objective.
- Option 2: intermediate package, incorporating additional policy measures, including some which we had identified as contingent on the policy measures in Option 1.
- Option 3: a comprehensive package, incorporating all the policy measures retained following the sift.

Our proposed options are set out in the following table.

Policy options

Option 1	Option 2	Option 3		Policy measure	Mandatory/ guidelines
●	●	●	1A	Reporting and monitoring national security data	M
		●	1B	Researching and disseminating worldwide security data	G
●	●	●	2A	Emergency egress and access to stations	G
		●	2B	Blast-resistant features on stations	G
		●	2C	Blast-resistant features on trains	G
●	●	●	3E	S/SMS threat level protocols	G
	●	●	3A	S/SMS ensure exchange of information by relevant parties	M
	●	●	3C	S/SMS contingency planning and incident recovery	M
	●	●	3F	S/SMS liaison, incident response, drills and exercises	G
		●	3B	S/SMS recording of vulnerabilities and inspection regimes	M
		●	3D	S/SMS contingency IT, communications and spares	G
●	●	●	4A	CCTV on stations, with recording and facial recognition	M
●	●	●	4B	CCTV on trains, with recording and facial recognition	M
	●	●	4C	Deploying staff where they can observe	G
	●	●	4F	Staff vetting and access controls	G
		●	4D	Training station/train staff in risk and behaviour monitoring	G
		●	4E	Awareness promotion among passengers	G

Source: Steer Davies Gleave analysis

Analysis of options

Notwithstanding the challenges arising from lack of data, which are discussed in the main report, we sought to quantify as many impacts of policy options as possible. In some cases, it was possible to place a monetary value on a subset of those impacts. Where there was insufficient evidence to quantify impacts, we carried out a qualitative assessment of the scheme impacts. Again, where the evidence permitted, we sought to allocate a 'score' to distinguish the relative impact of policy options. Where there was insufficient evidence to determine a relative score, we have provided a commentary regarding the relative performance of policy options.

The range of impacts to be assessed was specified within the Terms of Reference for the study. Following a review of the 30 separate economic, social and environmental impacts

suggested in the Terms of Reference, we concluded these to be sufficiently comprehensive for the purpose of this Impact Assessment. We then screened the impacts to determine how they should be assessed and drew conclusions regarding the most appropriate methodology on the basis of the proportionality principle described in the Better Regulation Toolbox (Tool #9) and with reference to :

- the significance of the expected (intended and unintended) impacts;
- the nature of the options under consideration;
- the maturity of the markets through which options will be delivered, such as security equipment suppliers, enterprise-level risk assessments, staff training; and
- the availability of reliable evidence regarding monetary valuations for non-market impacts (such as travel time savings), direct and indirect behavioural responses and contextual data to inform the qualitative assessment.

Comparison of options

We used a Multi-Criteria Analysis (MCA) to combine monetary, quantitative and qualitative assessments against individual criteria to provide an indication of the overall performance of policy options, the outputs of which are summarised in the table below.

Overall performance of policy options

Option	Multi-Criteria Analysis score	Rank
Option 1	23.3	3
Option 2	49.8	2
Option 3	72.1	1

Source: Steer Davies Gleave analysis

It is clear from the results that policy option 3 is the best performing package of policy measures. This is in line with expectations given the incremental nature of the policy options, with option 3 being the most comprehensive.

Recommendations

In the light of these results, in particular the identification of Option 3 as the preferred option, we make the following recommendations.

Recommendation 1: reporting and monitoring of security data

We recommend that the Commission establishes a Union-wide framework for reporting and monitoring of data relating to the security of high speed and international rail services. The monitoring framework should be supplemented with guidance on areas for further research and exchange of information on rail security beyond the European Union.

Recommendation 2: design of trains and stations for added security

We recommend that the Commission, in collaboration with relevant international and national bodies, prepares guidance on the design of station access and egress with a view to improving security at stations used by high speed and international services. We also recommend that it prepares guidance on standards for blast-resistance on trains and at stations.

Recommendation 3: risk assessment and contingency planning

We recommend that Member States should be required to ensure that rail organisations involved in the operation of high speed and international rail services introduce Security Management Systems (SMSs). Such systems should be based on an explicit risk assessment process and subject to approval by an appropriate national regulatory body.

We also recommend that the Commission, in collaboration with relevant national bodies, prepares guidance on:

- best practice in relation to the design of relevant information technology and communications systems to withstand attacks and the deployment of reserves and spare equipment for use following a security incident;
- appropriate liaison with emergency services and other relevant agencies as well as drills and exercises in incident response; and
- protocols for responding to changes in security threat levels identified at the European, national or local level.

Recommendation 4: monitoring and awareness of security risks

We recommend that the Commission, in collaboration with relevant bodies, prepares common mandatory standards for CCTV on trains and stations, recovering requirements for recording capability as a minimum and, optionally, for facial recognition and real time monitoring. In addition, Member States should be required to identify responsibilities for undertaking CCTV monitoring activity.

We also recommend that the Commission should prepare guidance on:

- the appropriate deployment of staff for the purposes of observing behaviour on stations, drawing on principles of good practice already adopted;
- training of on-train and station staff in security risks and behaviour monitoring;
- campaigns promoting awareness of security among passengers; and
- processes for vetting of staff and limiting access to particularly vulnerable or sensitive locations.

1 Introduction

Purpose and scope of the study

1.1 In August 2015, an individual boarded a high-speed Thalys train with a number of concealed weapons, and an incident ensued in which four passengers were injured. Following the incident, the European Commission (the Commission) was tasked with examining the impacts of possible initiatives for improving rail transport security in the European Union. As part of this work, the Commission asked Steer Davies Gleave to undertake a study of the options for implementing appropriate and proportionate security measures, at a Union-wide level, to improve the security of high-speed and international rail services. The study covers security of these services as a whole, including on infrastructure, stations and trains.

1.2 The study has covered a number of tasks, defined in our Terms of Reference, which can be summarised as shown in Table 1.1.

Table 1.1: Summary of study tasks

Task	Description
1	Collection of data supporting an analysis of the current legislation and arrangements relating to rail security in different Member States, covering planning, specific security interventions, training, incident management, contingency arrangements and cooperation between agencies and across borders.
2	Definition of security options to be analysed, building on a set of initial options defined by the Commission (including mandatory requirements, guidelines and exchange of best practice as well as the currently anticipated evolution of current arrangements).
3	Quantitative and qualitative analysis of the advantages and disadvantages of the options, taking account of economic, social and environmental impacts.
4	Comparison of options on the basis of their relative coherence, effectiveness and efficiency, noting issues of proportionality and impacts on different stakeholder groups.

1.3 This Final Report describes the methodology applied, the data used and the findings of the study.

Overview of methodology

1.4 Where possible, we have carried out this study in accordance with the Commission's Better Regulation Guidelines[1] using tools and techniques described in its Better Regulation Toolbox[2]. This report follows broadly the order of our analysis:

[1] Commission Staff Working Document: Better Regulation Guidelines, SWD (2015) 111 final, Strasbourg 19.5.2015.

[2] Better Regulation Toolbox, European Commission.

- **Desk research and literature review:** we undertook an extensive investigation of relevant academic literature, supplemented by desk research to identify key data sources to support the analysis. A bibliography identifying the literature reviewed is provided in Appendix A.
- **Stakeholder consultation:** we interviewed and/or received a written submission from 68 stakeholders, including transport ministries, regulators with security responsibilities, rail operators, infrastructure managers and a number of pan-European organisations representing different stakeholder groups. The stakeholder questionnaire is attached as Appendix B and a full list of the stakeholders contacted is attached as Appendix C.
- **Assessment of the current situation:** as a starting point for the analysis, we investigated and documented the current security situation on high-speed and international rail services operating in Europe. This included two key strands of work: investigation of data defining the current level of high-speed and international rail services, and collection of information on current rail security arrangements across the European Union, documented in Appendix D. Both strands were used to inform a baseline position on security on high-speed and international rail services for the purposes of subsequent analysis.
- **Definition of the problem:** from the assessment of the current situation we developed of a problem tree (illustrating underlying root causes and problem drivers as well as the links between them) supported, as far as possible, by evidence and quantification of the scale of the problem.
- **Definition of objectives:** from our definition of the problem we derived a number of objectives against which to test options for intervention. These included a general objective and specific objectives aligned with different aspects of the problem.
- **Formulation of options:** we identified and sifted a number of possible security interventions, combined these into policy measures, and then assembled from the security measures options to be assessed.
- **Analysis of options:** to the extent possible with the data available, we assessed the options in accordance with the Better Regulation Guidelines.
- **Comparison of options:** we compared the results of this analysis for each option.

1.5 We discuss in turn below our desk research, literature review and stakeholder consultation.

Desk research and literature review

1.6 Early in the study we carried out a literature review to identify information which might be relevant to the issues of security. The documents we examined are listed in Appendix A and allocated into six broad categories:

- descriptions of high-speed and international rail services and travel;
- descriptions of terrorists attacks and their consequences;
- security measures;
- legislation and acceptability;
- the costs of security measures; and
- the benefits of security measures.

1.7 Where relevant, we refer to the literature throughout this report in the our work to identify the current situation, the current problem, a baseline going forward, and a quantitative and qualitative impact assessment of options.

Workshop and stakeholder consultation

Workshop

1.8 We held a one-day workshop in Germany on 27 April 2016, hosted by the Federal Ministry for Transport and Digital Infrastructure (Bundesministerium für Verkehr and digitale Infrastruktur, BMVI) in Bonn, followed by a site visit to Köln Hauptbahnhof, hosted by DB Station&Service. In the course of the workshop we interviewed the stakeholders listed in Table 1.2.

Table 1.2: Stakeholders at workshop in Bonn/Köln

Organisation	Name	Role
Bundesministerium für Verkehr and digitale Infrastruktur, BMVI (Federal Transport Ministry)	Erich Schmid	Head of the Crisis Management Task Force
	Daniel Arzani	Crisis Management Taskforce
	Wolfram Neuhöfer	Head of Division Railway Technology; Operating Safety; Interoperability; National Investigation Body (LA 15)
	Ricardo Liesig	
Bundesministerium des Innern (Federal Interior Ministry)	Dirk Paulmann	
Bundespolizei (Federal Police)	Franz Vogl	
DB Station&Service	Host	
DB Sicherheit	Thorsten Buhrmester	Senior Referent Konzernsicherheit
DB	Bettina Hunold	Transport Policy Europe (TPE)
VDV	Marcus Gersinke	Head of Railway Business Management

1.9 We also studied the practicalities of operation of the station including the despatch of domestic, high-speed and international rail services from the same platform at short intervals. Further details are given in Appendix D, Appendix Table D.14 and Appendix Figure D.4.

Stakeholder consultation

1.10 As required by the Terms of Reference we also contacted a number of stakeholders:

- Appendix B shows the questionnaire sent to, or discussed with, stakeholders.
- Appendix C lists the stakeholders we contacted.
- Appendix D summarises the principal findings from the consultation.

Stakeholder questionnaires

1.11 We agreed with the Commission a stakeholder questionnaire, a copy of which is provided as Appendix B.

1.12 The design and length of the questionnaire took into account our experience of stakeholder consultation in previous studies for the Commission. With written questionnaires, there is a trade-off between the length of the questionnaire and both the response rate and the number of questions to which stakeholders provide an answer. Our experience of such consultations is that, as questionnaires grown longer:

- The overall response rate falls.
- The number of questions completed falls: in particular, respondents may ignore the later questions.
- The thoroughness of the answers falls: in particular, respondents may give only brief answers to later questions.

1.13 With stakeholder interviews, a similar issue arises, particularly as relatively few stakeholders are willing to dedicated more than 45-60 minutes to an interview. This can lead to later questions being omitted, although in practice where time is limited our interviewees focus on the questions which appear most likely to provide new information.

1.14 The principal topics on which we sought information are summarised in Table 1.3.

1.15 Given the practical limitations discussed above, the questionnaire was largely restricted to factual but qualitative information about the past or current position. We were able to ask only limited questions about the cost, effectiveness or potential impacts of existing and potential security measures, and in practice neither expected nor were given significant quantitative information. This limitation had major implications for our subsequent attempt to carry out an impact assessment of possible options, as we discuss later in this report.

Stakeholder consultation process

1.16 In March 2016 we began the stakeholder consultation exercise, contacting the stakeholders listed in Appendix C. This list is based, with a few exceptions, on the list of stakeholders and the questionnaire presented to the Commission at the inception of the study.

1.17 Figure 1.1 summarises the stakeholder consultation process:

- 149 stakeholders were successfully contacted.
- 53 did not respond.
- 23 declined to participate.
- 5 agreed to be interviewed but were in the event unable to agree an interview date.
- 68 were interviewed and/or made a written submission.
- 21 Member States were represented in the participants.

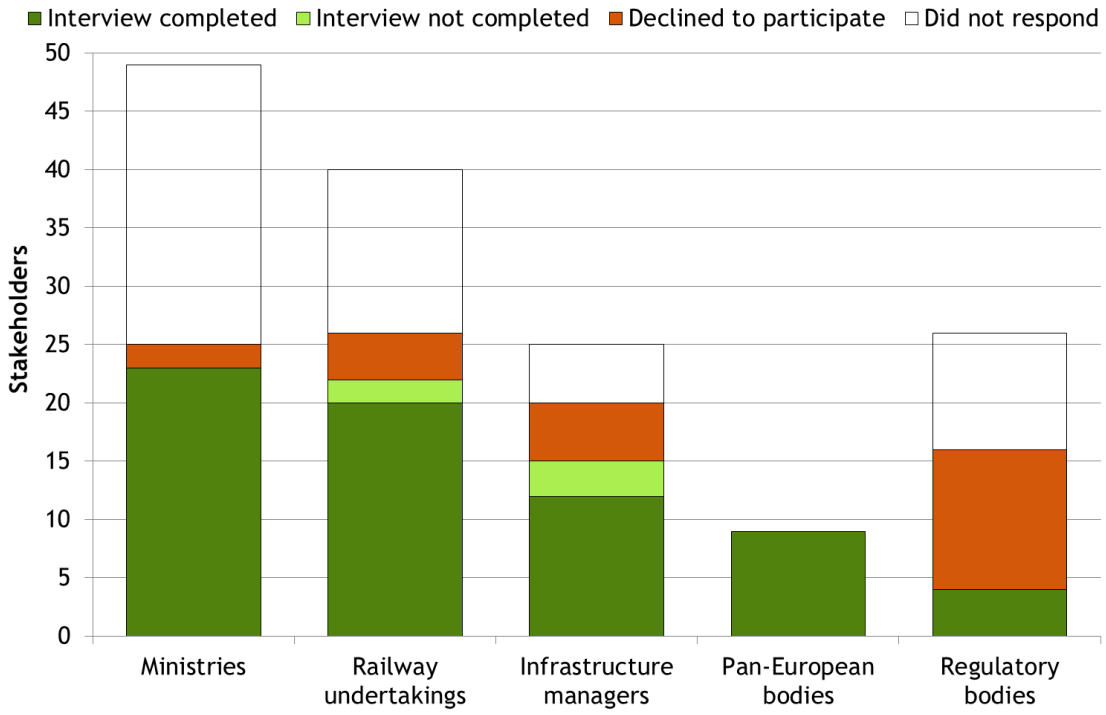
1.18 This represents an overall effective response rate of 46%. As Figure 1.1 shows, we successfully contacted stakeholders of every type, although only a small proportion of regulatory bodies (4 out of 26, or 15%, all of whom were interviewed and/or made a written submission) were willing to participate. In practice, as we recognise in Table 1.4, many regulatory bodies have no role in security, and there is no requirement in European law for them to do so.

Table 1.3: Overview of stakeholder questionnaire

Questions	Topic	Rationale
1-2	Rail services in scope	Which stakeholders provide, or are involved in the provision of, high-speed or international rail services.
3	High level threat assessment	Which stakeholders maintain a risk assessment process, and whether this includes security risks.
4-7	Relevant and evolution of policy and legislation	Which stakeholders can identify legislation and policy which relates to rail security.
8-13	Roles and responsibilities	Which stakeholders have which roles in relation to rail security.
14-15	Costs of rail security	Whether any costs are identified as relating to rail security, and which bodies bear them.
16-20	Cooperation between authorities and stakeholders	How stakeholders cooperate, and with whom, domestically.
21-22	Threat levels	Which stakeholders are aware of a national system of categorising threat levels
23-25	Cooperation between authorities and stakeholders	How stakeholders cooperate, and with whom, internationally.
26-27	Research	Which stakeholders carry out, or are aware of, research into reducing the security threat to rail services.
28-34	Dealing with incidents	Which stakeholders have contingency plans, exercises or training related to security or threat awareness.
35-36	Specific threats	Which stakeholders have plans relating to cyber-threats or to chemical, biological or radiological (CBR) weapons.
37-48	Existing security measures	Which stakeholders, if any, have measures: • To restrict access to stations • To avoid concentrations of people • To detect unusual behaviour • To check the identity of passenger, and how far in advance this is done • To mitigate the effect of alerts, such as through rapid evacuation • To train railway and third party staff to recognise unusual behaviour • To train railway and third party staff to respond to terrorism • To screen passengers or baggage before boarding, and on which trains • To patrol stations • To identify and protect vulnerable parts of the infrastructure
49-50	Susceptibility of train services	Which stakeholders, if any, consider particular types of train service more susceptible to terrorist attack.
51	Other views on security	Stakeholders' views on: • The success of existing security measures • Whether anti-terrorism measures reduce other crime • The shortcomings of the arrangements • Likely developments, and whether they deter passengers • Their highest security priority

Source: stakeholder questionnaire, see Appendix B for details.

Figure 1.1: Stakeholder consultation and responses



Stakeholder consultation coverage

1.19 Table 1.4 below summarises how the stakeholders we successfully consulted are affected by security incidents and whether they are responsible for detecting, deterring, mitigating or responding to security incidents.

Table 1.4: Key stakeholders causing or affected by the problem

Group	Stakeholder group									Members of group	Stakeholders contacted
	Security incidents							Security interventions			
	Cause problem	Deter	Detect	Mitigate	Respond	Immediate impacts	Delayed impacts	Direct impacts	Delayed impacts		
Railway funders		●								Competent national authorities	●
		●								Competent regional and local authorities	
Security agencies		●	●	●						Multinational security organisations	
		●	●	●						National intelligence services	
		●	●	●	●			●		National police	●
		●	●	●	●			●		Local police	
Railway security agencies		●	●	●	●			●		Railway police	●
		●	●	●	●			●		Railway security services	●
		●	●	●	●			●		Contracted security staff	
Railway actors		●	●	●	●	●		●		Infrastructure Managers (IMs)	●
		●	●	●	●	●		●		Station Managers	●
		●	●	●	●	●		●		Railway Undertakings (RUs)	●
		●	●	●	●	●		●		Metro and onward transport organisations	
						●		●		Freight operators and customers	
Passengers			●			●	●	●	●	Passengers, escorts and meeter-greeters	
Railway guests			●			●	●	●	●	Restaurant and retail staff	
			●			●	●	●	●	Non-passengers	
Responders						●				Civil defence and fire services	
						●				Ambulance and hospital staff	
						●				Repair workers	
Passengers' contacts						●	●		●	Friends and relatives	
						●	●		●	Employers and colleagues	
Community							●		●	Operators and users of other modes	

Source: Steer Davies Gleave analysis

1.20 Note that, in the specific context of a study on rail security:

- It was not practicable for consultation to include stakeholders who cause security issues.
- It was not practicable for consultation to extend to the many stakeholders outside the rail industry who deal with, or suffer the consequences of, security issues.

1.21 These constraints further limit the scope of the stakeholder consultation to identify the impacts of possible new options to address security.

Organisation of this report

1.22 The remainder of the report is organised as follows:

- Chapter 2 discusses the definition of high speed and international services and provides an estimated quantification of the scale of such services;
- Chapter 3 provides a definition of security in the context of high speed and international rail services;
- Chapter 4 sets out our definition of the problem, drawing on the results of the stakeholder consultation exercise and literature review and describes our baseline projection of the scale of the problem for the purposes of the impact assessment;
- Chapter 5 defines a general objective and a number of specific objectives for any intervention at the European Union level designed to address the problem;
- Chapter 6 describes a number of potential security interventions that could be covered by future policy and sets out the results of an initial sifting exercise;
- Chapter 7 describes a series of policy measures combining security interventions remaining following the sift;
- Chapter 8 defines three policy options for assessment, providing for successively greater intervention to improve security;
- Chapter 9 describes our approach to the impact assessment, including both quantitative analysis and qualitative assessment of each option;
- Chapter 10 sets out the results of the impact assessment and provides a comparison of the options; and
- Chapter 11 summarises our findings and sets out our recommendations for policy.

Organisation of the report appendices

1.23 The report also includes the following appendices:

- Appendix A lists the literature sources reviewed during the study.
- Appendix B reproduces the questions raised with different groups of stakeholders.
- Appendix C provides a list of stakeholders contacted during the course of the consultation and a breakdown of how they responded.
- Appendix D describes the findings from the stakeholder consultation, comparing approaches to rail security in different Member States and providing additional commentary on specific issues.
- Appendix E describes the analysis and assumptions that were used for the impact assessment.
- Appendix F sets out the results of the qualitative scoring of policy measures and provides summary rationales for the various scores.

2 Defining high-speed and international rail services

Introduction

2.1 In accordance with the Terms of Reference, we sought to identify the number of rail services within Europe that can be classified as:

- high-speed rail services (according to the existing EU definition of high speed);
- international rail services, of all speeds, that cross both internal Member State borders and also external borders to non EU Member States; and
- combined high-speed and international rail services.

2.2 We begin with illustrations of services which may fall into these categories.

High-speed rail services

2.3 Figure 2.1 below shows a 200 km/h capable High Speed Train (HST) calling at Liskeard station in Great Britain, and illustrates a number of points about high-speed services.

Figure 2.1: Example of a high-speed rail service

Source: **www.stationmaster.me.uk**, Liskeard station, Great Britain, with 200 km/h High Speed Train (HST)

The train

2.4 The train shown in Figure 2.1 was designed in the 1970s to operate at 200km/h, and is still capable of operation at this speed. However, the trains are now approaching 40 years old, and if they were "de-rated" to a lower maximum speed, they would no longer be considered high-speed trains and this photograph would no longer show a high-speed service.

The station

2.5 Liskeard station serves a population of under 10,000 people in a rural area and in 2014/15 was used by an average of just under 1,000 passengers a day[3]. It is served by trains for approximately 17 hours on a typical weekday, which suggests that the mean hourly usage is around 30 boarding and 30 alighting passengers. In practice, we would expect that demand is highly peaked and that modal hourly usage is fewer than 10 boarding and 10 alighting passengers. However:

- The station is only staffed for 12½ hours on weekdays, and unattended for a further 4½ hours during which trains are still operating.
- The platforms can be accessed directly from the car park and the road.
- Platform 3, not visible from the main station, or staffed at any time, is reached from the other platforms by crossing a public road, although it is not used by high-speed trains.

2.6 This combination of lack of continuous staffing, and open access from car park and public roads, may limit the levels of security which can be provided at the station.

The infrastructure

2.7 High Speed Trains calling at Liskeard may travel at 200km/h elsewhere on their journey, particularly between Bristol and London Paddington. However, the nearest point at which they operate at this speed is over 250 kilometres by rail from Liskeard.

International rail services

2.8 Figure 2.2 overleaf shows an example of an international rail service, a train from Reutte in Tirol in Austria to Kempten in Germany, about to call at Ulrichsbrücke-Füssen in Austria.

The train

2.9 All trains serving Ulrichsbrücke-Füssen are diesel-powered and operated by Deutsche Bahn.

The station

2.10 The station, sandwiched between two roads, one of which is shown on the left of the photograph, consists of a single curved platform approximately 100 metres long with no facilities or staff. The station is served by ten trains each way per day over approximately 17 hours per day. We have found no data on passenger numbers[4].

[3] ORR station statistics, provided at http://orr.gov.uk/statistics/published-stats/station-usage-estimates

[4] DB informed us that they do not make systematic estimates of station usage.

The infrastructure

The infrastructure at Ulrichsbrücke-Füssen, a single-track line used in both directions, is maintained by ÖBB.

Figure 2.2: Example of an international rail service

Source: **www.pro-bahn.de**, Ulrichsbrücke-Füssen station on Deutsche Bahn's Außerfernbahn in Austria.

2.11 In this chapter, we discuss and present the available data on high-speed and international services and address a number issues relating to their definition.

Data availability

2.12 We sought to collect information on rail services relating to both the level of security threat and the cost of mitigating it. As far as possible, we obtained or estimated data on:

- the number of Member States with international rail services;
- the number of passengers per year on each type of service;
- the number of services operated in each direction per typical weekday;
- the number of train sets required to operate these services;
- the number of stations served by these services; and
- the number of station calls per typical weekday.

2.13 We also investigated the scope to disaggregate this data by state, route or service.

2.14 Our experience of seeking data in the rail industry is that information of this type is rarely collected, calculated or published by any rail industry bodies. As we noted above, the UK's Office of Rail and Road now produces annual estimates of station usage (2.5), but DB does not make comparable estimates on a systematic basis (2.10). We therefore reviewed the

availability of data from a number of sources, and assessed its reliability, as shown in Table 2.2, using the codes shown in Table 2.1.

Table 2.1: Key to availability and reliability of data in Table 2.2

Code	Meaning
A	Accurate data are available, collected and collated.
E	Estimates are possible from public sources, indicatively to within ± 10%.
I	Indicative estimates are available from public sources, indicatively to within ± 50%.
T	Timetable analysis would, in principle, allow accurate data to be derived for a specified day or, with additional work, week or month, but this would require disproportionate effort, given that networks and timetables continue to change and not all services are actually operated as timetabled. (A notable example is that imposition of identity checks on passengers entering Sweden has resulted in extended journey times, cancellation of station calls and cancellation of whole services in both Denmark and Sweden. We discuss this further in Table 4.6.)
U	Information is unobtainable from public sources or not available in practice. For example, railway undertakings do not normally identify, for any given train service, any of the maximum operating speed of the infrastructure used, the maximum operating speed of the rolling stock used, the maximum speed at which the stock is timetabled on the particular service, or the efficient minimum number of train sets and crew necessary to provide the service.

Source: Steer Davies Gleave analysis, see text for details.

Table 2.2: Availability and reliability of data on high-speed and international rail services

Data for assessment	Level of detail	International	International high-speed	High-Speed
Member States	Of 26 with rail	A	A	A
Passenger numbers per year	Total	E	I	I
	By state(s)	E	T	T
	By route or service	A/U	A/U	A/U
Services operated each way per typical weekday	Total	E	I	I
	By state(s)	E	T	T
	By route or service	T	T	T
Train sets required to operate services efficiently	Total	E	I	I
	By state(s)	U	U	U
	By route or service	E/U	E/U	U
Stations served	Total	E	I	A
	By state(s)	T	T	A
	By route or service	T	T	T
Station calls per typical weekday	Total	I	I	I
	By state(s)	T	T	T
	By route or service	T	T	T

Source: Steer Davies Gleave analysis, see text for details.

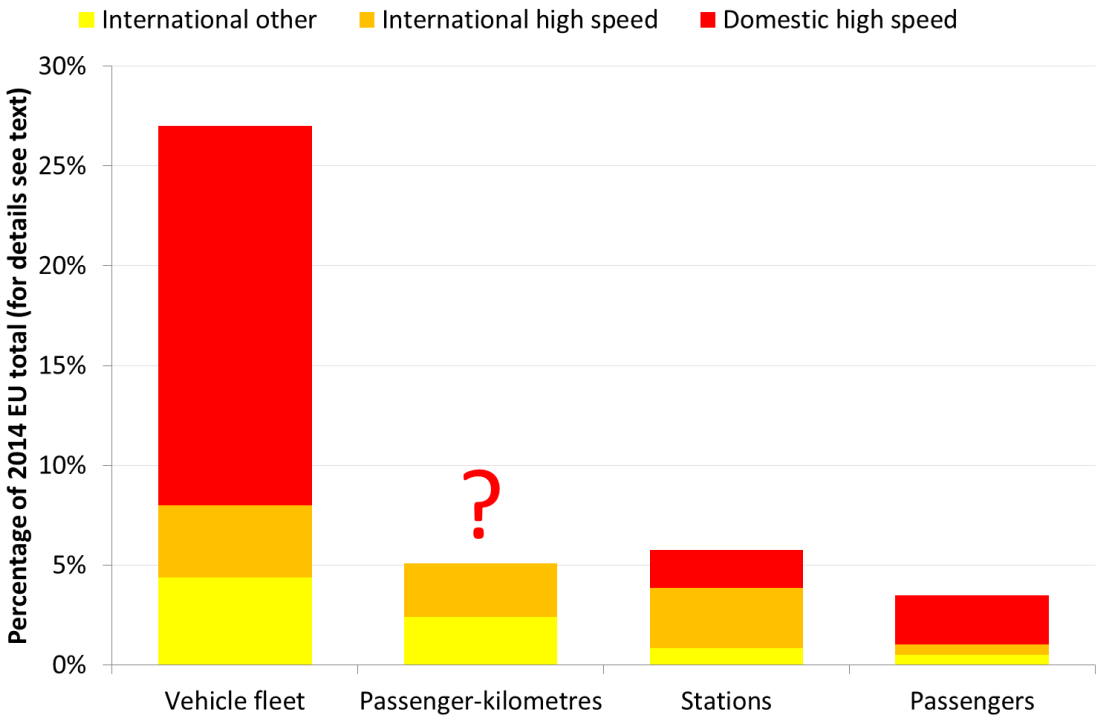
2.15 Our principal sources of data on rail services are as follows:

- We used Eurostat data on international services as a control total of passenger numbers.
- We used the European Rail Timetable January 2016, as a consistent source of the rail services which should in principle be operating during 2016.
- We used our own desk research, particularly on the websites of Railway Undertakings (RUs) and Infrastructure Managers (IMs).

2.16 We concluded that accurate data was available in only limited areas, such as the number of Member States with international rail services, and the number of stations served by high-speed services (which RUs often show on a clear "promotional" map). In contrast, information on the number of station calls by particular services could only be identified by complete analysis of the European Rail Timetable, and information on the number of train sets or crew used or required to operate any particular service could in most cases only be estimated, as we discuss below.

2.17 Our findings are summarised in Figure 2.3 and Table 2.3.

Figure 2.3: Estimates of share of high-speed and international rail services in EU total



Source: Steer Davies Gleave estimates, summarised in Table 2.3 below, for details see text.
Note: no estimates of total domestic high-speed passenger-kilometres found.

Table 2.3: Estimates of scale of high-speed and international rail services

Data	Level of detail	EU total	International	International high-speed (>260 km/h)	International high-speed (>210 km/h)	High-Speed (>260 km/h)	High-Speed (>210 km/h)
Member States		26 with rail	26	9	13	9 See Figure 2.9	13 See Figure 2.9
Passenger-kilometres per year	Total (Eurostat)	430 billion	22 billion				
Passenger numbers per year	Total (Eurostat)	9,200 billion	78 million EU 14 million CH+NO 4 million other	Order of 40 million	Order of 45 million	Order of 200 million	Order of 225 million
	By state		See Figure 2.6				
Services each way per typical weekday	Total		650 intra-EU 50 to CH+NO 20 to others	Order of 300 intra-EU	Order of 350 intra-EU	Order of 5,000	Order of 6,000
	By state		See Figure 2.5				
Train sets required to operate services	Total	50,000 vehicles	4,000 vehicles	Order of 200 sets 2,000 vehicles	Order of 220 sets 2,200 vehicles	1,050 sets 8,500 vehicles	1,200 sets 9,500 vehicles
	By state						
Stations served	Total	26,000 (estimate)	1,000 in EU 100 outside EU	Order of 200	Order of 220	400	500
	By state					See Figure 2.10	See Figure 2.10
Station calls per typical weekday	Total		6,500 in EU 500 in CH+NO 200 in others	Order of 3,000	Order of 3,400	Order of 15,000	Order of 18,000
	By state						

Source: Steer Davies Gleave analysis based on sources identified in paragraph 2.15.

2.18 We discuss our estimates further below, dealing in turn with:

- International rail services;
- high-speed rail services; and
- international high-speed rail services.

International rail services

2.19 We assumed that international rail services include any service, operated with a single train number, which crosses one or more international borders. Note, however, that:

- If this definition was adopted, railway undertakings could change train numbers so as to limit the scope of "international services" to the journey between stations immediately before and after the border.
- A definition could be adopted that a service ceases to be international once it has entered the last state in its journey. For example, some Eurostar services from London to Paris are treated as domestic French services between Lille and Paris. In this case we would expect

that approximately half of all current "international" station calls estimated in Table 2.3 would be redefined as domestic.

- In addition, some trains are not considered "international" before the last stop before the border. This is the case where "services" into Sweden, carrying one in twelve are now effectively domestic-only services within Denmark (as we describe in detail in Table 4.6).

Estimates of border crossing points by Member State and other states

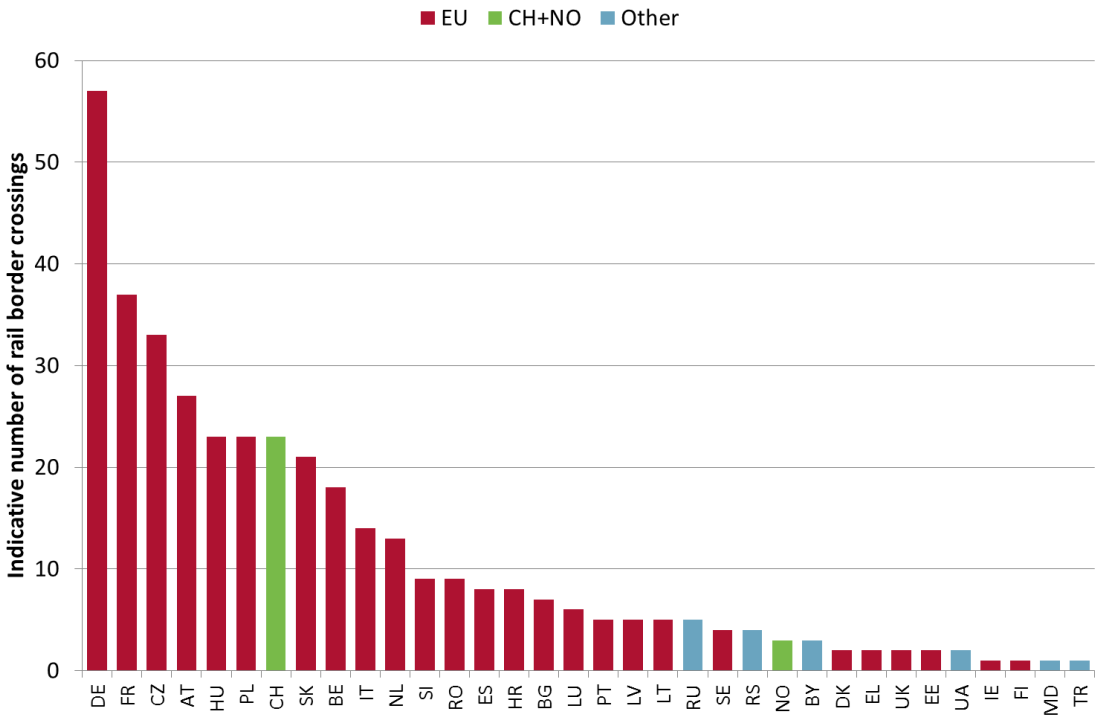
2.20 We counted the number of rail border crossing points for each Member State to estimate the number of international services within the EU and between the EU and other states.

2.21 On the definition in paragraph 2.19, all 26 EU Member States with a rail network have at least some international rail services although these might be with any of:

- other EU Member States;
- Switzerland and Norway; or
- other states.

2.22 Figure 2.4 shows our initial analysis of the number of points at which rail services cross the border of each state. Note that the chart shows the number of crossing points into and out of each of the 26 EU Member States with railways, plus Switzerland and Norway. This means that each of these crossing points is counted twice in the analysis, once for each of the bordering states.

Figure 2.4: Estimates of rail border crossing points by Member State and other states



Source: European Rail Timetable, Steer Davies Gleave analysis.
Note: may include some non-rail services excluded from further analysis, see text for details.

2.23 Note that:

- In Ireland and Finland there is only one point at which rail services cross into another country (the UK and the Russian Federation respectively).
- In Denmark, Greece, the UK and Estonia, there are only two points at which rail services cross into other Member States.
- In contrast, in Germany, we estimate that there may be more than 50 points at which services cross into other Member States, two of which are represented by the line serving Ulrichsbrücke-Füssen (shown in Figure 2.2), the Außerfernbahn, which leaves Germany and passes through Austrian territory before returning to Germany.
- Switzerland, which is not an Member State, has around 20 points at which rail services cross the border to or from a Member State. These include points close to the Swiss cities of Basel and Geneva, where there are significant volumes of cross-border commuting.

2.24 One peculiarity associated with the United Kingdom is that there are no international services on the network of the largest infrastructure manager, Network Rail:

- Eurostar services to and from France and Belgium used Network Rail infrastructure from 1994 to 2007 but now normally only use the small network of HS1[5].
- Enterprise services to and from Ireland use only the small network of Northern Ireland Railways.

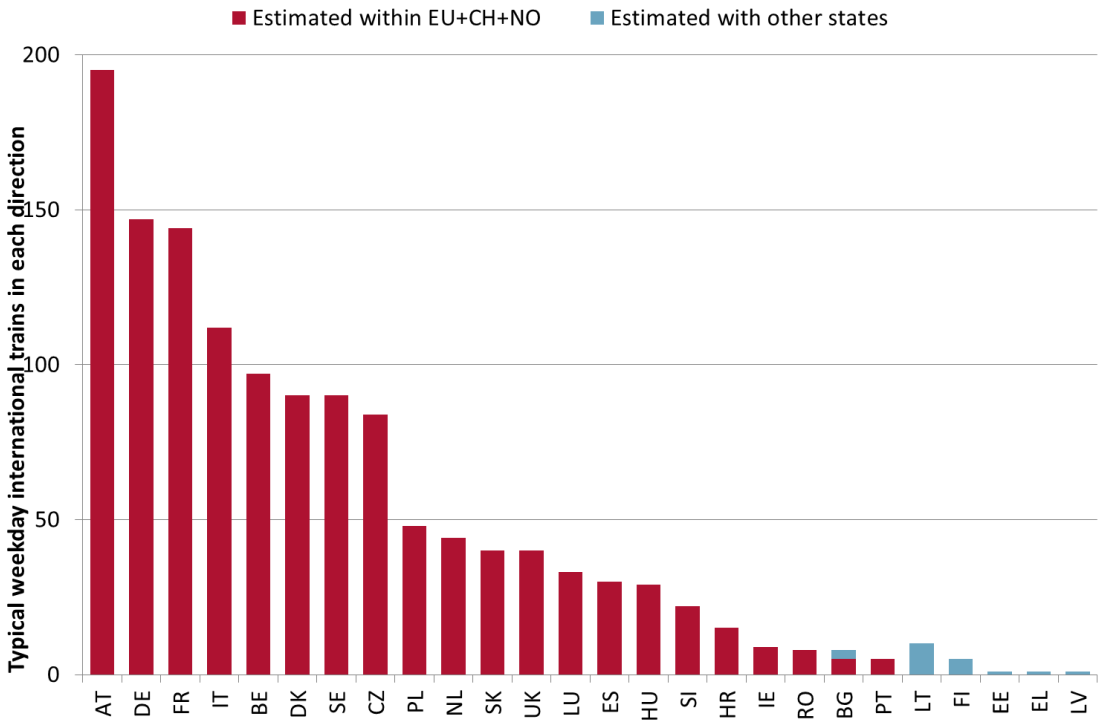
2.25 All the other main national IM's carry at least some international passenger services.

Estimates of rail cross-border services by Member State and other states

2.26 Figure 2.5 combines the initial analysis shown in Figure 2.4 with a more detailed analysis of the European Rail Timetable, to estimate the number of train services which cross each Member State's borders in each direction on a typical weekday. The estimation includes not only all the Member States but also Switzerland and Norway (EU+CH+NO).

[5]Eurostar's newer Class 374 ("e320") stock cannot use the restricted Network Rail gauge, and the older Class 373 stock no longer have the equipment to draw electrical power on it.

Figure 2.5: Estimates of cross-border rail services each weekday



Source: Steer Davies Gleave analysis of European Rail Timetable January 2016 weekday services.
Note: excludes Switzerland, Norway, Russia, Serbia, Belarus, Ukraine, Moldova and Turkey.
Note: excludes Eurotunnel shuttle services, for which there is no published timetable: see text for details.

2.27 In practice this analysis is complicated by a number of factors:

- Services vary from day to day, so that the choice of a "typical" weekday is arbitrary.
- The number of publicly timetabled services is not always the same in both directions.
- As we noted in Table 2.1, it is not currently possible to operate all the services timetabled between Denmark and Sweden, or internally within Denmark, and the estimates for these Member States therefore exceed the number of trains actually operated.

2.28 However, and as shown in Table 2.3, we estimate that, on a typical weekday, in each direction:

- 650 rail services cross borders between EU Member States, although in some cases, the same train, operating under the same train number, makes two or more border crossings.
- 50 rail services cross borders between an EU Member State and either Switzerland (from France, Germany, Austria or Italy) or Norway (from Sweden).
- 20 rail services cross borders between an EU Member State and another state.

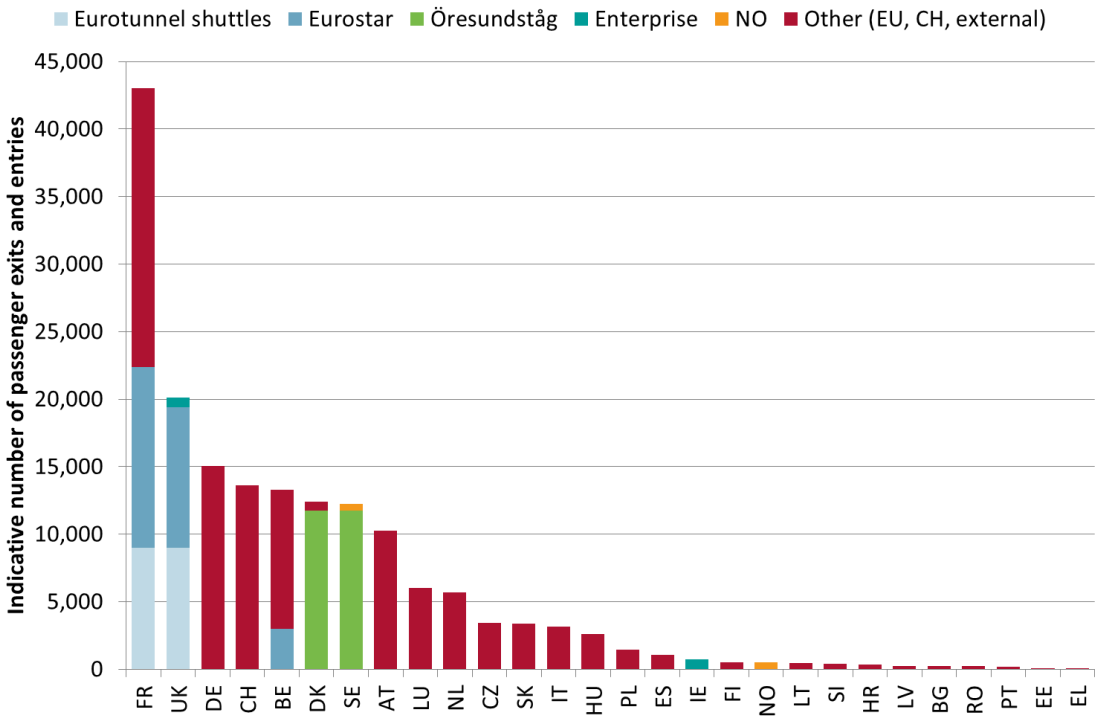
2.29 The reduction of services between Denmark and Sweden, however, means that only half the scheduled services between them currently operate, and around 40-50 trains weekday in each direction have been withdrawn. This means that a requirement to carry out identity checks, by one Member State on one service, has already led to the removal of around one in sixteen of all trains crossing EU borders.

2.30 These estimates also exclude Eurotunnel shuttle services between France and the UK, which do not operate to a published timetable, but can in principle include up to ten passenger and freight (truck) shuttles per hour.

Member States with international rail services

2.31 Eurostat provides estimates of the number of passengers carried on international rail services. Our checks showed that Eurostat data were not consistent with the operator data from which they should be derived: Eurostat's total for passengers to and from the UK was less that the totals reported by Eurotunnel and Eurostar alone. We did not contact Eurostat or any of the bodies which may have collected, processed and submitted the data it used. Instead, however, in Figure 2.6 we adjusted down the reported Eurotunnel passenger numbers to ensure that the totals match those provided by Eurostat.

Figure 2.6: Estimates of passenger border crossings (based on Eurostat)



Source: Eurostat and Steer Davies Gleave analysis
Note: passengers between EU Member States, Switzerland and Norway are counted twice.
Note: Enterprise is the brand name of services between Dublin in Ireland and Belfast in the UK.

2.32 Eurostat data suggest that, in 2014, around 78 million passengers crossed borders between EU Member States, 14 million crossed between EU Member States and Switzerland or Norway, and 4 million crossed between EU Member States and other states.

2.33 Of these, approximately:

- 12 million, or 15%, used services across the Öresund between Denmark and Sweden, the majority on the bi-regional Öresundståg network connecting Sjælland and Skåne.
- 10 million used Eurotunnel shuttle services with either trucks, coaches or private vehicles.
- 10 million used Eurostar services. All of them crossed the English Channel between France and the UK, and we understand that around 3 million of them also cross the Franco-Belgian border en route to Brussels.
- 22 million of the remaining passengers crossed between France and other states, including Belgium (other than on Eurostar), Luxembourg, Germany, Switzerland, Italy and Spain.

2.34 Taken together, these observations indicate that around 55% of all passengers crossing borders were entering or leaving France and a further 15% were entering or leaving Sweden.

2.35 We also note that 32 million crossings[6], or 40% of the total, used new infrastructure developed specifically to facilitate travel between neighbouring Member States. Construction of further international links, which is only likely to occur where there is high expected demand, seems likely to result in further growth in the number of passengers crossing borders.

Train sets required for international services

2.36 We found no direct means of estimating the number of trains, vehicles or crew required to operate international rail services, partly because individual fleets, train sets or crew may operate domestic and international services at different times, in some cases within the same day or same journey (see 2.19). We also note that, while rolling stock used on day trains may make many border crossings a day (a Eurotunnel passenger or truck shuttle train makes a round trip between France and the UK every two hours), night train stock may make only a single journey every 24 hours.

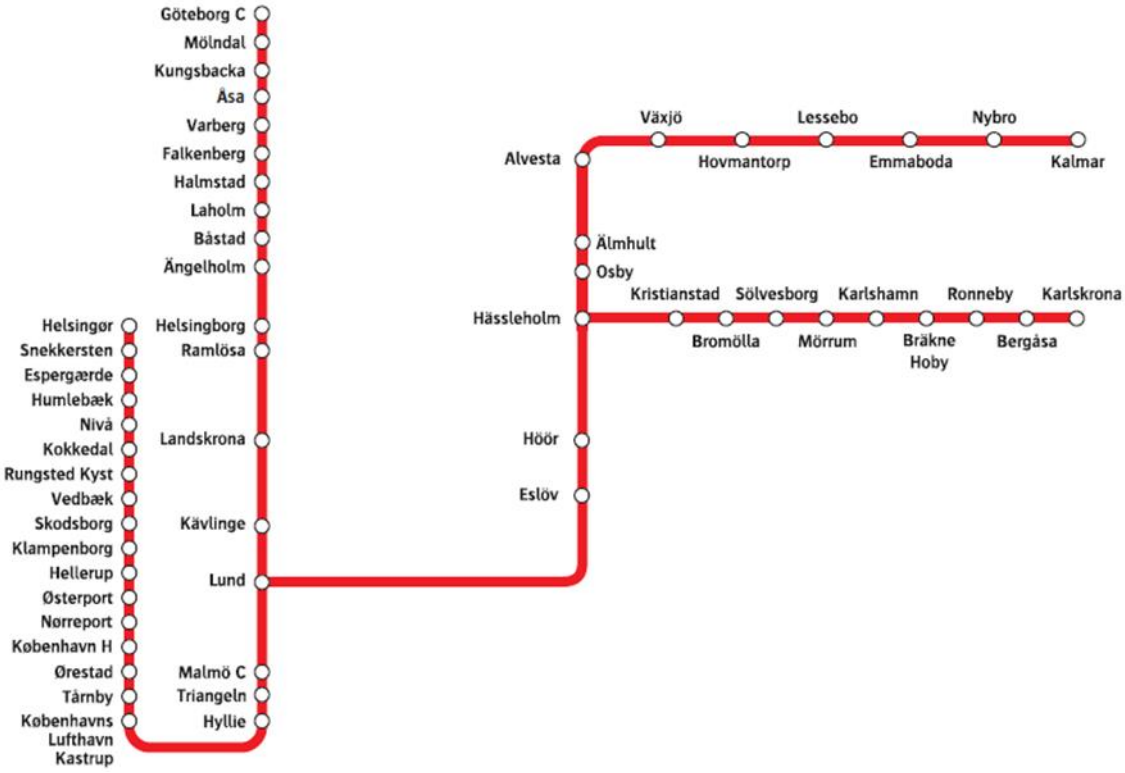
2.37 We compared data on rolling stock fleet sizes and reported number of passengers carried on a number of rail operators. We estimated that an individual rail vehicle used on international services typically carried 25,000 passengers per year, although our estimates varied widely around this number. This suggests that around 80 million international passengers in 2014 (see paragraph 2.31) were carried in approximately 4,000 rail vehicles, although we note that not all of these vehicles would be owned or operated by RUs based in the EU.

Stations served by international services

2.38 We did not attempt to calculate the exact number of stations served by international services. At one extreme, for example, Eurostar serves nine stations with up to four calls per service, but a non-stop London to Brussels train operates in three Member States but serves no intermediate stations. At another extreme, the Öresundståg network serves a large network in Denmark and Sweden, as shown in Figure 2.7.

[6] 20 million on Channel Tunnel opened in 1994, and 12 million on the Öresund Bridge opened in 2000.

Figure 2.7: Öresundståg network



Source: Skånetrafiken, Københavns Lufthavn Kastrup (bottom left) is in Denmark and Hyllie is in Sweden.

2.39 The network extends to 56 stations, and a single train from Helsingør in Denmark to Göteborg in Sweden could in principle call at up to 35 stations on both sides of the Öresund (bottom left on Figure 2.7, between Københavns Lufthavn Kastrup in Denmark and Hyllie in Sweden).

2.40 We reviewed a sample of timetables and concluded that, for indicative purposes, each of almost 200 cross-border services shown in Figure 2.4 calls at total of six stations (typically three in each of two Member States) which are not served by other international services. This suggests that around 1,200 stations are called at by international services, of which:

- 1,000 are stations in EU Member States.
- 200 are stations in other countries.

Station calls by international services

2.41 In the absence of detailed analysis, we assumed for indicative purposes that a typical international train makes 5 station calls, dominated by the relatively large number of long-distance and high-speed international trains connecting only capitals and major cities. If this estimate is correct, then the estimated total of 720 trains each way per weekday (see paragraph 2.28) will make around 7,200 station calls per day of which, indicatively:

- 6,500 are at stations in EU Member States.
- 500 are at stations in Switzerland and Norway.
- 200 are at stations in other states.

2.42 We stress that these are estimates of stations served and stations called at by international services but note that, as set out in Table 2.1 and Table 2.2, it would be necessary to analyse

the entire European Rail Timetable for a specific day, week or other time period to provide a definitive number. Even this analysis would still only be correct on a particular date.

States with high-speed rail services

Member States which appear to have a high-speed service

2.43 We also attempted to identify States with high-speed rail services. We worked, as required by the Terms of Reference, from "the existing EU definition of high-speed" taken from Directive 2008/57/EC ("the Interoperability Directive"), summarised in Figure 2.8.

Figure 2.8: The existing EU definition of high-speed

2. Trans-European high-speed rail system

2.1. Network

The network of the trans-European high-speed rail system shall be that of the high-speed lines of the trans-European transport network identified in Decision No 1692/96/EC.

The high-speed lines shall comprise:

- *specially built high-speed lines equipped for speeds generally equal to or greater than 250 km/h,*
- *specially upgraded high-speed lines equipped for speeds of the order of 200 km/h,*
- *specially upgraded high-speed lines which have special features as a result of topographical, relief or town planning constraints, on which the speed must be adapted to each case. This category also includes interconnecting lines between the high-speed and conventional networks, lines through stations, accesses to terminals, depots, etc. travelled at conventional speed by 'high-speed' rolling stock.*

This network includes traffic management, tracking and navigation systems, technical installations for data processing and telecommunications intended for services on these lines in order to guarantee the safe and harmonious operation of the network and efficient traffic management.

2.2. Vehicles

The trans-European high-speed rail system shall comprise vehicles designed to operate:

- *either at speeds of at least 250 km/h on lines specially built for high speeds, while enabling operation at speeds exceeding 300 km/h in appropriate circumstances,*
- *or at speeds of the order of 200 km/h on the lines of section 2.1, where compatible with the performance levels of these lines.*

In addition, vehicles designed to operate with a maximum speed lower than 200 km/h which are likely to travel on all or part of the trans-European high-speed network, where compatible with the performance levels of this network, shall fulfil the requirements ensuring safe operation on this network. To this end, the TSIs for conventional vehicles shall also specify requirements for safe operation of conventional vehicles on high-speed networks.

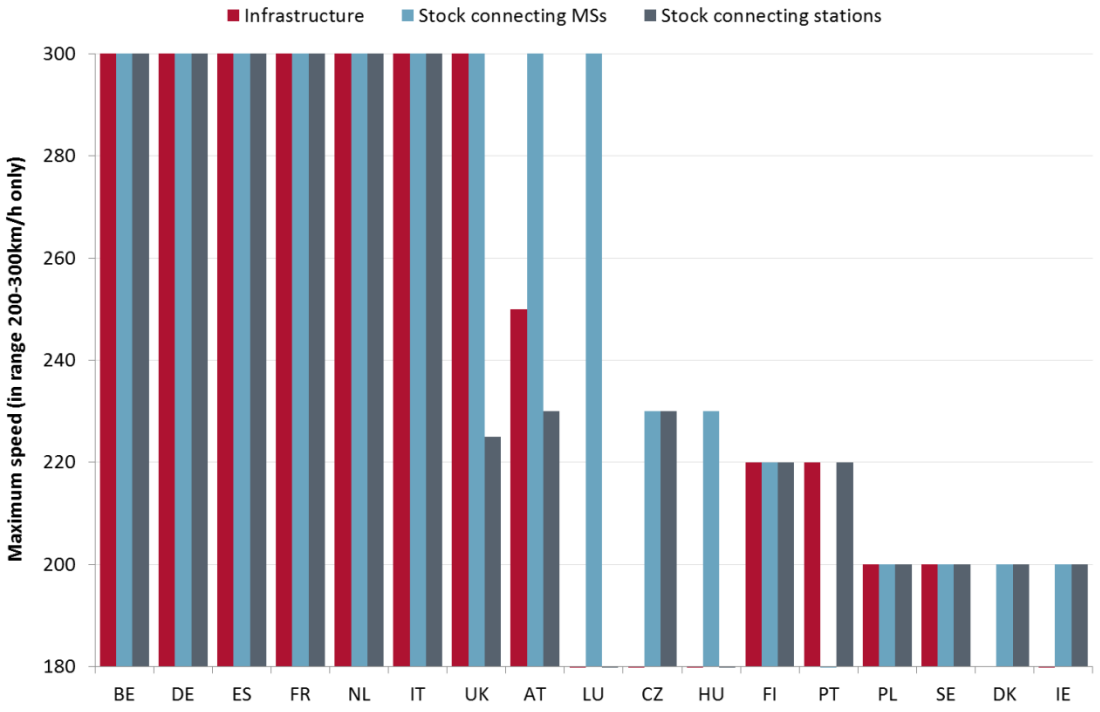
Source: Directive 2008/57/EC ("The Interoperability Directive")

2.44 In practice, the text of the Directive defines high-speed "network" and "vehicles", and the definition of "vehicles" appear to include the 200 km/h High Speed Train showing calling at Liskeard in Figure 2.1. However, the text does not define the characteristics of high-speed "services" referred to in the Terms of Reference. We therefore examined, for 17 states:

- whether any infrastructure within the state was equipped for speeds equal to or greater than 200 km/h;
- whether any services connecting stations in the state used rolling stock designed to operate at speeds equal to or greater than 200 km/h; and
- whether any services connecting stations in the state with stations in another state used rolling stock designed to operate at speeds equal to or greater than 200 km/h.

2.45 The results of our analysis are shown in Figure 2.9.

Figure 2.9: Member States which appear to have high-speed services



Source: see text
Note: stock connecting MS is the maximum speed of stock connecting stations in the state and another state
Note: stock connecting stations is the maximum speed of stock connecting two stations in the state

2.46 We conclude that 17 EU Member States either operate trains, or have stations served by trains coming from other Member States or neighbouring States, that are capable of operation at 200 km/h or more.

2.47 We considered treating all infrastructure and trains capable of operation at 200 km/h as high-speed, but rejected this approach for three reasons:

- Trains notionally or originally capable of 200 km/h are in practice operated on a range of services, often at considerably lower speeds. In some cases trains designed for 200 km/h may have had features such as their suspension “re-optimised” for lower speeds, and might require further modification to operate at 200 km/h again. Most noticeably, 200 km/h High Speed Trains (HSTs) dating from the 1970s are being used in Great Britain for services at Liskeard (Figure 2.1), 250 kilometres by rail from the nearest 200 km/h track, or wholly within Scotland, where no infrastructure permits speeds higher than 160 km/h. In addition, 200 km/h Swedish trains enter Denmark, but the Danish Ministry told us that it did not consider that this meant that Denmark had high-speed services.

- If the threshold of high-speed operation were set at 200 km/h, infrastructure managers and operators might "de-rate" infrastructure and trains, for example to "199 km/h", to avoid being covered by any specific requirements.

2.48 We therefore adopted, for illustrative purposes, two thresholds of "high-speed":

- Greater than 260 km/h. This is sufficiently high to exclude 250 km/h services in Austria, but sufficiently low to include all operation at 300 km/h or more by the Alstom TGV and Siemens ICE families of trains.
- Greater than 210 km/h. This is sufficient also to include 250 km/h services in Austria, 225 km/h services in the UK with Hitachi "Javelin" trains, and 220 km/h services in Finland and Portugal with Fiat (now Alstom) "Pendolino" trains.

Train sets used to provide services at over 260 km/h

2.49 Table 2.4 lists all the rolling stock we identified which operates in, or penetrates into, the EU, with a design speed of more than 260 km/h.

Table 2.4: Train sets capable of more than 260 km/h

Family	Fleet	Number of sets	Passenger vehicles per set	Passenger vehicles	Comments
TGV	Sud-Est	107	8	856	
	Atlantique	105	10	1,050	
	Réseau (including Thalys PBA)	90	8	720	
	Eurostar 18 car	31	18	558	
	Eurostar 14 car	7	14	98	
	Duplex	160	8	1,280	
	Thalys PBKA	17	8	136	
	TGV POS	19	8	152	
	TGV 2N2	95	8	760	Not all in use until 2019
	AVE 101	18	8	144	
	AVE 102	46	12	552	330 km/h
	AGV (Italo)	25	11	275	
ICE	ICE 1	59	12	708	280 km/h
	ICE 2	44	7	308	280 km/h
	ICE S	-	-	-	Test train only
	ICE 3 (Class 403)	50	8	400	
	ICE 3M (Class 406)	17	8	136	
	Velaro D	17	8	136	
	Velaro E (AVE 103)	26	8	208	
	ICE 4	130	-	-	Not in use until 2017
	Eurostar E320	11 (or 17)	16	176	Few in use yet
Approximate total		**1,050**		**8,500**	

Source: Steer Davies Gleave analysis, railway websites.

2.50 This suggests that the effective size of the 260 km/h plus high-speed fleet which will shortly be in use is probably around 1,050 sets with 8,500 vehicles.

Train sets used to provide services at over 210 km/h

2.51 Other train sets capable of 210 km/h but not 260 km/h include:

- 230 km/h ICE T stock;
- 230 km/h Railjet stock used in Austria, Germany, Hungary, Switzerland and Czech Republic (plus Italy from December 2016);
- 225 km/h Javelin stock used in the UK; and
- 220 km/h stock used in Finland and Portugal.

Table 2.5: Train sets capable of more than 210 km/h

Family	Fleet	Number of sets	Passenger vehicles per set	Passenger vehicles	Comments
ICE	ICE T	71	5 or 7	426	Tilting, only 230 km/h
Railjet	230 km/h fleet	58	7	406	Fleet expanding to 67, but only in 2016
Javelin	225 km/h Class 395	29	6	174	Often run in pairs
Sm3	220 km/h Finnish Pendolino	18	6	108	Tilting, much use is off the highest speed section
Alfa	Alfa Pendular, Portugal	10	6	60	Tilting
Approximate total		**180**		**1,200**	

Source: Steer Davies Gleave analysis, railway websites.

2.52 Again, taking into account that the vehicles constructed or still available may not all be needed to operate the current services, we estimate that the efficient size of this fleet is around 150 sets with 1,000 vehicles.

2.53 Our conclusions are summarised in Table 2.6.

Table 2.6: Estimates of trains providing high-speed services

High-speed threshold	Number of sets	Number of passenger vehicles
260 km/h	1,050	8,500
210 km/h but below 260 km/h	1,200	9,500

Source: Steer Davies Gleave analysis, railway websites.

2.54 We consider that these estimates are probably broadly accurate, but note that they include both domestic and international operations. In practice, many of the fleets may be used for both types of service and cannot meaningfully be identified to one or the other, although in some cases it might be possible to dedicate a subset of the high-speed fleet to operate high-speed international services.

Services operated by high-speed trains

2.55 RUs do not normally publish data on the services provided by each type of train (and the only estimate given to us by an RU during an interview proved on inspection to be much smaller than the actual number of services they operated). Following a review of a sample of

timetables, we assumed that each of the high-speed train sets listed in Table 2.6 typically made a 3-hour end-to-end journey and would complete five of these journeys in a day. From this we estimated that the total number of high-speed services on a typical weekday would be of the order of 5,000 with stock capable of over 260 km/h and of the order of 6,000 with stock capable of over 210 km/h.

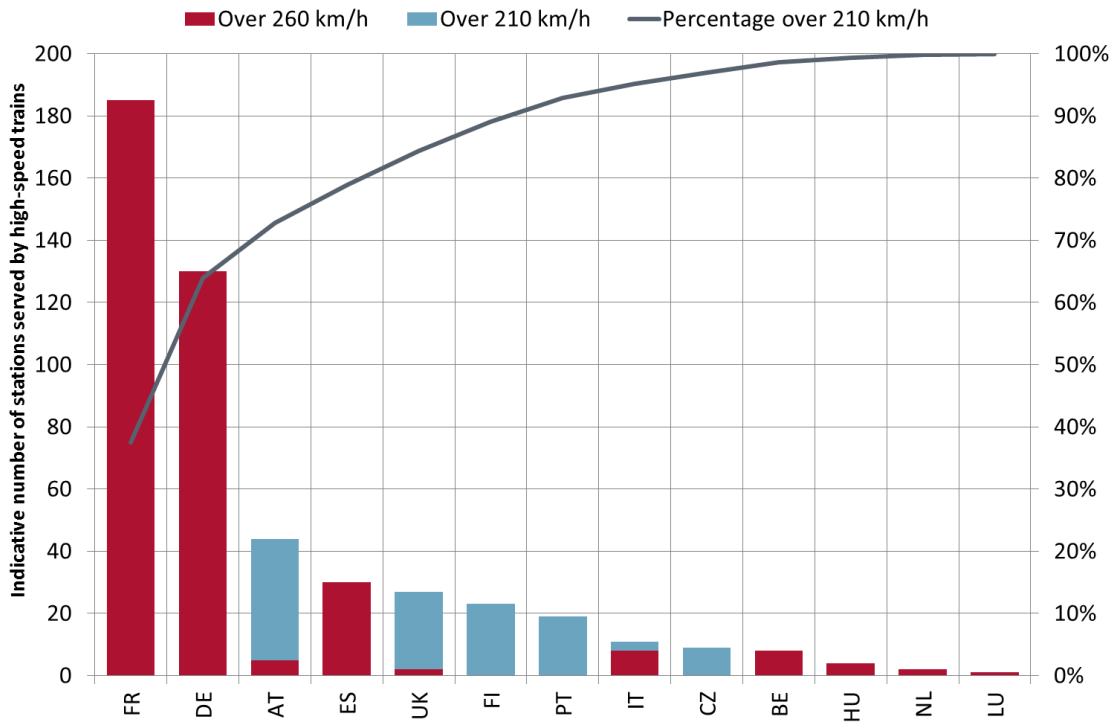
Station calls by high-speed services

2.56 Examination of the European Rail Timetable suggested that high-speed trains generally have a relatively frequent service. This is probably because investment in high-speed infrastructure can rarely be justified unless it will be relatively intensively used. If we assumed, as above, that each of the average of five 3-hour journeys per day by each train set involved three station calls, or 15 station calls per train set per day, this would suggest that the high-speed train sets listed in Table 2.6 made a total of around 15,000 station calls by stock capable of over 260 km/h and 18,000 station calls by stock capable of over 210 km/h.

Stations with a high-speed service

2.57 RUs in a number of Member States provide promotional material listing stations at which trains capable of high speed operate. We also examined the stopping patterns of services which we knew to operate at high speed, such as ICE in Germany, TGV in France, and "Javelin" services in the UK. The results are shown in Figure 2.10.

Figure 2.10: Estimates of high-speed stations served



Source: rail operator and infrastructure manager websites, European Rail Timetable, Steer Davies Gleave analysis.

2.58 We estimated that:

- Nearly 400 EU stations have services operated by trains capable of 260 km/h, over 300 of them in France and Germany.

- Nearly 500 EU stations have services operated by trains capable of 210 km/h. Almost two-thirds of all these stations are in France and Germany.

2.59 Data on stations served by the Alstom TGV family of trains reveals two other points.

2.60 First, at least 17 Swiss stations have TGV services operated by trains capable of 300 km/h (see Table 2.4). This suggests that, to provide a consistent approach to a whole service, any additional security interventions applied to TGV services might also need to apply in Switzerland, at least at these 17 stations.

2.61 Second, at least 27 French stations, and 18 in other Member States (such as London Waterloo International), have had "TGV" services and lost them. In many cases, these stations were served on an experimental basis, often as a result of local political pressure and financial support. Where the experiment fails, with very low numbers of passengers materialising, the service may not last more than a 12-month timetable period. This latter point suggests that the high-speed network is not static, and that any adaptions to stations to comply with the requirements of high-speed operation, including additional security features, may become redundant if services are subsequently withdrawn[7].

Passenger numbers on high-speed services

2.62 Assuming that each high-speed vehicle carries around 25,000 passengers per year (see 2.37), we estimate that the number of passengers on the high-speed train sets listed in Table 2.6 is of the order of 200 million on stock capable of over 260 km/h and of the order of 225 million on stock capable of over 210 km/h. We stress that, as shown in Table 2.2, these can only be indicative estimates, because RUs do not systematically publish statistics on passenger number by service type.

International high-speed rail services

2.63 In contrast to the data available on international services and high-speed services separately, we found few clear sources of data on international high-speed services. In practice, definition of such services is made difficult for a number of reasons:

- An international service may be operated by high-speed rolling stock on grounds of interior layout and facilities, "quality", prestige or marketing, but may not actually operate at high speed at any point on the journey.
- The same stock may be used by both domestic and international services (see also 2.19), making it difficult to define or quantify either the rolling stock or the crew associated with each type of service.

2.64 As a result, even with a complete list of all international services, and the rolling stock with which they were normally operated, it would not be possible to identify whether they reached high speed at any point on their journey, or how many train sets were actually required to provide them. We therefore estimated the number of international high-speed rail services as follows.

[7] Analogous investment occurs at airports which have invested in providing gates and taxiways capable of handling large aircraft such as the Boeing 747 and, more recently, the Airbus A380. In practice, airlines cannot guarantee either that they will continue to serve the airport or that they will continue to use particular aircraft, and the resulting investment can therefore be made redundant by subsequent changes in airline service patterns or fleets.

Passenger numbers per year

2.65 Given the estimates of international passenger numbers summarised in Figure 2.6, we note that EU internal borders are crossed by:

- all 300 km/h Eurostar and Thalys high-speed services; and
- some 300 km/h TGV and ICE train sets and many of the 230 km/h Railjet sets listed in Table 2.5.

2.66 However, not all the passengers on these trains cross borders: many may make a journey wholly within one Member State.

2.67 We estimated that around half of the total of cross-border passengers were on high-speed services, and indicatively estimated that 40 million were on rolling stock capable of over 260 km/h and 45 million were on rolling stock capable of over 210 km/h.

Services operated each way per typical weekday

2.68 We estimated in 2.28 that 650 rail services cross borders between EU Member States on a typical weekday, in each direction. We assumed that:

- 300 of these services were operated by rolling stock capable of over 260 km/h; and that
- 350 of these services were operated by rolling stock capable of over 210 km/h.

Train sets required for high-speed international services

2.69 Similarly, we assumed that approximately half the train sets required to operate international services were high-speed sets, suggesting that this would involve of the order of 200 train sets or 2,000 vehicles.

Station calls per typical weekday

2.70 If, as assumed in paragraph 2.56, each of these train sets made an average of five journeys per day with three calls per journey, then the total number of station calls on a typical weekday would be of the order of 3,000 by train sets capable of over 260 km/h and 3,400 by train sets capable of over 210 km/h.

Stations served

2.71 We did not attempt to carry out a detailed analysis of the stations served by high-speed train sets carrying out international journeys, but estimated that this might be around half the stations called at by all high-speed trains: of the order of 200 stations served by train sets capable of over 260 km/h and 220 stations served by train sets capable of over 210 km/h.

Summary

2.72 With rare exceptions such as Eurotunnel, the European railway industry publishes a relatively standardised timetable from which it is possible, in principle, to calculate the exact number of high-speed and international rail services, and the station calls they were timetabled to make, on any given day or in any given period. However, the industry does not routinely define or publish details of either of the rolling stock fleets or the crews dedicated to operating these services, or estimates of the number of passengers who use them, or of which of these passenger travel at any given speed, or cross one or more international borders while on board.

2.73 While it is in principle possible to make definitive estimates of the number of high-speed and international rail services, the stations they serve, and the station calls they make, data are not available to extend this to efficient fleet sizes or passenger numbers.

2.74 In addition, we note that any measures to increase security on high-speed and international rail services to improve security might result in industry reaction to minimise the associated cost and inconvenience to passengers. In particular:

- Measures related to international services might be avoided by strategies such as changing train numbers (see paragraph 2.19), reducing the total number of cross-border services (or seeking exemptions where a train crossed only a short distance into another state to a "border" station), limiting the number of stations they serve, and operating them with a smaller dedicated rolling stock fleet.
- Measures related to high-speed services might be avoided by "de-rating" infrastructure or rolling stock to a slightly lower speed. For this reason we have focused on illustrative speed capabilities of over 260 km/h and over 210 km/h (see paragraphs 2.47 and 2.48).

2.75 For both these reasons we conclude that the indicative estimates set out in Table 2.3, and summarised in Table 2.7 below, provide a reasonable estimate of the scale of high speed and international rail services which operate in Europe.

Table 2.7: Estimates of scale of high-speed and international rail services (summary)

Data	EU total	International	International high-speed (>260 km/h)	International high-speed (>210 km/h)	High-Speed (>260 km/h)	High-Speed (>210 km/h)
Passenger numbers per year	9,200 billion	78 million EU 14 million CH+NO 4 million other	Order of 40 million	Order of 45 million	Order of 200 million	Order of 225 million
Services each way per typical weekday		650 intra-EU 50 to CH+NO 20 to others	Order of 300 intra-EU	Order of 350 intra-EU	Order of 5,000	Order of 6,000
Stations served	26,000 (estimate)	1,000 in EU 100 outside EU	Order of 200	Order of 220	400	500
Station calls per typical weekday		6,500 in EU 500 in CH+NO 200 in others	Order of 3,000	Order of 3,400	Order of 15,000	Order of 18,000

Source: Steer Davies Gleave analysis based on sources identified in paragraph 2.15, see also Table 2.3.

3 Defining security

Introduction

3.1 The Terms of Reference refer only to "security", and cite as an example the incident on a high-speed international train, but defining security appears problematic, for a number of reasons.

3.2 The European railway industry uses no common definition of the word "security", and in some languages there is no clear distinction between "safety" and "security". However, it is possible to distinguish them by adopting definitions such as:

- Safety relates to accidents.
- Security relates to malice.

3.3 A related point is that there is no consistent distinction between the management of safety (related to accidents) and security (related to malice). This is partly because many of the measures, such as evacuation plans, or calling the police, are similar or identical. For example:

- The optimal response to a derailment may be identical whether it is caused by poor maintenance (neglect), by landslide (accident), or by vandalism or terrorism (malice).
- The optimal response to an explosion may be identical whether it is caused by a gas leak (accident) or terrorism (malice).

3.4 Moreover, in the case of either a derailment or an explosion, the passengers and rail staff who are first on the scene may have no means of knowing the cause of the incident, which may not be determined until long after the event. In these circumstances it may be meaningless to attempt to distinguish plans for, or responses to, events on the basis of a cause which may not be known at the time.

Crime on the railway

3.5 In practice, security (malice) relates not only to terrorism but also to a wide range of other criminal acts on infrastructure, stations and trains used, or in use, to provide high-speed and international rail services. As an example of the range of criminal acts which may be included, we examined the Statistical Bulletin of the British Transport Police, one of the police forces largely, but not exclusively[8], dedicated to policing the railway. This lists the crimes and offences on the railway network of Great Britain during reporting year 2014-15, as shown in Table 3.1.

[8] The British Transport Police also has polices the London Underground, Docklands Light Railway, the Midland Metro, Croydon Tramlink, Sunderland Metro, Glasgow Subway and Emirates Air Line, but not the Tyne and Wear Metro or Manchester Metrolink (a light rail system) with which it has no service agreement.

Table 3.1: Crimes recorded by the British Transport Police, 2014/15

Type of crime	Offence	Recorded	Solved[9]	Comments
Violence against the person	Homicide	2	0	Violent crime may include this
	Attempted murder	5	4	Violent crime may include this
	Serious assault	2,022	961	Violent crime may include this
	Common assault	4,324	1,574	Violent crime may include this
	Police assault	501	446	Violent crime may include this
	Firearms/explosives	29	21	May include some terrorism
	Racially aggravated harassment	1,171	550	Violent crime may include this
	Other violence	1,095	563	Violent crime may include this
Sexual crime	Sexual offences against females	847	290	
	Sexual offences against males	37	10	
	Exposure	161	52	
	Other sexual crime	354	133	
Criminal damage/ malicious mischief	Criminal damage/malicious mischief	1,509	340	Vandalism may include this
	Arson	68	11	Vandalism may include this
	Graffiti	1,687	526	Graffiti
	Other criminal damage	97	29	Vandalism may include this
Line of route crime	Destroy or damage/endanger safety	183	38	Vandalism may include this
	Obstruction	679	227	
	Throw missile at rail vehicle	251	9	
Theft of passenger property	Theft luggage	1,197	87	
	Theft personal property	5,503	407	
	Theft from the person	5,339	253	
Motor vehicle/ cycle crime	Theft motor vehicle	144	19	
	Take vehicle without consent	14	2	
	Theft from vehicle	685	35	
	Damage to motor vehicle	529	80	
	Theft/damage pedal cycle	5,776	1,049	
	Interfere with motor vehicle	83	6	
Robbery	Robbery	339	158	Violent crime may include this
	Assault with intent to rob	19	10	
Drug crime	Trafficking in controlled drugs	73	67	
	Possession of a controlled drug	2,271	2,182	
	Proceeds of crime (drugs)	1	1	
	Other drug crime	10	8	

[9] "Criminal Justice Outcomes". Note that, in a terrorist event such as a suicide bombing, the perpetrator may be identified but not prosecuted or formally found guilty.

Type of crime	Offence	Recorded	Solved[9]	Comments
Theft of railway/ commercial property and burglary	Burglary/housebreaking booking office	33	7	
	Burglary/housebreaking	446	60	
	Theft from shop/kiosk	2,097	1,236	
	Goods in transit offences	19	0	
	Theft from vending machines	213	72	
	Theft from undertaking stores	449	36	
	Live cable theft	194	53	Metal theft may include this
	Non-live cable theft	277	74	Metal theft may include this
	Other theft/burglary	245	51	
Public order	Bomb hoax offences	61	15	Terrorism may include this
	Other public order crimes	4,447	2,264	
Fraud	Ticket fraud	2	0	
	Forgery	81	60	
	Other fraud	291	175	
Other notifiable crime/ offences	Handling/reset	71	58	
	Other firearms offences	4	3	May include some terrorism
	Proceeds of crime (excluding drugs)	34	27	
	Other theft	284	36	
	Other offences	435	277	
Notifiable offences		**46,688**	**14,652**	
Less serious line of route offences	Railway trespass	7,108	1,694	
	Transport and works offences	5	5	
	Stone throwing	532	22	
	Other less serious line of route offences	167	2	
Less serious public order offences	Alcohol offences	2,272	2,158	
	Breach of the peace	22	16	
	Other less serious public order	8,376	2,658	
Less serious fraud	Travel fraud	3,925	3,251	
	Travel related crime/greater distance	2,727	1,381	
	Failure to provide details/show ticket	30	26	
Other less serious offences	Driving offences	4,411	2,935	May include vehicle penetration
	Vehicle related (byelaws)	323	273	
	Begging	337	253	
	Protection equipment	262	68	
	Other less serious offences	899	533	
Total non-notifiable offences		**31,396**	**15,275**	

Source: British Transport Police Statistical Bulletin 2014-15

3.6 The table illustrates a number of points.

3.7 First, the list of crimes, and the way in which they are categorised, reflects the British Transport Police's duty to enforce the criminal law of England, Scotland and Wales and devolved authorities within them. What constitutes a criminal act varies not only within the UK, but also between Member States and within other Member States, including by both location and time of day. Legislation on even minor issues such as smoking, cycling, skateboarding or photography or filming many vary widely between locations within the EU[10].

3.8 Second, the British Transport Police reports types of crime according to categories such as the relevant legislation, rather than to broad categories of crimes such as "metal theft", "vandalism" and "terrorism". Even with this detailed report, it is not possible to identify how many crimes of these types were reported or solved, although we have indicated types of crimes which we think may fall into one of these categories.

3.9 Third, Member States may not treat crimes of terrorism in the same way as other criminal acts: in particular the legislation and the actors involved, including the ministry responsible, may differ.

3.10 Fourth, even if security can be defined as relating to a number of actions which already are, or could be made to be, criminal offences on the railways of all Member States, this does not mean that they have a common cause. Trespass on the railway may be unintentional, if the trespasser is lost, or with the intent of graffiti, vandalism, theft or terrorism. All have different causes and it is difficult to devise a problem definition which identifies common root causes and problem drivers.

3.11 Fifth, there is no obligation on Member States either to collate data on all the diverse issues or security, or to do so for the railway, or to do so for some definition of high-speed and/or international rail services. The British Transport Police does not publish disaggregate statistics of where crime to place on this or any other definition[11].

3.12 Taken together, these points mean that there is no EU-wide consensus on what is meant by security, or of whether it is limited to terrorism or extended to include all criminal, or all malicious, activity which impinges on the railway. All these factors complicate the comparison of crime rates across different Member States[12].

3.13 Nonetheless, we agreed with the Commission that, for the purposes of this study, security should be defined to include all crime on high-speed and international rail services, including:

- violent crime, and in particular terrorism;
- non-violent crime involving damage to railway infrastructure and rolling stock such as metal and cable theft and graffiti; and

[10] In addition, reported crime rates and associated targets may be distorted with a view to reducing perceived crime levels. See http://www.parliament.uk/business/committees/committees-a-z/commons-select/public-administration-select-committee/news/crime-stats-substantive/.

[11] The British Transport Police Statistical Bulletin subdivides the crimes listed in Table 3.1 into eight geographical Divisions, but does not distinguish those on the national railway network from those on the other networks it polices.

[12] https://www.unodc.org/unodc/en/data-and-analysis/Compiling-and-comparing-International-Crime-Statistics.html

- other non-violent other crimes affecting passengers and staff such as endangering safety, obstruction, trespass and luggage theft.

3.14 In addition, even where crime is reported, it may not be identified or identifiable as being on or related to the railway, or on infrastructure, stations or trains used, or in use, to provide high-speed or international rail services.

Existing security interventions

3.15 Crime on the railway is already being addressed by a wide range of activities which can be described as security interventions. At the most basic level, as with most public and private property and buildings, this include provisions such as fences, gates, walls, doors and locks. Railways may also include interventions such as lights, staff and patrols.

3.16 Table 3.2 provides a non-exhaustive list of security interventions identified from our experience and desk research.

Table 3.2: Existing security interventions

Type of intervention	Examples identified in initial desk research
Basic	Fences, gates, walls, doors, locks, barriers, lights, staff and patrols
Communications and external liaison	Partnerships and liaison with third parties, emergency services, and security experts in other fields
Assets and equipment design	Station ticket barriers, queuing systems, passenger and baggage screening equipment
	Facilitation of emergency egress, duplicate access routes and walkways
	Minimisation of unseen areas, static detection equipment (such as CCTV), facial or behaviour recognition technology
	Recording of vulnerabilities in asset register, road vehicle intrusion protection, mobile detection equipment (such as drones)
	Blast-resistant luggage storage areas, stations, trains
	Resistant and contingent radio, IT and communications systems
Staff and training	Training in risk and behaviour monitoring, and in incident response
	Staff vetting, screening, and deployment
Risk assessment and planning	Threat level protocols
	Contingency planning, drills and exercises, and post-incident recovery
Procedures and systems	Identity checks and/or nominative ticketing
	Awareness promotion
	Targeted storage of contingency reserves, inspection regimes

Source: Steer Davies Gleave technical knowledge and desk research.

3.17 As part of our research, we investigated the extent to which these interventions have been or are deployed on the railways, and more specifically on infrastructure, stations and trains used by high-speed and international rail services. In Chapter 4 we return to the issue of how the use of these interventions may evolve in future.

Evidence of security failure

3.18 For the moment, we note that the collective effect of these interventions does not eliminate all crime on the railway. The crimes listed in Table 3.1, and on other railways, can therefore be seen as "security failure", and we next attempt to estimate the scale of this failure and the extent to which it is a problem. We discuss in turn:

- metal and cable theft;
- vandalism and graffiti;
- other non-violent crime;
- terrorism; and
- other violent crime.

Non-violent crime

Non-violet crime: metal and cable theft

3.19 Metal theft, driven by global demand for commodities, is a common issue for railways worldwide. The size of the European Union's rail network and the difficulty of monitoring large parts of the infrastructure make it susceptible to metal theft, the impact of which goes beyond the direct costs of replacing the materials and affects service reliability and journey times. Many of Europe's railways suffer from theft of metal, and in particular of copper cable, which can result in extensive disruption to services while the missing cable is replaced and safe operation re-established.

3.20 The railway industry and other parties have implemented a range of security interventions as countermeasures, including better record-keeping by scrap metal dealers, the banning of cash payments for scrap, and the proper identification of sellers of scrap. These countermeasures have been endorsed by the European Rail Infrastructure Managers Association (EIM). Nonetheless, at the national level:

- In the UK, Network Rail, the main IM, has reported that metal theft costs €23.7 million per year[13].
- In Greece, the national rail company has reported that cable theft has cost €12 million in two years, or €6 million per year.
- In Germany, DB has reported that metal theft grew 50% from 2010 to 2011.

3.21 EIM estimated that, over the four years 2011-2014, disruption from metal and cable theft caused 4.6 million minutes of delay to users of rail services, and the total cost of such theft to its members was some €270 million, or almost €70 million a year. This is the only estimate we have found of the Europe-wide effect of theft, although we note that the figures reported by the UK and Greece alone amount to €30 million, or nearly half EIM's estimated total for Europe.

3.22 The proportion of the impact of metal and cable theft associated with high-speed and international rail services is not estimated by either Member States or EIM. If, however, we assume that it is 10% of the total, broadly consistent with our estimates of the scale of total services in Figure 2.3, this would imply that the annual cost of metal and cable theft to high-speed and international rail services is approximately €7 million.

[13] EurActiv (2012): http://www.euractiv.com/transport/growing-cable-thefts-prompt-rail-news-515740

Non-violent crime: vandalism and graffiti

3.23 Vandalism on the railway, if defined as intentional damage to railway property, can include graffiti, litter, fly tipping and damaging railway property including fences, bridges, signs and track. Rail industry players including IMs and RUs take a number of steps to reduce the incidence and impact of vandalism[14].

3.24 Determining the level of vandalism on EU railways is difficult because reporting and categorising of vandalism is not standardised between Member States. Graffiti, for example, is considered by some to be antisocial behaviour and by others to be artistic expression. However, we identified a number of estimates of the scale and cost of vandalism and graffiti in 2014, which we summarise in Table 3.3.

Table 3.3: Estimates of the cost of vandalism and graffiti on railways, 2014

Context	Annual cost in 2014	Source
Deutsche Bahn AG, Germany	€50 million loss in 2014 due to 46,000 instances of all types of vandalism, including graffiti.	Bundespolizeiinspektion München
Ferrocarrils de la Generalitat de Catalunya (FGC), Spain	€175,000 cost of graffiti in 2014, excluding the cost of immobilising a train unit for a day to remove graffiti.	FGC
Network Rail, UK	€6.25 million (£5 million) per year spent cleaning graffiti from trains, excluding delays and any lost revenue.	British Transport Police

3.25 We note that graffiti may be on trains, whether in use, or stabled, or in a depot, on stations, or elsewhere on the infrastructure, including places (such as the outer faces of railway bridges) where it cannot be seen by railway staff and passengers.

3.26 The Statistical pocketbook 2016 provides information on the relative lengths of railway in 2014 in the EU, Germany, and on a high-speed network[15]. If we assume that the cost of vandalism throughout the EU is a fixed cost per route-kilometre, this would suggest that the total annual cost across the EU is approximately €280 million. If we assume that high-speed and international trains operate on approximately 10% of the total network (broadly consistent with our estimates in Table 3.3), this would suggest that the annual cost of vandalism and graffiti to high-speed and international rail services may be of the order of €30 million per year.

Other non-violent crime

3.27 The British Transport Police data listed in Table 3.1 identifies approximately 77,000 crimes, most of which are non-violent but only a small proportion of which appear to relate to metal and cable theft, vandalism and graffiti.

[14] Security interventions to reduce vandalism can, however, be counterproductive. The UK's Transport for London undertook a campaign of publicly communicating prosecution and convictions rates for vandalism and graffiti, but vandalism and graffiti increased and the campaign was deemed a failure.

[15] https://ec.europa.eu/transport/facts-fundings/statistics/pocketbook-2016_en, Section 2.5, gives 220,673 kilometres for the EU 28, 38,836 kilometres for Germany and 7,316 kilometres for the "High Speed Rail Network". From other sources we infer that these data may be the route-kilometres of the network of the largest IM, in Germany's case DB Netz. Note that the "High Speed Rail Network" will not correspond to the estimates of high-speed and/or international services we set out in Table 2.3.

3.28 We found no data on Great Britain defining either the relative seriousness of each type of non-violent crime or the extent to which they can be prevented or deterred by different security interventions. Similarly, we found no data quantifying and valuing other types of non-violent crime which occur either on Europe's railways or on infrastructure, stations or trains used, or in use, to produce high-speed or international rail services.

Violent crime

3.29 We also reviewed the evidence for the scale of violent crime affecting high-speed and international rail services, dealing in turn with terrorism and with other violent crime.

Violent crime: terrorism

3.30 We sought three types of evidence on the scale and impact of terrorism on high-speed and international rail services:

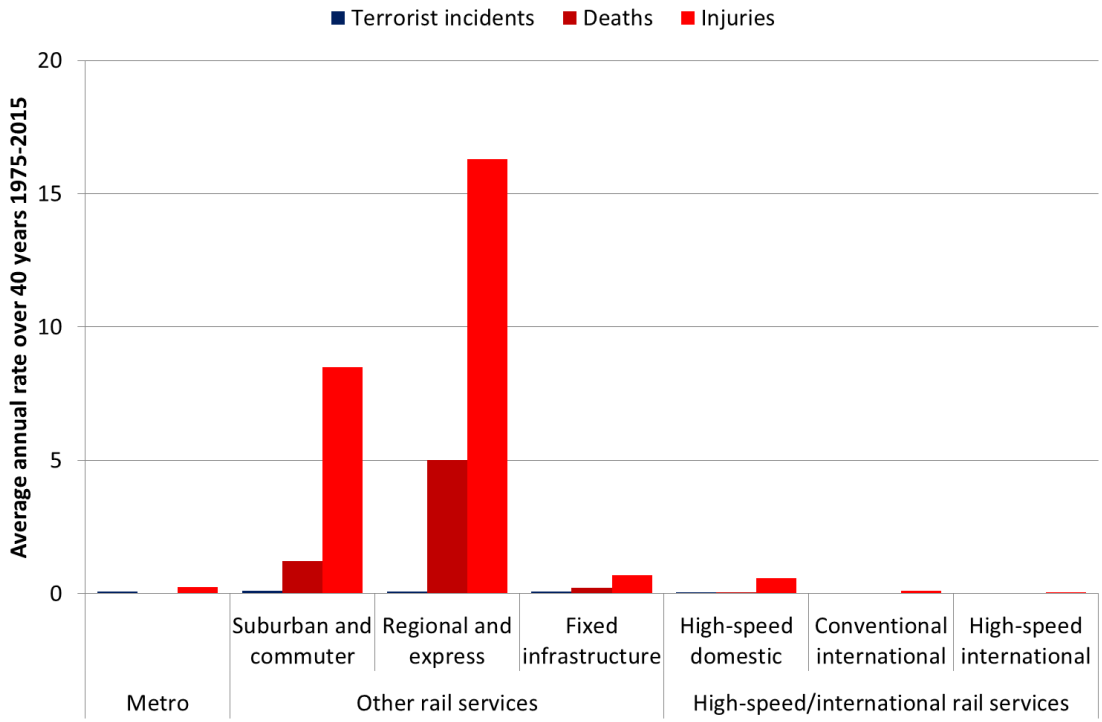
- historical records of terrorist incidents;
- current indicators of the threat level;
- current data on attacks foiled, failed and completed, and arrests; and
- estimates of the impacts of possible future attack scenarios.

Historical records of terrorist incidents

3.31 Kwink Groep[16] carried out an analysis of serious attacks on railways reported in the RAND Database of Worldwide Terrorism Incidents, from which we extracted the data shown in Figure 3.1. Over the period since 1975 they identified 16 terrorist incidents resulting in over 250 deaths and 1,000 injuries, to which we added the incident in August 2015, resulting in four injuries, which triggered this study.

[16] A study of land transport security regarding high speed trains, Final Report on Tender No. MOVE/A4/FV-521-2012, Annex 2: Overview of terrorist attacks (RAND) (WP1)

Figure 3.1: Serious attacks on railways in Europe 1975-2015, by type of rail service



Source: RAND Database of Worldwide Terrorism Incidents, Steer Davies Gleave analysis

3.32 Almost all of the incidents, deaths and injuries were on metro or suburban rail services. Only four incidents over the 40-year period related to high-speed and/or international rail services, as summarised in Table 3.4 below.

Table 3.4: Serious attacks on high-speed and international rail services in Europe 1975-2015

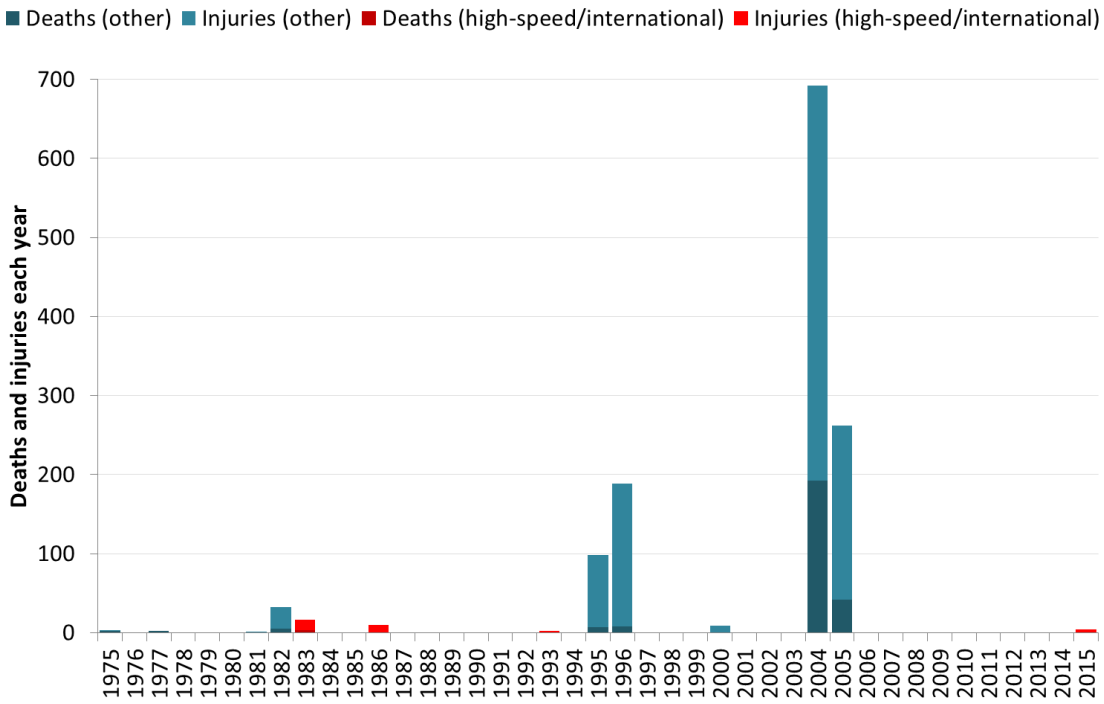
Year	Member State	Train		Deaths	Injuries	Description
		High-speed	International			
1983	France	●		2-3	13	RAND reports that a bomb on a TGV killed two people. BBC reports that three were killed and thirteen were injured.
1986	France	●		0	10	RAND reports that a high-speed train was bombed outside Paris, and ten people on board were injured.
1993	Ireland		●	0	2	RAND reports that a bomb placed on a train from Belfast to Dublin partially detonated in Dublin.
2015	Belgium	●	●	0	4	Terms of Reference state that an individual boarded a Thalys with firearms, ammunition, knives and petrol.

Source: RAND Database of Worldwide Terrorism Incidents, BBC, Terms of Reference, Steer Davies Gleave analysis

3.33 In contrast, the four incidents on high-speed or international trains resulted in a total of two or three deaths and 29 injuries over the 40-year period, half of them in the incident in 1983. There have been no deaths, and only six injuries, in almost 30 years since 1986.

3.34 Figure 3.2 shows the data from Figure 3.1 as a time series, with "other" referring to attacks on both metro and other rail systems. There have been no deaths or injuries due to terrorist attack for a decade from July 2005 to August 2015.

Figure 3.2: Serious attacks on railways in Europe 1975-2015, by date

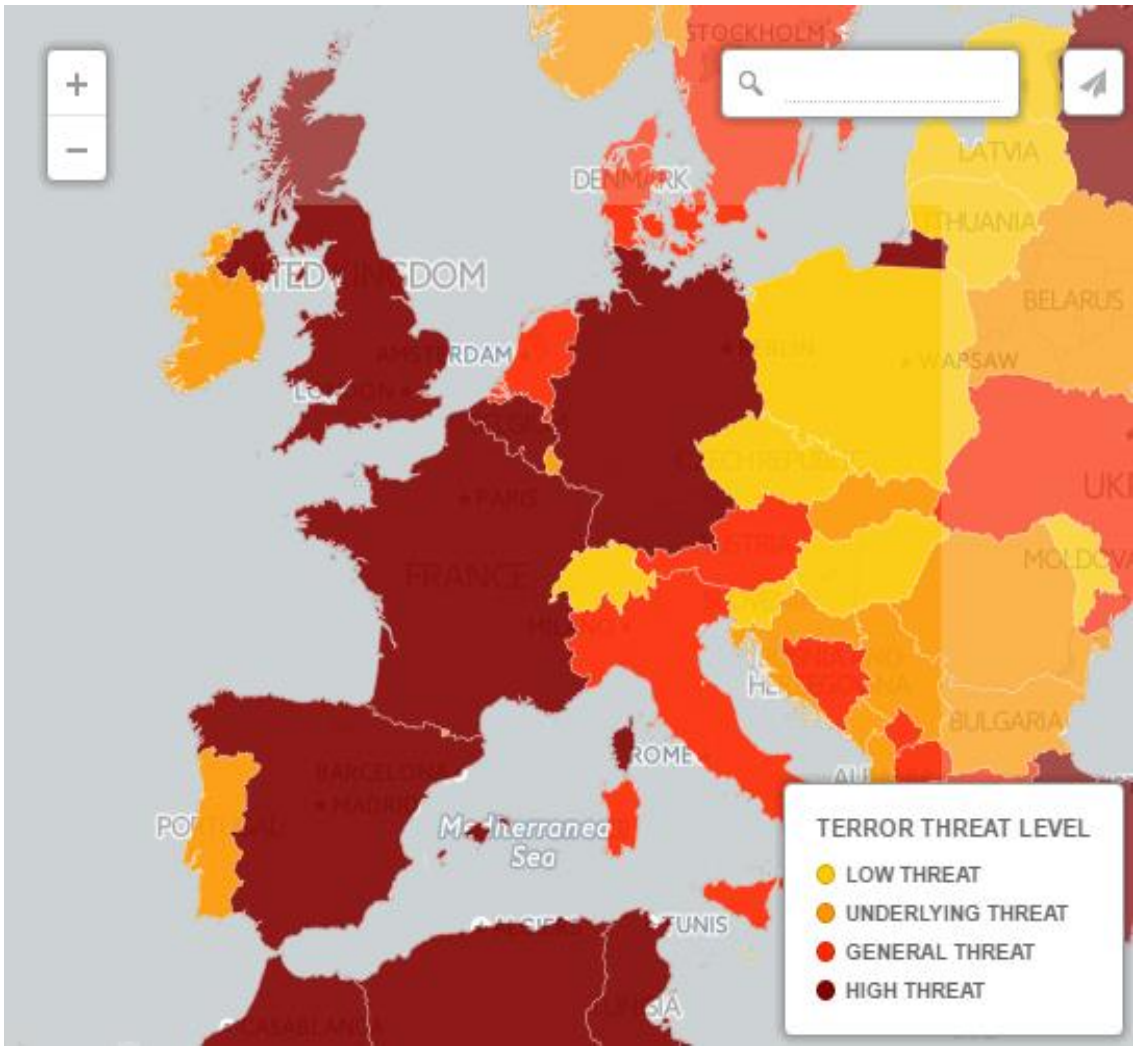


Source: RAND Database of Worldwide Terrorism Incidents, Steer Davies Gleave analysis.
Note: other includes attacks on metros shown in Figure 3.1.

Current indicators of the threat level

3.35 Given the lack of deaths or injuries in the decade before the incident in August 2015, we also sought evidence on the threat level throughout Europe. Figure 3.2 shows the UK Foreign Office's assessment of the threat across Europe.

Figure 3.3: European terrorist threat, as assessed by the UK Foreign Office



Source: UK Foreign Office, reported in Daily Telegraph[17]

3.36 A number of Member States, including Belgium, France, Germany, Spain and the UK, are assessed as having a high threat level.

Current data on attacks foiled, failed and completed, and arrests

3.37 We also found evidence supporting the assessment of threat levels. Europol's *EU Terrorism Situation and Trend Report (TE-SAT) 2016*, which includes all terrorist arrests, including ethno-nationalist and separatist arrests, reported that in 2015 there were over 200 failed, foiled and completed terrorist attacks across the EU, with over 1000 arrests, as shown in Figure 3.4.

[17] http://www.telegraph.co.uk/travel/maps-and-graphics/Mapped-Terror-threat-around-the-world/

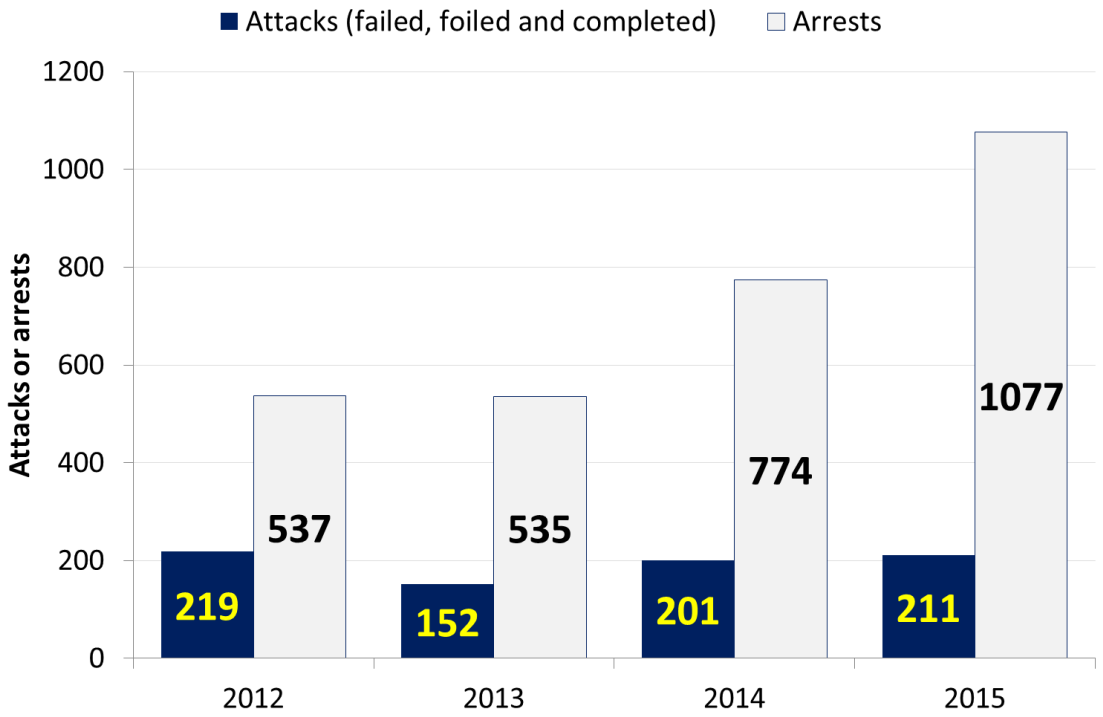
Figure 3.4: Europol reports of European terrorist attacks and arrests, 2015

Source: European Union Terrorism Situation and Trends Reports (TE-SAT) 2016
Note: Upper number (yellow on blue) shows "attacks" and lower number (blue on white) shows arrests.
Note: "attacks" are defined as "criminal acts committed by extremists with the potential to seriously destabilise or destroy the fundamental political, constitutional, economic or social structure of a country".

3.38 Figure 3.4 shows that the attacks and arrests are unevenly distributed across the Member States, with the most attacks in the UK and the most arrests in France.

3.39 Figure 3.5 shows how, while the number of attacks has remained broadly constant over the last four years, the number of arrests has almost doubled, largely because of the 424 arrests in France, where there were major attacks in January and November in Paris in 2015.

Figure 3.5: Europol reports of European terrorist attacks and arrests, 2012-2015



Source: European Union Terrorism Situation and Trends Reports (TE-SAT) 2016.
Note: "attacks" are defined as "criminal acts committed by extremists with the potential to seriously destabilise or destroy the fundamental political, constitutional, economic or social structure of a country".

Estimates of the impacts of possible future attack scenarios

3.40 Academic studies of terrorist activity have highlighted a number of direct and indirect impacts, all of which are likely to apply in the case of attacks on high-speed or international rail services[18,19]. These include:

- injury and loss of life to passengers, staff and third parties;
- damage to rolling stock, buildings and rail infrastructure;
- immediate economic damage due to reduced ability to travel;
- a reduction in travel relative to a situation in which passengers did not perceive any significant threat of an attack;
- an associated reduction in international trade and economic activity as businesses reduce their use of extended supply chains perceived to be under threat;
- an increase in insurance premiums paid by transport businesses and, in some cases, greater difficulty in obtaining certain types of insurance; and
- a reduction in investor confidence and increased costs of raising finance.

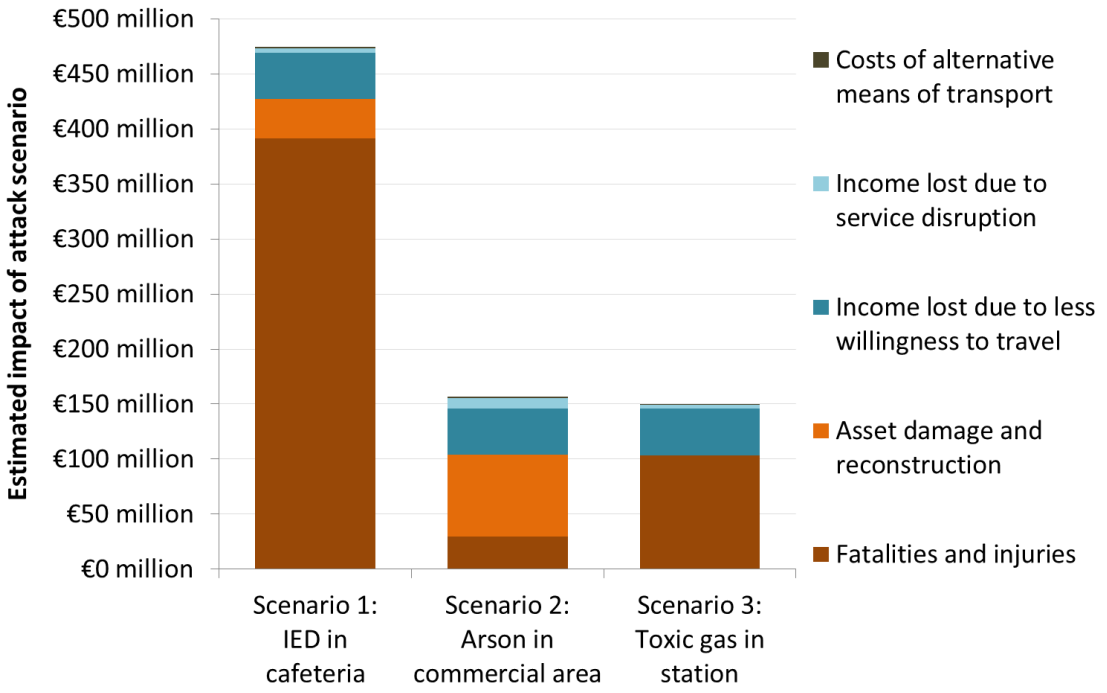
[18] Passenger Station and Terminal Design for Safety, Security and Resilience to Terrorist Attack; D.7.1 – Socio-economic potential impact (ISDEFE), 29 Nov 2013

[19] Securing America's Passenger Rails: Analysing Current Challenges and Future Solutions (N.J. Armstrong et al) 4 June 2014

3.41 We have not found any systematic attempt to quantify these impacts for attacks on high-speed and international rail services. However, as part of a recent European Commission FP7 funded study "Passenger station and terminal design for safety, security and resilience to terrorist attack", prepared under the Commission's Secure Station initiative, ISDEFE estimated the impact of a number of hypothetical scenarios involving some form of attack on rail services and/or property.

3.42 Figure 3.6 shows the estimated cost of different elements of the impact of each scenario, and demonstrates the potential for a single, unpredictable attack to cause catastrophic consequences.

Figure 3.6: Estimated impacts of three attack scenarios



Source: Passenger station and terminal design for safety, security and resilience to terrorist attack: D7.1 – Socio economic potential impact, ISDEFE, November 2013.

3.43 This suggests that, while terrorist attacks on high-speed and international rail services have been infrequent, the economic cost of some types of incident on a rail network could be €0.5 billion. In comparison, we found estimates of the economic costs of the 22 March 2016 bomb attacks on Brussels airport and metro of €1 billion[20] and 4 billion[21]. We have found no "official" estimate of the economic cost of these attacks consistent with the Commission's Better Regulation Guidelines.

[20] Politico, http://www.politico.eu/article/brussels-terror-attacks-cost-belgian-economy-almost-e1-billion-report/

[21] Newsweek, http://europe.newsweek.com/brussels-attacks-cost-belgium-4-billion-euros-440013?rm=eu

3.44 ISDEFE's exact estimate of €474 million comprises €357 million associated with 200 fatalities, €34 million associated with 317 injuries, and a further €83 million of other effects. If applied to the average annual deaths and injuries from attacks on rail services, excluding metros, shown in Figure 3.1, this suggests that the annual cost of terrorism over the 40 years since 1975 has been approximately:

- €20 million on all rail services; and
- €0.2 million on high-speed and international rail services.

Other violent crime

3.45 The British Transport Police data in Table 3.1 identifies 9,149 crimes of violence against the person, some of which we assume may be considered terrorism, and a further 1,399 sexual crimes, some of which might involve violence and/or be considered violent crime in some Member States. We have found no data from Great Britain defining either the relative seriousness of each type of violent crime or the extent to which they can be prevented or deterred by different security interventions. Similarly, we have found no data quantifying and valuing other types of violent crime which occur either on Europe's railways or on infrastructure, stations or trains used, or in use, to produce high-speed or international rail services.

Summary

3.46 Table 3.5 summarises our findings of the scale of security failures, resulting in a crime, at current levels of criminality and security intervention.

Table 3.5: Summary of estimates of the cost of security failures on rail services

Security failure	Average annual cost on rail services		Potential scale of a single incident
	All services	High-speed and international	
Metal and cable theft	€70 million	€7 million	
Vandalism and graffiti	€280 million	€30 million	
Other non-violent crime	No estimates found, but may be very large		
Terrorism	€20 million	€0.2 million	Up to €500 million
Other violent crime	No estimates found, but may be very large		
Total identified	**€370 million**	**€37.2 million**	
Passenger numbers	**9,200 million**	**300 million**	
Identified cost per passenger	4.0¢	12.4¢	
Terrorism cost per passenger	0.2¢	0.07¢	

Source: Steer Davies Gleave analysis, see text. Terrorism cost is based on European Commission Secure Station. Passenger numbers are from Table 2.3 (international plus high-speed >210 km/h).

3.47 If the patterns of crime on infrastructure, stations and trains used by high-speed and international rail services across Europe are broadly similar to those in Great Britain, listed in Table 3.1, then only a small proportion of total crime, and by implication a small proportion of total security failures, appears to relate to the areas for which we have quantified estimates.

3.48 In summary, we have been unable to form even an estimate of the total scale and cost of crime on high-speed and international rail services. However, on the basis of the limited data we have been able to identify, the total quantifiable annual cost of security failures on EU's rail

networks is €330 million or more, of which €40 million is high-speed and international lines. The largest quantifiable element relates to vandalism and graffiti.

3.49 The cost resulting from terrorism on high-speed and international rail services is a relatively small element, averaging only €200,000 per year, at broadly current prices, over the last 40 years. However:

- ISDEFE work for the Secure Station initiative has identified a credible scenario of a single terrorist attack resulting in economic costs of almost €0.5 billion, much larger than the annual average experienced at current levels of criminality and security intervention.
- Estimates of the cost of other terrorist attacks range up to at least €4 billion.

3.50 If these estimated costs are divided by our estimates in Table 2.3, of the number of rail passengers, and high-speed and international rail passengers, then:

- The cost per high-speed and international rail passenger of security failure is around 12.4¢ in total.
- The cost per high-speed and international rail passenger of terrorism-related security failure is around 0.07¢.

3.51 These estimates give an indication of the scale of additional security measures which, using a purely cost-benefit approach, could be afforded if they eliminated all remaining security failures of the types we have quantified. They also provide a context for defining a security problem, which we discuss in the next section.

4 Defining a problem

Introduction

4.1 Before developing options for increasing the security of high-speed and international rail services, we sought to define:

- the problem arising in respect of approaches to security adopted across the rail industry in the EU;
- the scale and causes of the problem; and
- the extent to which the problem is likely to persist in the absence of EU intervention.

The legislative framework

4.2 We asked stakeholders a number of questions (4-6) about national legislation on security. The responses, summarised in Appendix Table D.7 and the following text, revealed a wide range of legal frameworks. For example:

- In Austria, there is a much-amended Railway Law but railway security is governed by general legislation.
- In Greece, we were told of laws specifically related to railway theft or sabotage.
- In Spain, we were told of four different laws, one of which was specific to railways.
- In Poland, we were given a list of eight pieces of legislation, at least five of which were specific to railways.
- In Hungary, both IMs referred us to the same act on railway transport.
- In the UK, our attention was drawn to specific legislation relating to the Channel Tunnel.
- In the Czech Republic, Denmark different stakeholders referred to different legislation.

4.3 At the EU level, no legislation focuses on the security of rail or any other land transport services, although there are provisions relating to the carriage of dangerous goods, in which safety and security considerations overlap. Moreover, no pan-European body is responsible for the coordination of rail security in different Member States. However, the absence of a legislative and institutional framework, analogous to that applied in the aviation and maritime industries, is not in itself a problem. Rather, the need for such a framework must be demonstrated through the identification of a problem of significant scale that can only be addressed through intervention at the EU level.

The current situation

4.4 We set out in Section 3 how, in consultation with the Commission, we have taken security to mean:

- non-violent crime, including metal and cable theft, vandalism and graffiti; and
- violent crime, including terrorism.

4.5 We quantified the cost of security failures, to the extent possible with the data available, in Table 3.5.

4.6 From a social and legal perspective, any rail-related crime, or any other form of crime, must be considered unacceptable and represent a problem in the conventional sense. However, whether the level and cost of crime affecting Europe's high-speed and international rail services, as estimated in Table 3.5, is sufficiently unacceptable to justify further policy intervention, either at the EU or national level, is inevitably open to debate. Perceptions of an acceptable level of crime will depend on political and social perspectives, which in turn will be influenced precedents and experience in different Member States.

4.7 At the same time, security interventions against both violent and non-violent crime are likely to be sub-optimal from an economic perspective, because rail sector and other organisations can fail to undertake sufficient investment in security for a number of reasons:

- Commercially-focused organisations, while they will clearly bear significant loss following a terrorist attack or an incident involving theft of signal cable, will generally not bear the full costs to society as a whole, such as the costs of the resulting disruption to passengers. More generally, such incidents result in negative externalities that those making decisions about investment in security have no incentive to take into account.
- Public sector organisations, although they may be required to ensure the security of rail passengers, can face funding or other constraints preventing them from undertaking their preferred level of investment.

4.8 We asked stakeholders a number of questions (23-25, see Appendix B) about international cooperation and also about the practical issues of providing security against terrorism on international services.

4.9 In a number of cases stakeholders, and in particularly RUs, are unable to maintain security on cross-border services to the same standards as domestic services, because an effective approach requires some form of cross-border cooperation. At least some types of rail-related crime may therefore require better international coordination of countermeasures[22].

4.10 The threat posed by both non-violent and violent crime on high-speed and international rail services has a number of consequences, both direct and indirect:

- Crime, including terrorist attacks, may have impacts including disruption to services, damage to the railway or other property, injury and loss of life.[23]
- It can create a climate of fear for users/workers of the railways. If passengers were to perceive the threat to be significant and feel unsafe, they might be less willing to make rail journeys, undermining rail's contribution to the EU's economic and social development.

---

[22] The Council on Foreign Relations has noted that counterterrorism activity generally suffers from a failure to comply with and enforce instruments established through multilateral agreement. Within the rail sector specifically, the Community of European Railway (CER) and Infrastructure Managers, the European Rail Infrastructure Managers (EIM) and the Union Internationale des Chemins de fer (UIC) stated at a recent LANDSEC meeting that metal theft is "a cross border and organised crime which had an impact on the functioning of vital infrastructure services, inter alia railways".

[23] For example, the Port Authority of New York and New Jersey's World Trade Center station was closed for over two years following a terrorist attack, with disruption to services, damage to the railway and other property, injury and loss of life. The attack targeted nearby buildings rather than the railway itself.

- It can lead to further undesirable activity taking place, particularly in the case of graffiti. British Transport Police (BTP) in the UK have reported that the presence of graffiti tends to encourage both more graffiti and other crime[24].

4.11 Such outcomes conflict with current EU policy objectives and initiatives supporting an increase in the competitiveness of the rail sector and greater use of rail by passengers and freight.

4.12 In addition, the presence of a security threat that is regarded as unacceptable by at least a proportion of passengers is inconsistent with the Commission's overall objectives for the safety and security of transport systems, which are based in part on the concept of travel free from fear of attack as a basic right. It was against this background that the LANDSEC expert group was formed with the mission set out in Table 4.1.

Table 4.1: The mission of the Expert Group on Land Transport Security (LANDSEC)

The Group shall …
assist the Commission in formulating and implementing the European Union's activities aimed at developing policy on security relating to land transport, and shall foster ongoing exchanges of relevant experience, policies and practices between the Member States and the various parties involved.
assist the Commission in the development of instruments for monitoring, evaluating and disseminating the results of measures taken at European Union level in the field of land transport security.
contribute to the implementation of European Union action programmes in the field, mainly by analysing the results and suggesting improvements to the measures taken.
encourage exchanges of information on measures taken at all levels to promote the security of land transport and, where appropriate, put forward suggestions for possible action at the European Union level.
deliver opinions or submit reports to the Commission, either at the latter's request or on its own initiative, on any matter of relevance to the promotion of the security of land transport in the European Union.

Source: EU, http://ec.europa.eu/transparency/regexpert/index.cfm?do=groupDetail.groupDetail&groupID=2821

4.13 A question for this study is whether the activities of bodies such as LANDSEC, which have no formal powers, are sufficient to overcome the problems of externality and lack of coordination noted above and to enable the delivery of an effective level of security for users of high-speed and international rail services.

Quantifying the scale of the problem

4.14 We set out in Table 3.5 our estimates of the scale of the security problem, which we repeat for reference below as Table 4.2.

[24] The Commission informed us that they had also identified scientific studies showing that graffiti tends to encourage both more graffiti and other crime.

Table 4.2: Summary of estimates of the cost of security failures on rail services

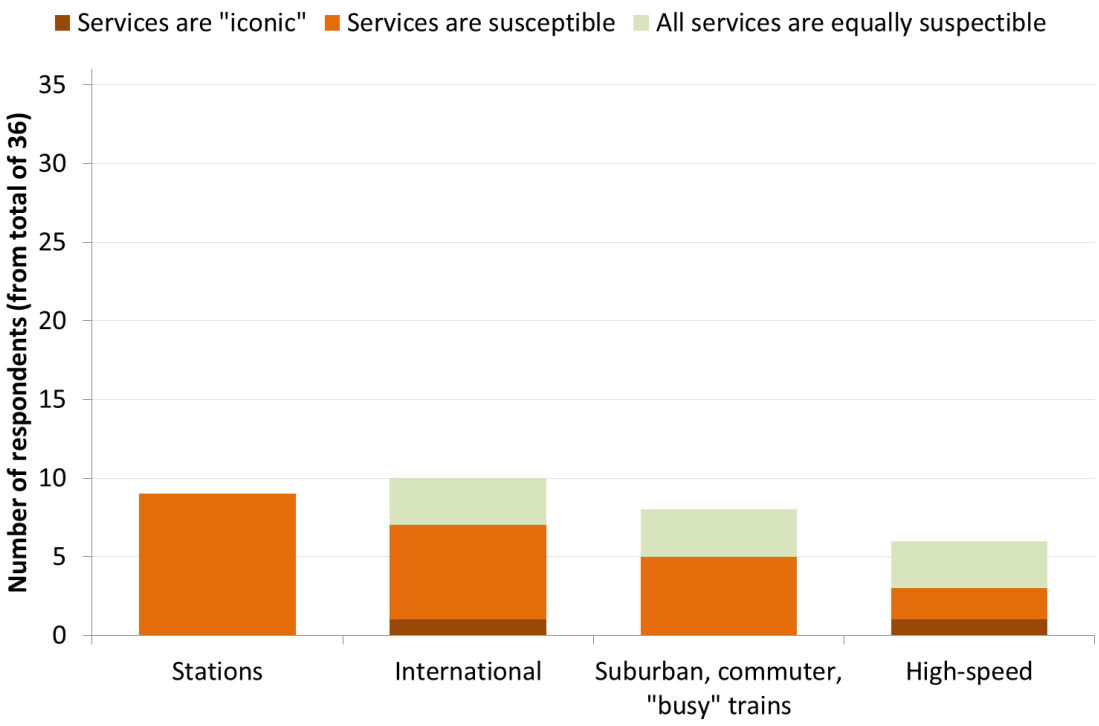
Security failure	Average annual cost on rail services		Potential scale of a single incident
	All services	High-speed and international	
Metal and cable theft	€70 million	€7 million	
Vandalism and graffiti	€280 million	€30 million	
Other non-violent crime	No estimates found, but may be very large		
Terrorism	€20 million	€0.2 million	Up to €500 million
Other violent crime	No estimates found, but may be very large		
Total identified	**€370 million**	**€37.2 million**	
Passenger numbers	**9,200 million**	**300 million**	
Identified cost per passenger	4.0¢	12.4¢	
Terrorism cost per passenger	0.2¢	0.07¢	

Source: Steer Davies Gleave analysis, see text. Terrorism cost is based on European Commission Secure Station. Passenger numbers are from Table 2.3 (international plus high-speed >210 km/h).

Terrorist crime: services at risk

4.15 We asked stakeholders what types of train were susceptible to terrorist attack. Their responses are summarised in Figure 4.1 and in Table 4.3, copied from Appendix Table D.1.

Figure 4.1: Services described as iconic or susceptible to terrorist attack



Source: stakeholder consultation, further details in Table 4.3 below.

Table 4.3: Trains susceptible to terrorist attack: stakeholder responses

MS	Source	International	High-speed	Other trains	Stations	Comment
AT	IM	No	No	-	Yes	
	RU Westbahn	No	No	-	-	Terrorists are attracted by volumes of passengers
BE	Ministry Interior	Yes	Yes	-	Main stations	Attack has occurred on a Thalys train
	Ministry Mobility	Iconic	Iconic	-	-	
CZ	Ministry	No	No	-	-	
	Regulator	No	No	-	-	
	RU ČD	-	-	-	-	Attacks are the only clear evidence of a threat
DE	DB Group	Yes	No	-	Yes	
DK	IM	No	No	Busy trains	Yes	
	Ministry	No	No	-	-	
EL	Ministry	-	-	-	-	No information available
ES	RU	Equal	Equal	Equal	Yes	Terrorists are attracted by stations and trains with a high volume of passengers
FI	Ministry	-	-	-	-	Not considered
FR	SNCF	-	-	-	-	
HR	Ministry	-	-	-	-	No variation between trains
	RU	Yes	-	-	-	International train links Croatia and Serbia
HU	IM GySEV	-	-	Passenger	-	Threat is seen to passenger, not freight
	IM MÁV	Yes	-	Commuter	-	
IE	Ministry	Yes	-	-	-	International train links to Northern Ireland and has had security issues in the past
NL	IM	Equal	Equal	Equal	-	The network is small and dense and it is difficult to differentiate
	Ministry	No	No	-	-	Threats are to “public space”
PL	Ministry	No	No	-	-	Terrorists choose places with low security
PT	IM	No	No	Suburban	Yes	Suburban stations and Rossio station are more crowded
SE	Ministry	-	-	Commuter	-	Resources should protect the many, not the high status or “iconic”
	RU	Equal	Equal	Equal	-	
SI	Ministry	-	-	-	-	No view
	RU	No	-	-	Yes	A few large stations have crowds which could be an attractive target
SK	Regulator	-	-	-	-	Slovakia is not a terrorist target
	RU	No	No	-	-	
UK	IM HS1	-	-	Commuter	Yes	Past attacks were commuter or metro
	IM NR	No	No	-	-	
	Ministry	-	-	-	-	

	Regulator	No	No	-	-	There is no evidence of some trains having an iconic status.
	RUs ATOC	No	No	-	-	Depends on terrorists' motivation
MN	Eurostar	Yes	Yes	-	Stations	Also supermarkets, sports and entertainment venues
	Thalys	-	-	-	-	Terrorist chooses easiest target

Source: stakeholder questionnaires and interviews, Steer Davies Gleave research. "-" = no response or discussion. Table is based on Appendix Table D.1 where further detail is provided.

4.16 Some stakeholders commented that rail services and stations are a particularly attractive target for terrorists because of the potential to cause large numbers of injuries and inflict substantial damage and disruption by attacking them. Other stakeholders and studies suggested that terrorists seeks targets that are either unprotected or lightly protected, and that "iconic" targets are attractive because of their symbolic value[25]. A number of high-speed and international rail services could be said to meet both these criteria, although Eurostar, which is arguably the most high profile service, and carries one in six of the passengers crossing EU borders[26], is already subject to airline-style security interventions.

4.17 Table 4.4, a summary of Table 2.3, shows our indicative estimates of the scale of high-speed and international rail services operated and the number of passengers using them.

Table 4.4: Estimates of scale of high-speed and international rail services (summary)

Data	EU total	International	International high-speed (>260 km/h)	International high-speed (>210 km/h)	High-Speed (>260 km/h)	High-Speed (>210 km/h)
Passenger numbers per year	9,200 billion	78 million EU 14 million CH+NO 4 million other	Order of 40 million	Order of 45 million	Order of 200 million	Order of 225 million
Services each way per typical weekday		650 intra-EU 50 to CH+NO 20 to others	Order of 300 intra-EU	Order of 350 intra-EU	Order of 5,000	Order of 6,000
Stations served	26,000 (estimate)	1,000 in EU 100 outside EU	Order of 200	Order of 220	400	500
Station calls per typical weekday		6,500 in EU 500 in CH+NO 200 in others	Order of 3,000	Order of 3,400	Order of 15,000	Order of 18,000

Source: Steer Davies Gleave analysis based on sources identified in paragraph 2.15, see also Table 2.3.

4.18 Given the number of high-speed and international rail services across the EU, and the volume of passengers carried, targeting such services has the potential to cause considerable injury, damage and economic loss, as ISDEFE identified in the Secure Station study (see Figure 3.6).

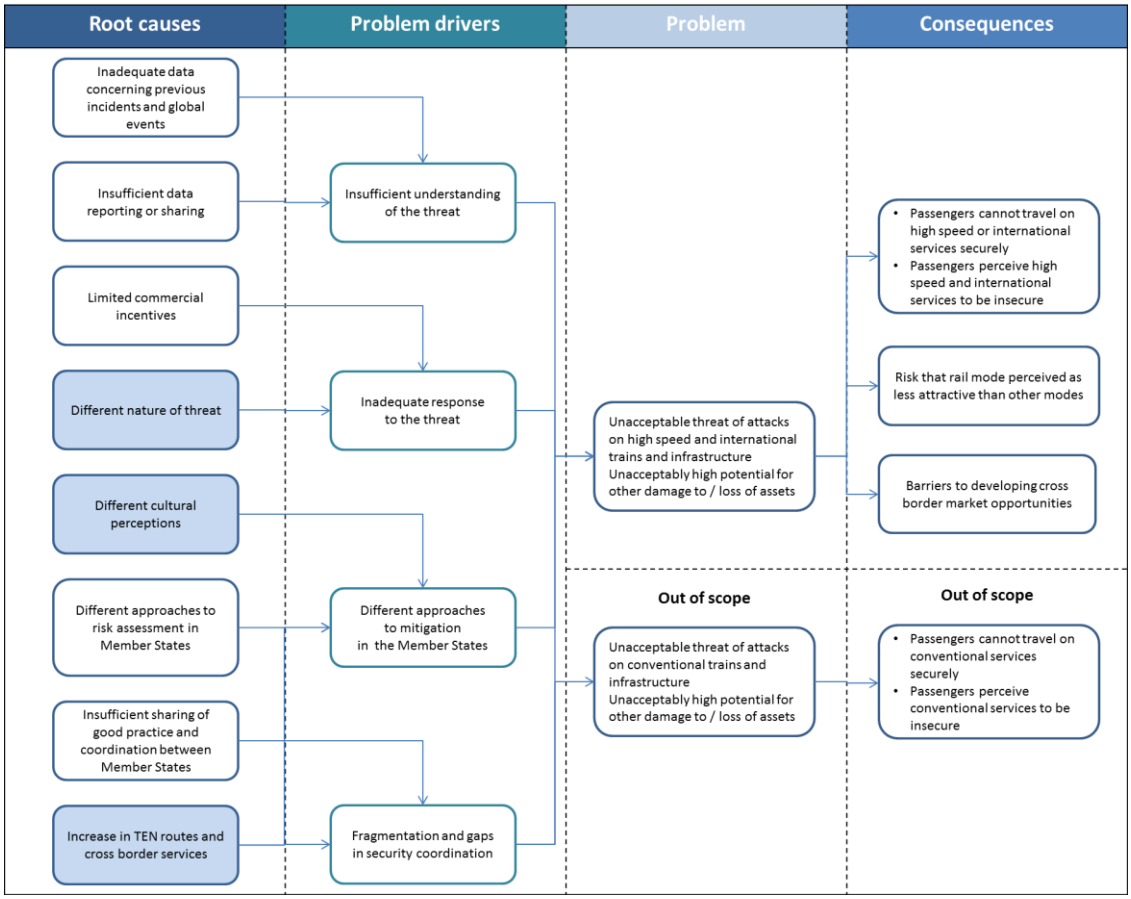
[25] Brian Michael Jenkins and Bruce Robert Butterworth, Explosives and incendiaries used in terrorist attacks on public surface transportation: a preliminary empirical examination, Mineta Transportation Institute, March 2010.

[26] Eurostar carries 13 million of the estimated 78 million passengers crossing EU borders, see Figure 2.6.

Problem tree

4.19 In discussion with the Commission, we developed a "problem tree", shown in Figure 4.2, which provides a possible interpretation of how a problem of lack of security on high-speed and international infrastructure and trains can be defined and related to a number of underlying causes. We developed the definition of the problem and problem drivers from our review of relevant literature and stakeholder consultation. The problem tree provides an overview of the apparent problem, highlighting a number of key drivers and root causes which we discuss below. As indicated, we have defined the problem as an unacceptable threat of attacks on high speed and international trains and infrastructure, together with an unacceptably high potential for other damage to, or loss of, railway assets.

Figure 4.2: Problem tree



Source: Steer Davies Gleave analysis, Commission feedback.
Note: shaded root causes are external/contextual elements and cannot be addressed by policy interventions.

4.20 We note that terms such as "unacceptably high" are open to the challenge that they are subjective since the appropriate level of security threat will vary from one observer to another. More specifically, establishing an appropriate threat level involves balancing perceptions of the relative costs and benefits of reducing the potential for crime on the railway, and perceptions will inevitably differ between individuals. However, we suggest that decision-making frameworks currently applied in the fields of both safety and security, notably the "As Low As Reasonably Practicable" (ALARP) approach identified by a number stakeholders (see, for example, **Error! Reference source not found.**) explicitly recognises the need for subjective judgements about "reasonable" risk. We also note that Tool #12 of the Better

Regulation Toolbox similarly allows for subjectivity in referring to the term "intolerable" in the context of risk assessment. We therefore consider our definition of the problem to be appropriate given the nature of security.

4.21 In our view, the problem drivers and root causes apply equally to all rail services and could inform a wider general discussion about rail security. However, services other than high-speed and international rail services are outside the scope of this study, and we only discuss them further where evidence from the rail sector as a whole is relevant to high-speed and international rail services.

4.22 On this definition of the problem, we consider the problem drivers to be:

- insufficient understanding of the threat to the rail services in question;
- an inadequate response to the threat;
- the different approaches to mitigating the threat in different Member States; and
- fragmentation of, and gaps in, the security arrangements in place.

4.23 These problem drivers are to some degree interlinked, and tend to reinforce one another. The different approaches to security may result in inadequacy of security arrangements in some parts of Europe, and the differences contribute to fragmentation and lack of coordination, particularly in the case of cross-border services. At the same time, each driver has a number of root causes, each of which must be understood if the problem as a whole is to be addressed.

The problem drivers

Problem driver: insufficient understanding of the threat

4.24 The issue of insufficient understanding of the threat relates primarily to the threat of terrorism, rather than to recurring problems such as graffiti. In the case of the terrorist threats, Table 4.3 shows how stakeholders have different views on both the scale of the threat and which stations or services are likely to be targeted:

- In some cases, the particular services highlighted by stakeholders as being vulnerable are a reflection of understandable and justifiable concerns with particular risks. In Croatia and Ireland, well-documented cross-border tensions have existed for a number of years.
- In others, there is recognition of the tendency of terrorists to target public spaces, including stations, where security is relatively low and large crowds of people accumulate.

4.25 However, stakeholders in several Member States either did not express a view or had no strong views on the susceptibility of different services and key priorities for security. Overall, the responses indicate that perceptions of the threat are driven by the circumstances and historical experience within the Member State concerned, rather than by systematic analysis of the problem across the EU as a whole.

4.26 This lack of a thorough appreciation of the threat of violent crime can be seen as the result of two underlying root causes. First, it reflects the fact that terrorist attacks in general, and those on high-speed and international rail services in particular, are infrequent events (as indicated in Figure 3.1 and Figure 3.2) and that the data on which to assess the likelihood of an event and its impacts are therefore necessarily limited. In the terminology of a recent study[27], terrorist incidents are "black swans", outside the normal experience of most people,

[27] Nassim Nicholas Taleb, The Black Swan: the impact of the highly improbable, 2007.

organisations and industries, but with an extreme impact on the individuals and communities affected by them. By their nature, such events are impossible to predict, since their likelihood cannot be assessed by statistical techniques[28]. It is therefore difficult to plan for their prevention or mitigation through the introduction of proportionate security interventions.

4.27 Understanding this aspect of the security problem is therefore considerably more difficult than assessing the likely impact of metal and cable theft, vandalism and graffiti. Detailed data on crime in Table 3.1 show that these crimes are relatively frequent, with 1,687 offences of graffiti and 1,509 of criminal damage compared to only 29 of firearms/explosives. The effect is that the associated costs, summarised in Table 4.2, can be estimated with greater confidence, and prevention and mitigation measures designed accordingly. The persistence of these security failures results from the difficulty of policing extensive national and international rail networks, rather than the inherent unpredictability of the events themselves.

4.28 At the same time, Appendix Table D.24 suggests that there is only limited reporting, sharing and analysis of information relating to security incidents that have occurred. More specifically, we did not identify any systematic collection and processing of data relating to such incidents, analogous to the work on safety by the European Union Agency for Railways (the Agency)[29]. As the agency responsible for promoting rail safety in the EU, the Agency has made a significant contribution to improving the safety of rail standards over a number of years, partly through monitoring of well-defined Common Safety Indicators (CSIs) and regular publication of safety reports used to inform national safety policies. There is no equivalent framework for rail security, although there is some overlap in safety and security interventions, and the Agency's work may therefore have also led to some improvements in security.

4.29 This lack of systematic collection and analysis of data is not the fault of the rail industry in isolation, since it is a feature of the monitoring of terrorist incidents more generally. Experts on terrorism have pointed to the fact that there is no central database on terror suspects to which security agencies in all Member States have access[30]. While the Schengen Information System contains information on undesirables, missing persons, individuals with outstanding arrest warrants and stolen cars, passports and weapons, not all Member States provide data, and those that support the database do not report information on a consistent basis.

4.30 Table 4.5 below summarises the responses to questions (26-27, see Appendix B) regarding research and suggests, at best, a mixed picture in terms of the appreciation of information and research findings available.

[28] This is particularly true of attacks carried by individuals acting alone, whose motivations are driven by their particular history rather than their association with known terrorist groups. A number of the recent attacks in Europe appear to have been perpetrated by such individuals, although at the time of writing there is considerable uncertainty about their motivation.

[29] Prior to June 2016, the European Union Agency for Railways was known as the European Railway Agency (ERA).

[30] Peter Neumann, Countering online radicalisation: a strategy for action.

Table 4.5: Research identified by stakeholders

MS	Source	Research in organisation (Q26)	Aware of other research (Q27)	Comments
AT	IM	✓	-	See Appendix A for further details.
	RU Westbahn	-	-	When the police reviewed Westbahn's existing practices, they found no need for change in its approach to rail security. If advised by the police that a change was needed, they would implement it.
BE	IM	✓	-	See Appendix A for further details.
	Ministry Interior	✓	✓	
CZ	Ministry	×	×	
	Regulator	×	×	
	RU ČD	-	-	Regular international meetings let RUs share knowledge.
DE	Ministry BMVI	-	-	See Appendix A for further details.
	DB Group	-	-	See Appendix A for further details.
DK	IM	×	UIC	See Appendix A for further details.
	Ministry	×	×	
	RU	×	UIC	See Appendix A for further details.
ES	RU	✓	✓	
FI	Ministry	×	-	May consider research in the future.
FR	SNCF	✓	✓	See Appendix A for further details.
HR	Ministry	×	✓	
	RU	×	×	
HU	IM GySEV	Some	✓	Some research is under way by MÁV (see next row).
	IM MÁV	✓	✓	
IE	Ministry	×	×	See Appendix A for further details.
	RU	×	×	
NL	IM	✓	-	See Appendix A for further details.
	Ministry	✓	-	See Appendix A for further details.
PL	Ministry	×	×	See Appendix A for further details.
PT	IM	×	×	Research is not specific to the rail sector.
SE	Ministry	×	×	Transport Ministry does not deal with terrorism security.
	RU	×	✓	Research is necessary, and RU SJ may do some in the future, but it is also aware that UIC is active in this area.
SI	Ministry	×	✓	Research may be done by universities or research institutes.
SK	Ministry	×	×	
	Regulator	×	×	
	RU	-	✓	
UK	IM NR	×	✓	Network Rail is involved in work by RSSB and the NSA, and referred to work undertaken by EIM.
	Ministry	✓	-	
	Regulator	×	✓	ORR referred to work by RSSB related to cybercrime.

MS	Source	Research in organisation (Q26)	Aware of other research (Q27)	Comments
	RU ATOC	×	✓	ATOC referred to work by the Department for Transport.
MN	Eurostar	×	-	Eurostar monitors developments but cannot fund research. It is particularly interested in technological developments such as mass screening and remote scanning.
	Thalys	×	✓	Thalys referred to work by COLPOFER.

Source: stakeholder questionnaires and interviews, Steer Davies Gleave research. "-" = no response or discussion. Table is based on Appendix Table A.23 where further details are provided.

4.31 Many rail industry stakeholders do not analyse data on rail security and/or are not aware of relevant research undertaken by other organisations. Technological research is being conducted by both Germany and France, with Austria taking a serious interest in the benefits of using facial recognition software for cable theft, but other Member States do not consider it a funding priority.

4.32 These findings tend to support the argument of at least one stakeholder[31] that better use could be made of the information available on security incidents. DB suggested that more could be done to assess the impact of security interventions already in place, and that such an assessment should be undertaken before any introduction of further measures at the EU level. It also expressed support for more practice-oriented research into security within the EU, arguing in its response to the Commission's Staff Working Document on Transport Security that:

"*the common threat resulting from international terrorism and the freedom of movement inside the Schengen Area frequently call for concerted, coordinated action. Close cooperation can save resources and the exchange of experiences enables the different actors to learn from one another*"[32]

4.33 The Commission has already taken action to encourage exchange of information on security of land-based transport by setting up LANDSEC (see Table 4.1), which provides a forum for discussing experience and good practice in the design and implementation of security interventions. However, we note that Commission Decision 2012/286/EU establishing LANDSEC neither confers any formal powers on the group nor provides explicitly for the systematic collection and publication of relevant data analogous to that undertaken by the Agency in the field of safety. In the absence of such information, a better understanding of the threat to high-speed and international rail services will continue to depend on the ad hoc and largely voluntary initiatives of individual industry stakeholders.

Problem driver: inadequate response to the threat

4.34 It is difficult to demonstrate that a given response to a security threat is inadequate, because any assessment of adequacy will vary with perceptions of risk and, as discussed above, the risk of an attack cannot be quantified with confidence. However, we describe the range of

[31] DB Group (DE), DSB (DK).

[32] Position statement on the Commission Staff Working Paper on Land Transport Security, DB (2012).

responses and its implications for the maintenance of security in Table 4.7, Table 4.8 and Table 4.9, which show how the responses and implications vary between Member States. We note that it may not be clear to an international passenger, particularly one familiar with the consistent approach to security for domestic and international air travel, why security arrangements for international rail services may change at each border.

4.35 As shown in the problem tree in Figure 4.2, we consider that inadequate responses to security threats arise for two reasons, each of which is discussed in turn below:

- commercial incentives to invest in security interventions are limited; and
- the primary threat, or perceptions of the primary threat, vary between Member States, with some responses prioritised and others ignored.

4.36 We noted above (4.7) that, given the externalities arising from terrorist attacks (see footnote 23), commercial incentives may not result in optimal investment in security interventions. Stakeholder confirmed that such incentives are weak: Westbahn and DB both stated that some high-speed or international services, operated commercially rather than under a Public Service Contract (PSC), would be made unviable by some security interventions. Westbahn, an open access operator in Austria, reported that the business case for many of the services it operates is marginal and could easily be undermined by further security costs.

4.37 We also understand that it is particularly difficult to provide commercial operators with adequate compensation for the disruption caused by recently introduced identity checks on travellers entering Sweden. To illustrate the potential costs of security arrangements, Table 4.6 summarises the findings of a recent report on the impact of Swedish identity checks[33], which disrupt the journeys of almost one in six of all passenger border crossings in the EU[34]. While the impact can be expected to vary considerably by location, these observations demonstrate the potential for substantial service disruption and associated losses for operators.

[33] The identity checks were introduced to stop the problem of illegal migration and not specifically to prevent terrorism.

[34] 12 million of 78 million passengers crossing borders.

Table 4.6: Impact of identity checks on passengers entering Sweden from Denmark

Issue	Effect
Railway operations	Københavns Lufthavn Kastrup (Copenhagen Kastrup airport) station is used for border controls: passengers towards Sweden must alight, change platforms, and board another train after identity checks. Suburban and regional services at peak times cut from 6 trains per hour to 3 trains per hour. Long-distance X2000 services from Sweden to Denmark no longer call at the airport. Regional services within Denmark cancelled.
Effect on passengers	Some trains cancelled, as listed above. Lower peak frequency and hence capacity means extreme crowding. Travel times are 10-60 minutes longer, depending on journey, and less predictable. Sweden-Denmark commuting and collecting children from school are extremely difficult. 12% fewer passengers in early 2016, against expected 5% growth, an effective 16% fall. 8% fewer travel passes issued in Sweden.
Effect on other transport	Copenhagen metro has expanded services to Kastrup airport to relieve overcrowding. 21% more coach travel across the Öresund bridge reported by Swebus. 500 more car trips per day across the bridge, even with extensive car-pooling.
Economic costs (all modes)	Estimated €150 million annual cost to the regional economies with checks into Sweden. Estimated €300 million annual cost to the regional economies with checks in both directions.

Source: Øresundsinstituttet. Note that economic costs include the (smaller) effects on bridge and ferry services.

4.38 Against this, it can be argued that some investment designed to meet other objectives, such as investment in station gating to reduce fraud, has security benefits. This is an example of a positive externality, with the introduction of gating tending to discourage (although not necessarily eliminate) attacks and vandalism. However, stakeholders have confirmed that incidental security benefits of this kind are limited, and that the lack of a commercial case for gating stations in sparsely populated areas, many of which may not currently be staffed (see Figure 2.2) will mean that railway systems will remain open and vulnerable in the absence of specific security requirements[35].

4.39 Our stakeholder interview programme also demonstrated that different Member States, and different regions within Member States, prioritise different security responses based on their perceptions of the primary threat. Hence, the focus may be on:

- vandalism and cable theft, in Member States that do not consider themselves targets of terrorist activity, such as Slovakia;
- domestic terrorism, in regions with a history of such attacks, such as the Basque region of Spain and Northern Ireland within the UK; and
- international terrorism, in Member States that experienced attacks by groups claiming to be motivated by unrest in Africa and the Middle East, such as Belgium and France.

4.40 This focus on the primary threat from a domestic perspective is understandable and rational, given constraints on public funding and the consequent need to prioritise particular types of security intervention. However, this approach introduces a risk that stakeholders will fail to

[35] Stakeholders in Belgium, Germany, France and Croatia reported a philosophy access cannot be prevented to stations as they are open, although restriction of access to (some) platforms may be acceptable. This is also evidence in Figure 2.2 (taken in Austria on a line operated by Deutsche Bahn).

take account of their potential role in reducing security threats across the EU as a whole, for example by limiting measures that might help to limit terrorist access to international rail services. This underlines the importance of coordination across borders highlighted by DB (See Appendix D, **Error! Reference source not found.**).

Problem driver: different approaches to mitigation

4.41 The findings from our interview programme demonstrate a wide range of approaches to maintaining security across the EU.

4.42 Appendix Table D.4, repeated below as Table 4.7, summarises specific security interventions deployed to protect rail services and infrastructure in different Member States.

Table 4.7: Existing security interventions

MS or RU	Ticket and identity (ID) checks				Baggage and passenger screening				Patrols	
					Specific train		Wider area			
	Ticket check or gating for station	Ticket check or gating for specific train	Must show ID	Ticket and ID matched "Nominative ticketing"	Baggage	Passenger	Baggage	Passenger	On train	Wider area
AT	×	×	×	×	×	×	×	×	×	Risk
CZ	×	×	×	×	×	×	×	×	Some	Some
DE	×	×	×	×	×	×	×	×	Risk	Police
DK	×	×	Only to SE	×	×	×	×	×	×	Police
ES	Most	×	×	×	Some	Some	×	×	Risk	Some
FR	×	×	Some	Some	Some	×	Some	×	×	Some
HR	×	×	×	×	×	×	×	×	Risk	Some
HU	×	×	×	×	×	×	×	×	Some	Some
IE	×	Some	×	×	×	×	×	×	×	Some
PT	Some	×	×	×	×	×	×	×	×	Some
SE	×	×	×	×	×	×	×	×	×	Some
SI	×	×	×	×	×	×	×	×	×	Some
SK	×	×	×	×	×	×	×	×	Some	Some
UK	Some	×	×	×	×	×	×	×	×	Police
Eurostar	×	Yes	Yes	×	Yes	Yes	×	×	×	Police
Eurotunnel	Yes	Yes	Yes	×	×	×	×	×	×	×
Öresundståg	×	×	Only to SE	×	×	×	×	×	×	×
Thalys	×	×	Some, in FR	×	Some	Some	×	×	Police	Police

Source: stakeholder questionnaires and interviews, Steer Davies Gleave research. "-" = no response or discussion.
Note: all national networks have many stations which are unstaffed and not patrolled.
Note: on patrols "Police" means that the police may patrol if they wish, "Risk" means a risk-based approach.

4.43 Table 4.8 summarises stakeholder responses on measures to protect infrastructure.

Table 4.8: Security interventions to protect railway infrastructure

MS	Source	Identification of vulnerable infrastructure/ mitigation	Interventions to protect remote infrastructure	Comments
AT	IM	✓, and patrols	✓	Patrolling occurs to deter all crime, such as metal theft.
BE	IM	✓	✓	See Appendix D for further details.
DK	IM	×	×	Police assess that terrorists could not do material damage. Security is limited to fencing car parks to deter graffiti.
	RU	×	-	Paris attacks were against dense crowds of people, not remote infrastructure.
EL	Ministry	✓	-	See Appendix D for further details.
FR	SNCF	✓	✓	Infrastructure assessments are confidential. SNCF is working with Thales and Airbus on drones to protect infrastructure.
IE	RU	✓	-	See Appendix D for further details.
HU	IM GySEV	×	×	No critical infrastructure is identified, but the IM will respond once an incident has taken place.
NL	IM	✓	✓	Drones are being considered to patrol infrastructure, such as to monitor bridges, and could contribute to security. See Appendix D for further details.
PT	IM	✓	✓	The busiest bridges and tunnels are identified. Some infrastructure has intruder alarms and video surveillance.
SE	IM	×	-	See Appendix D for further details.
SI	RU	✓	-	SŽ has identified two critical infrastructure locations which would cause major economic damage if disabled, deliberately or otherwise, and IT and signalling systems.
UK	IM NR	✓	-	Most critical items are on the national register.

Source: stakeholder questionnaires and interviews, Steer Davies Gleave research. "-" = no response or discussion. Table is based on Appendix Table A.20 where further details are provided.

4.44 Table 4.9 summarises stakeholder responses on training measures, further details of which are provided in Appendix Table D.18.

Table 4.9: Security interventions in the form of training

MS	Source	Regulatory required training on response to security threats	Specific training on threat awareness	Specific training on reacting to a terrorist attack	Training of others (third parties	Staff/others suspicious behaviour	Staff/others correct response
AT	IM	×	✓	✓, see text	×, see text	-	-
	RU Westbahn	-	✓, see text	?, see text	Not relevant	-	-
BE	IM	×	×	-	✓	-	-
	Ministry Interior	✓	-	-	-	-	-

MS	Source	Regulatory required training on response to security threats	Specific training on threat awareness	Specific training on reacting to a terrorist attack	Training of others (third parties	Staff/others suspicious behaviour	Staff/others correct response
	Ministry Mobility	×	-	-	-	-	-
CZ	Ministry	✓	-	-	-	-	-
	Regulator	×	-	-	-	-	-
	RU ČD	?	✓	✓	✓	-	✓
DE	Ministry BMI	-	-	-	×	-	-
	DB Group	?	-	-	-	-	-
DK	IM	×	×	×	×	×	×
	RU	-	✓	✓	×	-	-
ES	RU	✓	-	-	✓	×	×
FI	Ministry	×	-	-	-	-	-
FR	SNCF	✓	×	×	×	-	-
HR	Ministry	×	-	-	-	-	-
	RU	×	×	×	×	-	×
HU	IM GySEV	✓	×	×	×	×	×
	IM MÁV	×	✓	×	-	✓	×
IE	Ministry	✓	-	-	-	-	-
	RU	✓	✓	✓	✓	✓	-
NL	IM	?	✓	×	×	×	×
	Ministry	?	-	-	-	-	-
PL	Ministry	?	-	-	-	-	-
PT	IM	✓	×	×	-	×	-
SE	IM	×	-	-	-	-	-
	RU	×	×	×	×	×	-
SI	Ministry	✓	-	-	-	-	-
	RU	-	✓	?	-	-	-
SK	Ministry	×	-	-	-	-	-
	RU	✓	✓	-	-	✓	✓
UK	IM HS1	×	-	-	-	×	-
	IM NR	✓	✓	✓	✓	✓	-
	Ministry	✓	-	-	-	-	-
	Regulator	×	-	-	-	-	-
	RU ATOC	✓	✓	✓	-	✓	✓
MN	Eurostar	✓	✓	-	-	-	-
	Thalys	?	✓	✓	×	-	-

Source: stakeholder questionnaires and interviews, Steer Davies Gleave research. "-" = no response or discussion. Table is based on Appendix Table A.18 where further details are provided.

4.45 The tables illustrate a number of points.

4.46 Table 4.7 shows that, other than patrols, the deployment of security interventions to protect services in most Member States is limited, although France and Spain make use of screening, and France also employs identity checks. The most intensive security relates to Eurostar, Eurotunnel and Thalys, reflecting either the specific requirements for services operating through the Channel Tunnel, which serves one in four of all passenger border crossings in the EU[36], or direct experience of an attack on a train. However, Thalys advised us that it only carries out systematic checks of passengers and baggage at Paris Gare du Nord[37].

4.47 Table 4.8 shows that, in a number of Member States, vulnerable infrastructure has been identified, and mitigation measures have been put in place but, in other Member States, remote infrastructure appears to be relatively unprotected.

4.48 Table 4.9 shows that there is no consistency in the approach to training in security, with some Member States making training a regulatory requirement and others leaving the extent of training to rail organisations to decide. There is also no consistency in the types of training provided, although few Member States appear to provide training in all aspects of security.

4.49 The general lack of airline style security interventions, including identity checks and screening, reflects railway operational constraints and the fundamental nature of the services operated. In the course of our interview programme, both Westbahn (an open access operator in Austria) and DB (a national rail operator) stated that their business model was based on “turn up and go”, whereby passengers could arrive at a station and purchase a ticket after boarding a train. Westbahn further informed us that many of its passengers are attracted to its services from ÖBB, the incumbent RU in Austria, which requires them to book in advance, and that over 60% of its passengers arrive at the station less than 10 minutes before departure. DB, in its response to the Commission Staff Working Paper on Land Transport Security cited above, has also stated that railway infrastructure has been designed for accessibility.

4.50 The literature review, and discussions with stakeholders, identified two main causes of the observed differences in the type of security interventions adopted in Member States.

4.51 First, cultural differences affect attitudes to, and hence willingness to deploy, different kinds of security interventions. In a study undertaken as part of the Secure Station initiative, D'Appolonia SPA (DAPP) provided evidence that the presence of visible security interventions tends to enhance the sense of security among passengers[38]. However, stakeholders suggested that attitudes to specific measures can vary considerably. For example:

- CCTV monitoring is ubiquitous in the UK, but requires special justification in Sweden;
- routine searching of passengers is similarly regarded differently in different countries; and

[36] 20 million of 78 million passenger border crossings, see Figure 2.6.

[37] A number of stakeholders also commented that these arrangements were merely for show, and were not systematically applied, undermining their effectiveness and rationale (see 6.36).

[38] DAPP, Passenger station and terminal design for safety, security and resilience to terrorist attack: Research into the acceptability of security options recommended by Secure Station, 2014.

- items such as pocket knives, which can clearly pose a threat to passengers and staff at stations and on trains, are routinely carried in some parts of Europe[39].

4.52 Second, different approaches to risk assessment lead to different conclusions about the appropriate focus of security expenditure. Table 4.8 indicates that patrolling of railway infrastructure, typically out of sight of passengers on stations and trains, is commonplace across the EU. However, public attitudes to patrolling of stations and other public areas by identifiable security personnel, armed police, or military personnel, vary considerably. Such patrols have become relatively frequent in Belgium and France, following recent terrorist attacks, but we were told that armed patrols on stations and trains would be unacceptable in Sweden. Swedish RU SJ told us that patrols at stations are undertaken by station staff, and that trains are not normally patrolled at all.

4.53 The deployment of security interventions is also affected by the approach to risk assessment adopted in a given Member State, which may itself be influenced to a degree by cultural factors. Stakeholders indicated that the majority of Member States made some assessment of the threat of a terrorist attack, but the extent to which this drives decision-making within the rail sector varies (see also Appendix Table D.6):

- Germany has a localised threat level, as many stations in the country are remote and unattended.
- France has a national threat level determined by the state.
- Hungary has no formal system of defined threat levels.
- Some interviewees could not state the current threat level.
- Other interviewees knew the threat level, which informs decisions on security within the rail sector. This might be through predefined standard procedures associated with each threat level, but in many cases the security agencies give specific advice and instructions on the basis of the information they hold about the level, nature and location of the threat.
- Some interviewees commented that the threat level was rarely or never changed, and that no linkages had been developed between the threat level and security interventions adopted in the rail industry.

4.54 We also asked whether security requirements were prescriptive (giving exact rules, directions, or instructions about how to ensure appropriate security levels) or output-based (defined only in terms of a required level of security) and whether there was an explicit risk assessment. The responses summarised in Table 4.10 indicate a wide range of approaches, although it appears that most Member States carry out some form of risk assessment.

Table 4.10: Approaches to determining appropriate security interventions

MS	Source	Requirements	Risk assessment	Safety Management System (SMS)	Comments
AT	IM	Output-based	In hand	In hand	See Appendix D for further details.
	RU Westbahn	Output-based	✓	✓	See Appendix D for further details.

[39] We note, however, that the British Transport Police Statistical Bulletin identifies crimes related to "firearms/explosives" but not crimes related to knives (see Table 3.1).

MS	Source	Requirements	Risk assessment	Safety Management System (SMS)	Comments
BE	IM	Output-based	✓	✓	See Appendix D for further details.
	Ministry Interior	-	✓, OCAD	-	See Appendix D for further details.
	Ministry Mobility	Output-based	Not formally	-	See Appendix D for further details.
CZ	Ministry	-	✓	-	Rules are set out internally in the agreements between the contracting authority and the security agencies.
	Regulator	-	×	-	
	RU ČD	Output-based	✓	-	
DK	IM	Output-based	✓	Unclear	See Appendix D for further details.
	Ministry	-	×	-	See Appendix D for further details.
	RU	Prescriptive	✓	-	See Appendix D for further details.
ES	RU	Both	✓	-	There is a process of continuous improvement.
FI	Ministry	Not applicable	✓	-	The Ministry TSA maintains a risk register, but this is because it is the NSA and this applies to general safety rather than terrorism.
FR	SNCF	-	✓	-	See Appendix D for further details.
HR	Ministry	-	×	-	The Ministry of the Maritime Affairs, Transport and Infrastructure has no risk assessment process.
	RU	Prescriptive	✓	-	RU maintains risk assessment process covering all type of risks, but only for rail services.
HU	IM GySEV	Prescriptive	✓, in SMS	✓	
	IM MÁV	Prescriptive	✓	-	
IE	Ministry	Output-based	Unclear	✓	RUs meet regularly with police to discuss risks but apparently no systematic risk assessment. There is some use of Cost Benefit Analysis.
	RU	Output-based	-	✓	See Appendix D for further details.
NL	IM	-	✓, see text	-	
	Ministry	-	✓, see text	-	
PL	Ministry	Prescriptive	✓, in SMS	✓	The SMS is owned by the IM.
PT	IM	-	✓	-	
SE	Ministry	Set informally by the police	✓	-	Terrorism is considered as a risk but not as a high risk.
	RU	-	✓	-	Much legislation on safety is overall prescriptive but highly output-based.
SI	Ministry	Prescriptive	×	-	See Appendix D for further details.
SK	Ministry	-	×	-	See Appendix D for further details.
	Regulator	-	-	-	See Appendix D for further details.
	RU	Prescriptive	✓	-	The framework is prescriptive, but some parts are solved operationally.

MS	Source	Requirements	Risk assessment	Safety Management System (SMS)	Comments
UK	IM HS1	Output-based	✓	-	See Appendix D for further details.
	IM NR	Mixed	✓	✓	See Appendix D for further details.
	Ministry	-	✓	-	See Appendix D for further details.
	Regulator	-	✗	-	See Appendix D for further details.
	RU ATOC	Mixed	✓	-	ATOC said that requirements were "75% prescriptive"
MN	Eurostar	Varies by MS	✓	-	See Appendix D for further details.
	Thalys	-	In hand	-	See Appendix D for further details.

Source: stakeholder questionnaires and interviews, Steer Davies Gleave research. "-" = no response or discussion. Table is based on Appendix Table A.12 where further details are provided.

4.55 In addition, the methodologies used to assess risk vary significantly. A clearly structured approach was described in the Netherlands, with a systematic methodology to:

- identify the risks;
- develop scenarios;
- compile risk profiles;
- draw up an inventory of measures;
- determine the residual risks; and
- carry out a cost-benefit analysis and select appropriate solutions.

4.56 In the Netherlands, both IM ProRail and RU NS are obliged under their contracts to implement an operational risk-and-threat based management system. They must also continue to report to the Ministry to ensure effective implementation of the security management system. We found no evidence of this approach to risk assessment and implementation being replicated in other Member States. By contrast, the relevant Ministry in Slovenia informed us that a counter-terrorism threat assessment is undertaken at the national level but this is not specific to the rail sector. Rail security requirements are relatively prescriptive, as is the case in a number of East European Member States.

4.57 As part of the Secure Station initiative, InteCo compiled a catalogue of user requirements for security systems, and noted the need for a recognised risk assessment methodology for security risk which allows for prioritisation of threats. It also suggested that there is a need for guidelines on accepted methods of risk mitigation, supported by examples of best practice. The responses to InteCo's questionnaire showed that, while 94% of InteCo's respondents carried out safety risk assessments, only 74% undertook security risk assessments.

4.58 While the risk of a given security threat can clearly vary between Member States:

- It is difficult to provide a justification for material differences in the methodologies used by railway organisations to assess risk.
- There is no clear justification for such organisations relying on general assessments made by Ministries, with only limited reference to the particular vulnerabilities of rail services and infrastructure.

4.59 More specifically, different approaches to risk assessment can mean that perceptions of risk, and associated mitigation measures, differ because of the methodology applied rather than because the underlying risk is materially less on one side of a border than the other. Hence, in

the absence of a consistent methodology, it is difficult to determine whether the response to a given threat in a particular Member State is adequate.

Problem driver: fragmentation and gaps in security coordination

4.60 We asked stakeholders about legislative arrangements, and of the allocation of responsibility for rail security matters in different Member States. The following examples illustrate the challenge in ensuring effective coordination between key stakeholders with complementary and/or overlapping responsibilities.

4.61 In Belgium, the main security authorities are the Chief of Police Services and the National Security Council (NSC), which is the responsibility of the Minister of Internal Affairs. The National Safety Authority (NSA) also has a significant role given the link between safety and security. The National Authority for Security of Rail Transport plays a coordinating role, in collaboration with IM Infrabel and RUs in assessing the vulnerability of the rail network and establishing best practice security responses. Unlike IMs in other Member States, Infrabel is not responsible for stations, although it considers that it has a "moral duty" to protect all infrastructure assets.

4.62 In Germany, the approach to decision-making in the field of security reflects the country's federal structure. There is a Joint Centre for Counter Terrorism, providing a platform for cooperation between the different security bodies at both Federal and Länder level. The Federal Police have powers to access CCTV in stations and to recommend installation and upgrading, but have no authority to install it. Instead, decisions to install CCTV equipment are made by the relevant competent authority, which may instruct a railway undertaking to carry out the necessary works. There is also a separate railway security service, DB Sicherheit, which provides a security presence at stations and has limited powers to respond to security incidents: for example, it can seal off the area around a suspected explosive device, but cannot taking action to dispose of it. We understand that there has been no training of DB Sicherheit staff in responding to terrorist attacks or detection of suspicious behaviour, because these responsibilities fall to the Federal Police.

4.63 In the UK, IMs are responsible for maintaining the security of the network and are not permitted to delegate the role to another agency. However, a security company patrols the network and maintains relationships with communities bordering the infrastructure. Network Rail, the main IM, is responsible for implementing a National Rail Security Programme (NRSP) mandated by the Department for Transport (DfT).

4.64 The allocation of responsibilities is important, because individual organisations will limit their response to a given threat according to their defined role. This can result in gaps in security coverage, potentially making it easier for perpetrators to carry out an attack. Stakeholders did not provide specific examples related to high-speed or international services, but the Belgian Ministry noted that the Brussels metro is the responsibility of the city authorities and is therefore not patrolled by the national railway police. In Great Britain, the British Transport Police also patrol many, but not all, of the British metro and light rail networks (see footnote 8). However, while the examples given above relate to coordination between national bodies, we note that the greater the number of such bodies, the more complex coordination across international borders is likely to be.

4.65 The difficulties of coordinating national authorities with different areas of responsibility are mirrored by the challenges of coordinating security arrangements across borders, particularly in the case of international services. As indicated in the problem tree in Figure 4.2, we

consider shortcomings in such coordination to be a key root cause of the fragmented security arrangements observed in a number of cases. More specifically, while relevant agencies in different Member States do collaborate to maintain security on cross-border services, in most cases they continue to operate within their respective national jurisdictions, which can result in an inconsistent response to security threats.

4.66 A number of issues were highlighted by the literature review and stakeholder engagement:

- Thalys noted that powers granted to police in one Member State may not apply in another. SNCF police, who are armed, are not permitted to enter Belgium, where they have no right to bear arms. SNCB police, who are not armed, are permitted to enter France but once there have no powers to search, arrest or even question passengers.
- UIC, in a presentation to a UNECE Workshop on Rail Security in 2013, noted that equivalent constraints apply to railway staff. Train managers employed by Thalys have authority to challenge passengers without tickets, or exhibiting other behaviour indicative of a potential security threat, in the Netherlands but not in Belgium, France or Germany.
- Similar issues arise in respect of access to CCTV footage, which is typically protected by national data protection legislation. CCTV monitoring is ubiquitous in the UK, but requires special justification in Sweden (4.51), and in Germany the Federal Police have powers to access it but not to require that it is installed or to specify its coverage (4.62). This means that, despite the need for coordinated effort to identify a potential perpetrator of an attack on an international service, it may not be possible to share footage with security agencies on the other side of a border.

4.67 We also identified examples of security interventions introduced by one Member State having unintended consequences in another. In particular, the introduction of identity checks on rail passengers entering Sweden has reduced suburban and regional services on the Öresundståg network (Figure 2.7) by 50% (see Table 4.6). This has imposed substantial costs on the operator, resulting in the withdrawal of some international services and affecting a number of Danish domestic services and station stops.

4.68 In contrast, the need for effective coordination of security arrangements within and between different Member States has increased with the development of the TEN-T and broader international rail network. As the size of the network has grown (particularly with new links such as the Channel Tunnel and Öresund Bridge, see 2.35), facilitated by EU initiatives to improve interoperability, such coordination has become more challenging and gaps in, and fragmentation of, security arrangements more evident.

4.69 The challenge of maintaining the security of a growing network is further complicated by the fact that both high-speed and international rail services are often integrated with domestic services. For example, in the course of our interview programme:

- Infrabel, the IM in Belgium, told us that only Eurostar services are fully segregated at Brussels Midi. Platforms 3 to 6 are generally, but not exclusively, used for Thalys services. The segregation of Thalys services has been investigated but has not proved possible because of the need for other services to use these platforms in the peak.
- Thalys advised us that there is segregation of its services at Gare du Nord in Paris, with a fence separating adjacent platforms used by French TGV domestic services. However, this requires substantial resourcing, including dedicated staff to undertake X-ray control of baggage and to prevent items from being passed over the fence.

- Iarnród Éireann, the RU in Ireland, noted that some segregation of international services is possible but this is not complete, and measures such as baggage screening were introduced in the past during periods of heightened tension.

4.70 This makes high-speed and international rail services difficult to segregate for the purposes of security, at least without substantial investment in the infrastructure. Further, the interfaces between these services and conventional services can be expected to increase as the high-speed and international networks develop, making it more difficult to reconcile the open nature of rail systems that underpin their competitiveness with higher levels of security for specific types of operation.

The EU dimension

4.71 Development of international rail services, some of which are also high-speed, is a key element in the creation of a single railway area and they contribute more generally to the growth of the single market. Any threat to the security of passengers using such services that might reduce their attractiveness and undermine the Commission's efforts to promote the competitiveness of rail travel relative to other modes. It might also inhibit the broader movement of goods, services, people and capital across national borders, reducing competitiveness and economic and social development across the EU as a whole.

4.72 However, while these cross-border consequences suggest the need for an EU level response to the problem, the international aspects of the underlying causes are arguably more important in providing a justification for supplementing national rail security policy with EU initiatives. The evidence suggests that the EU dimensions of the problem can be summarised as:

- insufficient sharing of information between different actors within the EU rail sector, tending to accentuate the problem of an overall lack of data, due to the infrequency of the events that security interventions are intended to prevent or mitigate;
- different approaches to risk assessment, which make it difficult to determine whether the different approaches to rail security often applied on different sides of a border reflect genuine and material differences in underlying risks, or different (and potentially mistaken) perceptions of risk arising from the methodologies applied;
- specific coordination issues, typically preventing staff with security responsibilities from acting effectively to reduce security risks along the entire length of an international journey; and
- the growth of high-speed and international networks across the EU, coupled with the difficulties of segregating these services from necessarily open domestic networks sharing the same stations and track.

The stakeholders

4.73 Our stakeholder engagement exercise has not included engagement with the parties primarily responsible for the problem, in the form of security threats, but we have collated interviews and written requests for information from the stakeholders identified by the final column in Table 1.4.

The evolution of the problem

4.74 We have considered how the problem might evolve in order to define a baseline scenario for the purposes of modelling impacts of options for improving security. The baseline includes a projected profile of the cost of security incidents over a defined time period in the absence of

any further intervention to improve the security of high speed and international rail services at the EU level. It is therefore determined by:

- the expected number of security failures of different kinds, including both incidents involving violent crime such as terrorist attacks and non-violent incidents such as metal theft;
- the impact of those incidents, including damage to property, disruption to rail services and, in the case of violent attacks, casualties among rail passengers and staff; and
- the evolution of security interventions of various kinds having an impact on the frequency of security failures and/or their effects as well as on perceptions of security.

4.75 The baseline is also defined by reference to the level of the security threat in each Member State and its impact on the demand for high speed and international services, which is separate from, although potentially influenced by, the scale and frequency of actual security failures.

4.76 We describe our assumptions in relation to each of these elements of the baseline in the following paragraphs. We begin by considering the development and application of security interventions of the kind summarised in Table 3.2, noting that there are no independent forecasts of such developments and that any observations on possible progress in their implementation must be based on the opinion rail sector stakeholders and security experts.

Evolution of security interventions

Basic interventions

4.77 None of the stakeholders we contacted mentioned any initiatives to change the extent of basic security interventions such as fences, gates and locks. We assume that these are mature technologies and their scope and effectiveness will continue broadly as at present, although we note that they might in principle be rendered superfluous by other, more effective interventions. For example, locks might be replaced by smartcards or facial recognition.

Interventions in communications and external liaison

4.78 Changes to national legislation on matters such as the powers of the police, or duty to liaise with emergency services might, in principle, result in changes to the patterns of communications and external liaison in security matters. However, none of the stakeholders reported expecting major changes in their networks of communications and liaison, and over time we would expect there to be a mixture of new linkages and networks being established and existing ones being used less or abandoned.

Interventions in assets and equipment design – barriers, screening and segregation

4.79 Ticket barriers have been used for many years on the railways and are a mature technology. Stakeholders did not mention any material plans to extend the use of barriers, and in a number of Member States they informed us that there was an active policy that the railway should remain open. We concluded that there would be no major expansion of the use of ticket barriers in the absence of an intervention by the EU, although more barriers might be installed for commercial reasons as networks develop.

4.80 Stakeholders confirmed that clustering of passengers before a process can create a target, and mentioned queues at the screening of Thalys passengers at Paris Gare du Nord. However, they also pointed out that holding passengers back might only move the point of vulnerability. We

concluded that there would be no material new measures to introduce queueing systems in the absence of an intervention by the EU.

4.81 None of the stakeholders mentioned any proposals to extend the screening of either passengers or baggage (whether when left in a luggage office or taken onto a train). Given the cost to the industry, and inconvenience to passengers, of these interventions, we concluded that there would be no change in their application in the absence of an intervention by the EU.

4.82 In principle, Member States might take measures to increase segregation of high-speed and international rail services from other services, as is already the case on Eurostar and has been implemented to a limited degree on Thalys, the Spanish AVE network, and the Öresund network for travel into Sweden. However, none of the stakeholders reported any proposals to increase segregation and they frequently indicated that it would be impracticable or at least extremely costly to do so. We concluded that there will be no material increase in segregation, including in the construction of new high-speed lines[40].

Interventions in assets and equipment design – monitoring technology and IT equipment

4.83 Facial recognition technology is maturing and is, for example, now being used to identify passengers at a growing number of airports, and SNCF informed us of its in-house research on the technology. We envisage that it will become a standard software feature of CCTV technology over the next 10-15 years, although we would also expect that it would be disabled where this was considered necessary to comply with local laws on, or expectations of, privacy. In principle, behavioural recognition technology may also emerge, but stakeholders did not report any specific initiatives or programmes to introduce it.

4.84 Most stakeholders told us that their IT systems were sufficiently robust to withstand normal outages, including cyber-attacks, but there may be insufficient local duplication to ensure that systems remain robust around, for example, the site of an explosion. We concluded that this situation would continue in the absence of an intervention by the EU.

Interventions in assets and equipment design – station design

4.85 Stakeholders did not mention any initiatives to improve station security and, given the combination of limited financial resources and long-lived station assets, we concluded that it was unlikely that further interventions would be adopted in the absence of an intervention by the EU. In any event, we would expect major changes to security at stations, for example to eliminate unseen areas, to occur only when new stations were built or existing ones were upgraded[41]. Given the usable life of many station facilities, however, we would expect existing stations to be replaced only over a period of 50-100 years, if at all[42].

---

[40] For example, Great Britain's High Speed 2 will have dedicated platforms for high-speed services at some stations, but at many stations high-speed trains will share platforms with other services. In addition, High Speed 2 is not expected to come into operation before 2026.

[41] For example, the £220 million project to enhance Cardiff Central Station in Great Britain includes, among other safety and security features, 300 square metres of glazed blast-resistant façade system.

[42] In practice, older railway stations in some Member States are now protected as architectural heritage, such as over 100 Grade II listed stations in the United Kingdom. Any legislation to require security interventions would need to consider whether such protection should be overruled.

4.86 Vehicles have been used in previous attacks on rail services, to carry an explosive device or to travel to and enter stations and other locations. However, we only identified one systematic programme to protect against vehicle intrusion, in the UK, and we assume that no material new measures would be introduced in the absence of an intervention by the EU.

4.87 We envisage that some improvements to emergency egress from stations will emerge, either to handle larger passenger flows or to comply with national safety legislation, and that this will also provide a security benefit. We have not, however, found any means of quantifying or forecasting the effect.

Interventions in assets and equipment design – rolling stock design

4.88 By contrast, we expect that some improvements in rolling stock will come about, over time, through a number of mechanisms:

- the requirements of Technical Specifications for Interoperability (TSIs), although no stakeholder suggested that these were likely to include measures such as blast-proofing;
- technological improvements, reducing the cost of fitting systems such a CCTV and the associated image transmission, storage and analysis systems;
- competitive pressures of manufacturers to offer new features, including those which contribute to security; and
- competitions to provide PSO services, leading competent authorities to specify more features and/or bidders to offer them.

Asset management

4.89 UIC has carried out work in the field of asset management including, in 2010, the publication of asset management guidelines. These discussed an asset management strategy including the use of asset registers. With such work by a pan-European body, we envisage that asset registers will become more consistent in their treatment of security issues, but that in the absence of an intervention this process will be slow.

Staff and training

4.90 Stakeholders expressed strong support for training in risk and behaviour monitoring to improve security. Some commented that police and specialist security staff, such as DB Sicherheit, are trained in behavioural monitoring to a high level, and that this can be very effective, but that such staff can only be deployed on a relatively limited basis. We concluded that training and deployment of such staff would continue to improve in the absence of an intervention by the EU, but that this would be incremental and variable across Member States.

4.91 Stakeholders also consistently reported that the industry's procedures for responding to a terrorist incident are normally the same as those applied to accidents and other types of incidents. As we set out above (paragraph 3.4), the passengers and rail staff who are first on the scene of an incident such as a derailment or an explosion may have no means of knowing its cause. We would therefore expect responsiveness to all kinds of incidents, including security failures, to improve over time. We have, however, identified no means of quantifying or forecasting this effect.

4.92 Stakeholders mentioned the need to consider the "insider threat", which can operate at a number of different levels. However, one interviewee reported a concern that vetting is becoming less relevant to the prevention of terrorism, given the speed with which radicalisation can take place (See Appendix D, **Error! Reference source not found.**). It may be

necessary to develop a culture in which staff are able raise concerns about fellow colleagues, perhaps through confidential reporting arrangements. We concluded that there would be no material change in the extent of staff vetting in the absence of an intervention by the EU.

4.93 Staff vetting is closely related to access control arrangements and identity checks. Stakeholders referred to the importance of having clear methods of staff identification and of ensuring that subcontractors or traders participate. However, we were not informed of any proposals to introduce new access controls, which we envisage will remain unchanged in the absence of an intervention by the EU.

4.94 We would expect that staff deployment will continue to be arranged such that members of staff can effectively patrol and monitor activity as part of their duties. This role is consistent with other business needs and does not necessarily represent an additional cost, especially for staff who would otherwise have periods of inactivity. We concluded that there would be no material change in the absence of an intervention by the EU.

Risk assessment

4.95 The establishment of LANDSEC provides a forum for exchange of information between rail and other transport service providers, and we would expect it to enable better dissemination of best practice. Other fora such as the United Nations Economic Commission for Europe (UNECE) and pan-European representative bodies such as CER, EIM and UIC are also likely to contribute to better information exchange, particularly if the threat of violent attacks is perceived to have increased significantly. We would therefore expect the understanding of the threat of both violent and non-violent crime among stakeholders to improve to some degree, even in the absence of further intervention by the EU.

4.96 However, progress towards adopting a common, best practice approach to risk assessment is likely to be particularly slow. The stakeholder engagement revealed a wide range of approaches, and in several cases there was no assessment specific to the rail sector itself, much less to particular types of rail service. In some Member States we saw little evidence of a focused effort to improve, although fora such as LANDSEC provide a means for the necessary exchange of information and learning. We found no evidence of a concerted effort among Member States with less developed approaches to risk assessment to learn from others and to adopt best practice.

Threat level protocols

4.97 The use of categories of threat level is employed in most, but not all, Member States to indicate the prevailing level of risk of an attack. What varies between Member States, and potentially between locations within them, is:

- whether the prevailing level is known to those outside the “security community”;
- whether there has been significant experience of the level being changed; and
- whether there is any defined and known linkage between the threat level and activity by rail actors: in many cases this will not be predefined in railway procedures, but will be advised in detail by the police or security agencies at the time that the level changes.

4.98 Ideally, security activities can be cut back when threat levels fall, thereby improving the cost effectiveness of security arrangements. One concern noted during consultation was that if the threat level is raised in response to a specific event, it can be difficult to achieve early agreement to the level being reduced again.

4.99 Stakeholders did not mention any initiatives to extend the dissemination of threat levels to the rail industry, and we concluded that there would be no material change in the absence of an intervention by the EU. This would also mean that, in the absence of an intervention by the EU:

- There will continue to be a diversity of nomenclature of threat levels, of the extent to which they are disseminated to the industry, and of the protocols for responding to each threat level.
- There will continue to be a lack of coordination between neighbouring Member States to deal with the fact that prevailing threat levels will differ between them.

Contingency planning

4.100 The term "contingency plan" is used by different parties, and in different contexts, to convey differing meanings. The Fourth Railway Package proposals, for example, use the term with respect to the reorganisation of the timetable following perturbation. For this study we interpret contingency planning as meaning all aspect to the response to incidents. Stakeholders indicated that contingency planning has a significant role to play in:

- dealing with specific threats and suspicious incidents;
- dealing with the immediate impact of an attack; and
- seeking to restore operations following an attack.

4.101 Even railways that do not see a requirement to plan specifically for recovery from security incidents will prepare for responding to other types of incidents. This is not only a matter of having contingency plans but of more fundamental considerations such as ensuring that alternative routes and facilities are available to resume operations in the face of a major outage. However, stakeholders did not identify any need for, or benefits of, a coordinated European approach. We conclude that "contingency plans" are unlikely to become standardised in the absence of intervention by the EU.

Drills and exercises

4.102 Stakeholders confirmed that contingency plans need to be supported by exercises to test their effectiveness and to ensure that staff gain experience of responding to a security threat or incident in a simulated environment. They also confirmed that such exercises play a particularly important in testing the effectiveness of interfaces between multiple agencies and ensuring that their respective plans are consistent. Their responses suggested that this principle is embedded in the rail sector, although there is wide variation in the extent to which exercises are held. Infrequent exercises held jointly by various agencies might help to highlight major differences of approach, but could not embed the required thinking in the minds of the staff likely to find themselves in the front line at the time of an incident.

4.103 In a number of Member States we were told that there is scope for the number of exercises of all types to be increased significantly and for ensuring that terrorism is the subject of the some scenarios. One stakeholder stated that it deliberately uses the term "drill" rather than "exercise" to emphasise that this activity forms a part of "business as usual". However, we saw no evidence that the use of drills and exercises would increase in the absence of an intervention by the EU.

Post-incident recovery

4.104 Post-incident recovery is concerned with returning to near-to-normal operations as quickly as possible after an event, whether an accident, attack or false alarm. In each case, the aim is to ensure continued availability of rail services and to reduce any tendency of users to change to other modes.

4.105 One interviewee stated that some Member States or competent authorities might prioritise commuter and/or PSO services, which often handle large volumes of passengers, and that some high-speed and international services, often seen as purely commercial services, would not be a priority for operation. We note, for example:

- While disruption to high-profile services such as Eurostar is newsworthy, it affects far fewer passengers than the commuter services, normally specified in PSOs, in the three capitals (London, Paris and Brussels) that it serves.
- The withdrawal of the Fyra train fleet resulted in a sustained reduction in the interurban service between Amsterdam and Brussels, but did not materially affect commuting to and within those cities.

4.106 In practice, Member States take similar approaches to recovering from other types of incident. For example, it may be possible to identify diversionary routes, and alternative timetables that make use of them, and to ensure that drivers and train crew maintain familiarity with them. However, while this may be possible for relatively minor accidents, attacks or false alarms, major damage to infrastructure may require a sustained period of operation of a timetable tailored to the infrastructure which can still safely be used. In these circumstances it would be difficult to have a tailored and comprehensive contingency plan in place in advance: this would instead require an intense period of planning by a specialist team.

4.107 In the absence of EU intervention, it appears likely that Member States will continue to adopt different approaches to mitigation. However, the scope for harmonisation of approaches will in any case be limited by the need for recovery measures to reflect local infrastructure, operations and culture.

Procedures and systems

4.108 Various interventions are already in place to identify passengers, although not always with an objective of security:

- Some operators require passengers to produce a unique object, such as a credit card or identity document, to prevent abuse of print-at-home tickets.
- Eurostar has banned cash purchase of tickets for immediate travel between Brussels and Lille.
- Sweden has imposed a requirement for identity checks on passengers entering Sweden by train. The arrangement is achieved by making railway undertakings responsible for ensuring that passengers have the right to enter Sweden, and the railway undertakings in turn making production of valid identity documents a condition of carriage.

4.109 Such arrangements do not exist at present but the aviation sector is leading the way in this regard following the European Parliament's adoption of the EU Passenger Name Record (PNR)

Directive in April 2016[43]. Eurostar informed us that it had actively lobbied for Passenger Name Record (PNR) data to be gathered in the rail sector, although it stated that a key objective was to establish a passenger manifest that could be used following an incident. We note, however, that identity checks require data exchange, which can be difficult to achieve given the sensitivity of data held by national security agencies. We concluded that an increasing proportion of passenger will be expected and willing to identify themselves on a voluntary basis to support the use of print-at-home tickets, but that Member States will be reluctant to make identification compulsory.

4.110 Desk research and stakeholder consultation identified some programmes of awareness promotion, particularly in relation to issues such as pickpockets (where the security issue is theft), unattended baggage (where the security issues are theft and potential bombs), and suspicious behaviour. In some cases, dedicated telephone numbers are available to make reports. We envisage that there will be a general increase in the extent, and effectiveness, of awareness promotion programmes, although their impact is hard to predict.

4.111 Stakeholders did not mention any programmes to increase storage of contingency reserves, and we assume that there would be no change in the absence of EU intervention.

Evolution of security failures and their impacts

4.112 Based on this review of possible security interventions, we have not identified any material trends likely to drive either the number of security failures or their impacts in a particular direction. Neither have we identified any independent forecasts of the frequency or cost of such incidents. We also note that any improvements in security, for example in the form of deployment of new technology, could eventually be matched by increased capability to overcome them on the part of would-be perpetrators of crime. While it is not possible to observe such an effect explicitly in historical data, the proposition that crime prevention and detection techniques and the ability of perpetrators to overcome them move together over the long term is well documented.

4.113 By way of example, in a recent report[44], the United Nations Congress on Crime Prevention and Criminal Justice noted the following:

"The speed of technological advancement, increasing globalization, and the exponential growth of global markets have created opportunities for criminal activities, often with a low risk of detection and using new forms of anonymity. Preventing and combating new and emerging crimes is a challenging task. Crime is continually evolving and adapting…"

4.114 Similarly, McQuade (2006) notes that "crime, policing and security are enabled by and co-evolve with technologies that make them possible"[45], while Gunasekaran (2007) has

[43] The proposed Directive would only apply to airlines, and Denmark is not participating. See http://www.consilium.europa.eu/en/press/press-releases/2016/04/21-council-adopts-eu-pnr-directive/

[44] New and Emerging Forms of Crime: Threats The World Must Reckon With, United Nations Congress on Crime Prevention and Criminal Justice, 2015.

[45] Technology-enabled Crime, Policing and Security, Sam McQuade, 2006

concluded that "as fast as new technology is being implemented to stop thieves, thieves are finding ways to get around this new technology"[46].

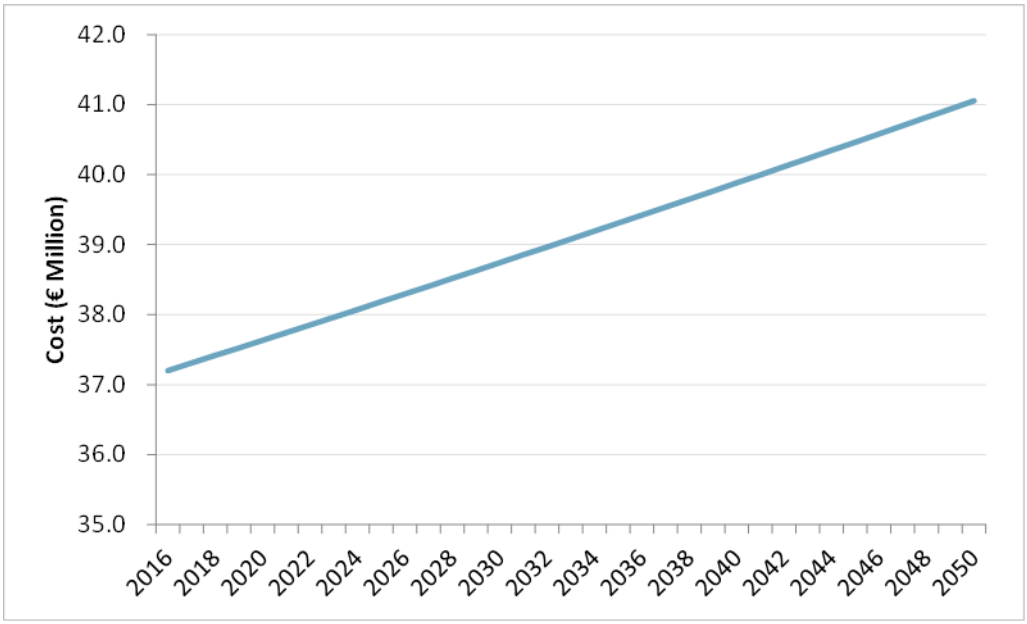
4.115 Against this background, we have developed the baseline on the assumption that the underlying security threat and level of security failures remains constant over the timescale of the impact assessment (from 2016 to 2050, the time horizon for the transport forecasts provided by the PRIMES-TREMOVE transport model). More specifically, our projection of the costs of security failures in the baseline is based on the following methodology:

- We have taken the estimates of the cost of security failures on international and high speed rail services, as indicated in Table 4.2, as 2016 starting values. These include an estimate of the impact of terrorist incidents, based on a review of such incidents over the past 40 years (similar to the timescale for the impact assessment). They also include separate estimates of the annual impact of vandalism (reflecting the cost of repairing and replacing damaged assets) and metal and cable theft (reflecting both the cost of replacement and the cost of disruption to train services).
- In line with standard cost benefit analysis, we have assumed that the value of the impact of terrorist attacks will increase in proportion to the value of Gross Domestic Product per capita (GDP per capita). This is because the impact includes fatalities and injuries as well as service disruption and reduction in travel, all of which are valued by reference to the value to the economy of passengers affected (and of the productive time lost when their travel is disrupted). The OECD provides long term forecasts of GDP for the Euro area, and these have been combined with population forecasts from the PRIMES-TREMOVE model to generate forecasts of GDP per capita with which to inflate cost values to 2050.
- Similarly, we have assumed that the value of the impact of metal and cable theft increases with GDP as such crime often leads to service disruption (for example, as a result of associated signal failure).
- In the case of vandalism, including graffiti, we have assumed that the value of the impact remains constant in real terms over the timescale of the impact assessment. This is because the value is determined largely by the cost of repair and replacement and does not generally reduce the productive potential of the economy by causing casualties or service disruption (although we are aware of cases involving cancellation of train services following withdrawal of trains covered in graffiti, much of the vandalism observed on train networks does not interfere with the operation of the service).

4.116 The baseline cost of security failures derived using this methodology is shown in the figure below.

[46] Modelling and Analysis of Enterprise Information Systems, Angappa Gunasekaran, 2007.

Figure 4.3: Baseline cost of security failures



Source: Steer Davies Gleave analysis based on estimated of cost of security failures in Table 4.2 and OECD long term forecasts of GDP for the Euro area

4.117 Note that the projection shown represents the direct impact of security failures, and does not include the impact of perceptions of security on the demand for rail travel. This is discussed in the following section.

Evolution of the security threat and passenger demand

4.118 Perceptions of the security threat to international and high speed services affect the demand for travel on these services independently of the impact of any particular security failure, although perceptions will themselves be influenced by the number and scale of incidents observed. We have not identified any direct, pan-European measures of passenger perceptions of security. However, as discussed in paragraphs 4.24 to 4.33, some Member States define and disseminate threat levels, although there is no consistent approach to measuring them across Europe. For the purposes of modelling impacts, we have used the threat levels defined by the UK Foreign Office, as shown in Figure 3.3, which provide for a systematic grading of security threats and an assessment of the current level of threat in different Member States. In the absence of any independent forecasts of how these might evolve (which would involve forecasting the likely level of terrorist attacks and other forms of crime over an extended period), we have assumed that current threat levels will remain constant over the period of the impact assessment in the baseline.

4.119 The table below reproduces the UK Foreign Office threat levels and shows their assessment of the current threat in different Member States. Note that, for the purposes of modelling, we have converted the levels defined into a 10-point scale. This allows for greater differentiation in the modelling of impacts under different options. For example, it allows for the possibility that a given improvement in security will reduce the threat level from, say, 'underlying threat' to a point midway between 'underlying' and 'low threat'. We consider that the use of a four- or five-point scale would constrain the analysis unduly, since not all possible interventions could be expected to achieve a movement from one of the Foreign Office's defined levels to another.

Table 4.11: Threat levels in the baseline

UK Foreign Office threat level	Scale used in modelling	Member States experiencing indicated threat level
	1	
Low threat	2	Czech Republic, Estonia, Finland, Hungary, Latvia, Lithuania, Poland, Slovenia
	3	
Underlying threat	4	Bulgaria, Croatia, Ireland, Luxembourg, Portugal, Romania, Slovak Republic
	5	
General threat	6	Austria, Denmark, Sweden, Greece, Italy, Netherlands
	7	
High threat	8	Belgium, France, Germany, Spain, UK
	9	
State of emergency	10	

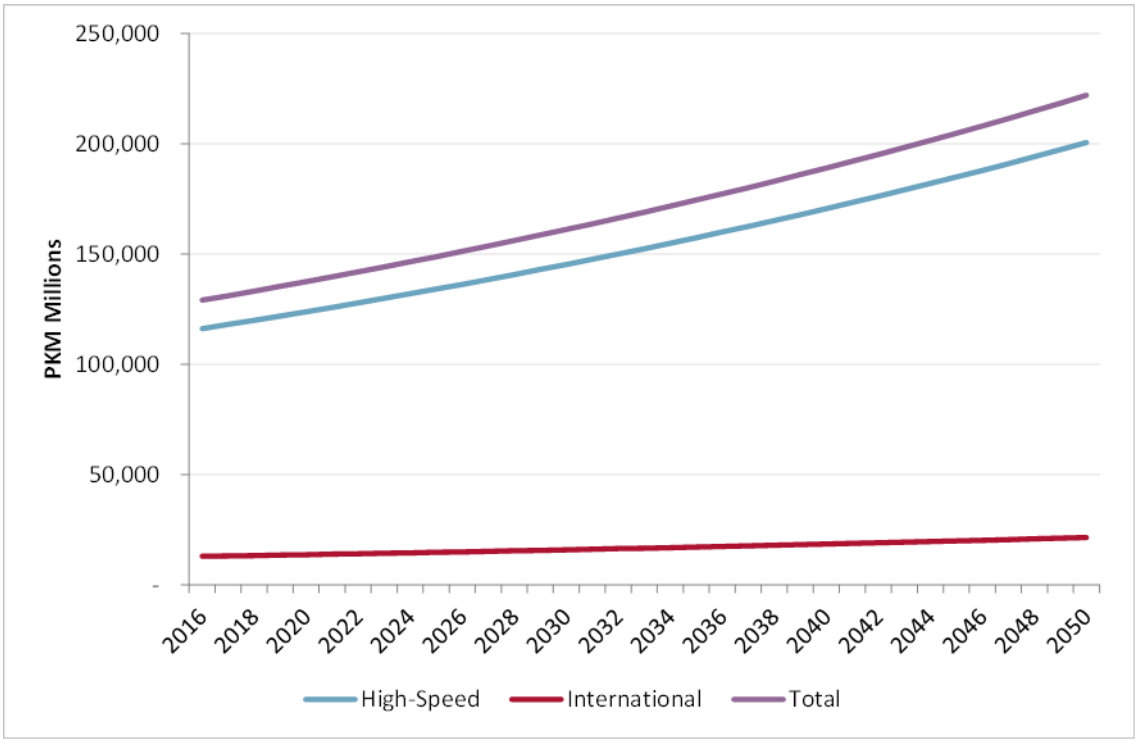
Source: Steer Davies Gleave assessment based on UK Foreign Office information and stakeholder consultation responses

4.120 We have assumed that the persistence of these threat levels over the period to 2050 is consistent with the passenger demand forecasts provided by the PRIMES-TREMOVE transport model and set out in the 2016 EU Reference Scenario[47], and used the growth rates underpinning these forecasts to generate demand profiles for both high speed and international services. The starting year value for high speed service demand, measured in passenger kilometres, was also taken from the 2016 EU Reference Scenario. In the case of international services the equivalent value was derived by adjusting the Eurostat estimate of international rail passenger kilometres to take account of double counting. More specifically, we reduced the value by the estimated proportion of international passengers travelling on high speed services shown in Table 2.7.

4.121 The resulting baseline demand profiles are shown in the figure below. These have been combined with EEA forecasts of CO2 emissions per passenger and estimates of future carbon costs taken from the 2016 EU Reference Scenario to derive a monetised value of environmental impacts for the baseline.

[47] EU Reference Scenario 2016: Energy, transport and GHG emissions trends to 2050, European Commission July 2015.

Figure 4.4: Profile of demand for high speed and international services (passenger kilometres)



Source: Steer Davies Gleave analysis based on

4.122 Our methodology for assessing the incremental impacts of policy options, relative to this baseline scenario, is described in Section 9.

5 Defining objectives for intervention

Introduction

5.1 In principle, the most important change in behaviour required to address the problem described in Section 4 is a reduction in the willingness of individuals to undertake rail-related crime of all kinds. Understanding the motivation for such behaviour, and the means for changing it, is beyond the scope of this study, since it would involve comprehensive investigation of the causes of violent and anti-social behaviour more generally. As we noted in paragraph 1.20, in this study it was not practicable for consultation to include stakeholders who cause security issues.

5.2 However, it is within the scope of our work to consider how potential perpetrators might be discouraged from targeting rail networks in general and high-speed and international rail services in particular. While there is clearly some risk that this will lead to a displacement of crime to conventional rail networks or even to other sectors, a risk that underlines the need for a holistic approach to security, this does not remove the need for a sector-specific assessment of the problem.

5.3 Against this background, and in line with the Better Regulation Guidelines and Better Regulation Toolbox (in particular, Tool #13), we developed a number of objectives to guide the design of potential rail security policy interventions. The objectives link the analysis of the problem definition to the options for policy response. In this section, we define a general objective and a number of specific objectives and explain how they relate to the problem drivers identified in the previous section. In Chapters 6, 7 and 8, we describe security interventions, policy measures and policy options which might address these objectives.

General objective

5.4 The general objective is intended to address the overarching problem, the threat of attacks on high-speed and international rail services and infrastructure and broader potential for other damage to, or loss of, assets used to provide such services. However, given the difficulties of segregating these services (see 4.69), we suggest that the general objective can be drawn more broadly, as follows:

> "To reduce the risk and impact of criminal acts on the European rail network"

5.5 Note that:

- there is no distinction here between high-speed and international rail services and all other types of services, reflecting the fact that even when measures are directed towards particular services, they are likely to have the effect of making the other parts of the network more secure; and
- the objective is to reduce both the likelihood and the impact of attacks.

5.6 Note that, while services other than high-speed and international rail services are outside the scope of this study, this objective could in principle apply to all rail services.

Specific objectives

5.7 Tool #13 says of specific objectives:

"*These set out concretely what the policy intervention is meant to achieve. They should be broad enough to allow consideration of all relevant policy alternatives without prejudging a particular solution.*"

5.8 Accordingly, and to the extent possible:

- We developed a set of specific objectives mapped to key elements of problem tree, ensuring that any potential package of intervention measures covers the problem in its entirety.
- We excluded cultural factors as these are not specific to the rail industry and cannot be addressed through rail-specific policy intervention.
- We developed specific objectives with the aim of satisfying the SMART (Specific, Measurable, Achievable, Realistic and Time-dependent) criteria identified in Tool #13, taking into account the need to support the general objective; the dependence of their achievement on the smooth functioning of the EU railway market rather than on other (external) causes; and their quantification and monitoring.
- We sought, in defining each objective, to take account of the fact that decision-making within the rail industry, as in many industries, takes place in a complex environment in which issues of safety, security, feasibility, costs and benefits must be balanced.

5.9 The specific objectives are set out in Table 5.1 below. We stress that these objectives are not fixed points, achievement of which would eliminate security problems. However, implementing further security interventions, policy measures and policy options consistent with these specific objectives will tend to reduce further the scale of the problem defined in Chapter 4.

Table 5.1: Rationale for specific objectives

Problem drivers (See Figure 4.2)	Specific objective	Rationale/comment
Insufficient understanding of the threat	**Shared EU understanding** Ensure relevant stakeholders have a more thorough and shared understanding of the security threat across the EU.	While the problem is partly the result of underlying data limitations, more could be done to ensure that rail industry and other stakeholders across the EU share a better understanding of the threat.
Inadequate response to the threat	**Reflect EU-wide benefits** Ensure that the response to the threat adopted by the industry takes full account of the economic and social benefits of security interventions across the EU.	There is a need to address externalities, in the form of security benefits that are not taken into account in commercial decision-making. At the same time, the economic and social benefits of security interventions need to be fully considered by public sector decision-makers determining investment priorities.
Different approaches to mitigation in Member States	**Consistent risk assessment** Ensure that mitigation of the security threat in different Member States is based on a consistent assessment of underlying risks.	While the specific security interventions adopted in different Member States will vary according to circumstances, it is important that common risks are assessed using the best methodologies available to the industry.
Fragmentation and gaps in security coordination	**Holistic and coordinated approach** Ensure that the security threat to high-speed and international rail services is addressed in a holistic and coordinated manner.	Mitigation measures should be applied consistently and coherently to an entire service or group of services, so that measures employed on one part of a journey cannot be circumvented or undermined by perpetrator actions taken on another part.

Source: Steer Davies Gleave analysis

6 Potential security interventions

Introduction

6.1 In consultation with the Commission we developed a three-stage approach to developing options capable of contributing to some or all of the specific objectives set out in Table 5.1:

- First, as described in this Chapter, we identified a number of practical **security interventions**, including a number listed in the Terms of Reference, and sifted them to identify security interventions to be retained for further consideration.
- Second, as described in Chapter 7, we identified how these retained security interventions could be grouped into a number of **policy measures**.
- Third, as described in Chapter 8, we identified how these policy measures could be applied, singly or in combination, as **policy options** to address the four specific objectives.

6.2 We stress at the outset that the nature of the security issue, the problem drivers, and the specific objectives, means that policy options are not mutually exclusive. In particular, no single measure, except closure of all high-speed and international rail services, could eliminate all theft, vandalism, graffiti, crime and terrorism associated with them. This means that:

- Any one specific objective might best be addressed by a number of policy measures.
- Any one policy measure might contribute to addressing a number of specific objectives.

6.3 We discuss this issue further in Chapter 8, but begin this chapter by discussing possible security interventions.

Long-list of potential security interventions

6.4 The Terms of Reference required us to examine a number of security interventions, which we summarise in Table 6.1 below.

6.5 We also identified, in Table 3.2, a range of other security interventions used in other industries or mentioned in literature or by stakeholders. Table 6.2 groups the resulting long list of 30 potential security interventions into five groups: communications and external liaison; assets and equipment design; staff and training; risk assessment and planning; and procedures and systems.

6.6 We note again that these security interventions, whether proposed in the Terms of Reference or by us, are not mutually exclusives, and could in principle all be adopted, although we would expect in practice that there would be some interactions and interdependencies between them.

Table 6.1: Potential security interventions specified in Terms of Reference

Description in Terms of Reference (Some text is abbreviated slightly to fit)	Steer Davies Gleave interpretation and description	Number (Table 6.8)
RUs and IM to have action plans to adjust according to the level of threat, as defined by the national authorities	Threat level protocols	1
RUs and IMs to have contingency plans for responding to security incidents (including drills and exercises, liaison plans with emergency services, and post-incident recovery plans	Contingency plans	2
	Drills and exercises	3
	Liaison with emergency services	4
	Post-incident recovery plans	5
RUs and IMs to have minimum security training requirements for persons working in the railway environment (trains and stations)	Training in risk and behaviour monitoring	6
	Training in incident response	7
Standards for security design features on railway carriages (e.g. making carriages more blast-resistant through design)	Blast resistant stations and trains	8
Nominative ticketing for all cross-border and high-speed trains	Nominative ticketing	9
Use of CCTV equipment on stations and on trains	Static detection equipment (CCTV)	10
Minimum standards for equipment, and common rules on their use when deployed on cross-border and high-speed trains	This is considered as policy measures 2D and 4B in Chapter 7.	
Installation of security equipment at railway stations, in order that it can be used when required	This is considered as policy measures 2A, 2C and 4A in Chapter 7.	

Source: Terms of Reference, RU = Railway Undertaking, IM = Infrastructure Manager

Sifting of potential security interventions

6.7 We sifted the long list of potential security interventions listed in Table 6.3 against a number of criteria summarised below. In our sift we also took into account the estimated scale of the security problem, set out in Table 4.2 and repeated below as Table 6.4, and the need for proportionality in relation to the small estimated annual average cost of terrorism.

Table 6.2: Summary of estimates of the cost of security failures on rail services

Security failure	Average annual cost on rail services		Potential scale of a single incident
	All services	High-speed and international	
Metal and cable theft	€30 million	€7 million	
Vandalism and graffiti	€280 million	€30 million	
Other non-violent crime	No estimates found, but may be very large		
Terrorism	€20 million	€0.2 million	Up to €500 million
Other violent crime	No estimates found, but may be very large		
Total identified	**€330 million**	**€37.2 million**	
Passenger numbers	**9,200 million**	**300 million**	
Identified cost per passenger	3.5¢	12.4¢	
Terrorism cost per passenger	0.2¢	0.07¢	

Source: Steer Davies Gleave analysis, see text. Terrorism cost is based on European Commission Secure Station. Passenger numbers are from Table 2.3 (international plus high-speed >210 km/h).

Table 6.3: Potential security interventions identified in research: long list

Intervention Notes: ● = primary objective addressed + = secondary objective addressed		Terms of Reference	Potential scope			May address objectives?			
			Infrastructure	Stations	Trains	Shared EU understanding	Reflect EU-wide benefits	Consistent risk assessment	Coordinated approach
Communications and external liaison									
EL1	Partnerships with third parties							●	+
EL2	Liaison with emergency services	4	●	●	●			●	+
EL3	Liaison with security experts in other fields								
Assets and equipment design									
EA8	Station queuing systems		●						
EA11	Mobile detection equipment (drones)		●						
EA12	Passenger and baggage screening equipment		●						
EA13	Station ticket barriers		●						
EA6	Recording of vulnerabilities in asset register		●	●		+		●	
EA7	Road vehicle intrusion protection		●	●					
EA4	Station duplicate access routes and walkways			●			●		
EA3	Facilitation of emergency egress at stations			●	●		●		
EA1	Blast-resistant stations and trains	8		●	●		●		
EA2	Minimisation of unseen areas			●	●				●
EA5	Blast-resistant luggage storage areas			●	●				
EA9	Facial or behaviour recognition technology			●	●				●
EA10	Static detection equipment (CCTV)	10		●	●				
EA14	Resistant radio and communications systems		●		●			●	+
EA15	Contingency IT and communications systems		●		●			●	+
Staff and training									
SR1	Training in risk and behaviour monitoring	6	●	●					●
SR2	Training in incident response	7	●	●				●	+
SR3	Staff vetting		●	●	●	●			●
SR4	Staff physical screening		●	●	●				
SR5	Staff deployment		●	●	●				●
Risk assessment and planning									
RP1	Threat level protocols	1				●		●	+
RP2	Contingency planning	2	●	●	●			●	+
RP3	Drills and exercises	3	●	●	●			●	+
RP4	Post-incident recovery	5	●	●	●			●	+
Procedures and systems									
PS1	Identity checks and/or nominative ticketing	9	●						
PS2	Awareness promotion among passengers		●						●
PS3	Targeted storage of contingency reserves		●	●				●	+
PS4	Inspection regimes		●	●	●			●	

Impact on passengers

6.8 First, we estimated the likely impact of a policy intervention on passengers, focusing on whether it would delay their journey. In practice:

- Security interventions such as passenger screening would delay all passengers.
- Security interventions such as drills and exercise might cause minor disruption to passengers who were inconvenienced when they took place.
- Security interventions such as staff vetting would have no effect on passengers.

Table 6.4: Scale for assessing impact on passengers

Red	Orange	Yellow	Light green	Green
●	●	●	●	●
The intervention would impose delay all, or many, passengers		The intervention would impose minor delay on a few passengers		The intervention would impose no delay on passengers

Evidence of proven technology

6.9 Second, we identified the extent to which the proposed security intervention is a proven technology in an environment of high-speed and international trains.

Table 6.5: Scale for assessing evidence of proven technology

Red	Orange	Yellow	Light green	Green
●	●	●	●	●
Not yet proven or not proven on rail	Rarely used on rail	Use on rail varies or is mixed	Some use on rail	Common or rail, well-proven

6.10 At one extreme, for example, use of mobile detection equipment such as drones is not yet proven technology, particularly in close proximity to a working railway.

Stakeholder views

6.11 Third, we summarised the views of stakeholders who had commented on a particular security intervention, a range from strongly negative to strongly positive. Where stakeholders expressed a wide range of views, we assessed them as neutral or mixed.

Table 6.6: Scale for assessing stakeholder views

Red	Orange	Yellow	Light green	Green
●	●	●	●	●
Strongly negative	Slightly negative	Neutral or mixed	Slightly positive	Strongly positive

Cost and time to implement

6.12 Fourth, we included our own indicative estimates of the likely time, and capital and operating cost, required to implement different security interventions. We stress that our estimates can only be indicative, given the uncertainties both in the volume of stations, trains and infrastructure at which interventions would be applied (see Chapter 2) and the extent of activity which would be required at each of them.

Table 6.7: Scale for estimating cost and time to implement

	€	€€	€€€	€€€€
Capital cost/time			Over € 1 billion	Over €10 billion
Operating cost per year	Over €1 million	Over €10 million	Over €100 million	Over €1 billion

6.13 For example, if capital works were required at each of the estimate of 1,000 stations served by international trains in Table 2.3, a programme which might take many years to complete:

- Capital expenditure of €1 million per station would cost €1 billion. This might be sufficient for interventions such as installing ticket barriers and fencing to limit access to platforms.
- Capital expenditure of €10 million per station would cost €10 billion.

6.14 Similarly, operating expenditure such as passenger and baggage screening might require an average of five full-time equivalents during opening hours, or 25-30 employees, at an indicative cost of €50,000 per employee. This might mean average annual costs of over €1 million per station or €1 billion for all stations served by international trains[48]. In the context of the estimated cost of terrorism shown in Table 6.2, it would be for policymakers to decide whether expenditure on this scale would be considered proportionate.

6.15 We sifted potential security interventions against each of these criteria in turn, rejecting any intervention for which impact on passengers was assessed as high or evidence of proven technology was absent. We also rejected four further interventions:

- Mobile detection equipment (drones) is being used on some railways, on a limited basis and for various purposes. However, there is as yet no agreement on what role drones should perform or how standards should be defined. We saw little or no scope for defining standards for their role and use until more consistency has emerged on where and how they should be used.
- Liaison with security experts in other fields would in practice require individual industry bodies or individuals to identify relevant other fields and experts. Some Member States are landlocked and may have few or no experts on maritime safety, and smaller Member States have a single airport and may have no dedicated expertise in aviation safety. We saw little of no scope for defining a requirement for such liaison in legislation or guidelines.
- Systematic physical screening of staff appears impracticable at stations with no gated or secure areas, or one or few staff members. It would imply full-time security staff to let part-time railway staff enter an open station, such as at Ulrichsbrücke-Füssen (see Figure 2.2).
- Systematic road vehicle intrusion projection appears impracticable as it would also potentially require the construction of thousands of kilometres of crash-proof barriers, including at locations such as Ulrichsbrücke-Füssen (see Figure 2.2).

6.16 The results of our sift are summarised in Table 6.8.

[48] We were told that baggage screening at one platform can cost €2.5 million per annum, see 6.36.

Table 6.8: Potential security interventions identified in research: sifting

Intervention		Impact on passengers	Proven in use, ideally on railways	Stakeholder views	Cost and time to implement	Result of sift
Key to symbols		Table 6.4	Table 6.5	Table 6.6	Table 6.7	
EA5	Blast-resistant luggage storage areas	🔴	🔴	🔴	€€€€	Fail
EA13	Station ticket barriers	🔴	🟠	🔴	€€€€	Fail
EA12	Passenger and baggage screening equipment	🔴	🟠	🔴	€€€€	Fail
EA8	Station queuing systems	🔴	🟠	🔴	€€€	Fail
PS1	Identity checks and/or nominative ticketing	🔴	🟠	🔴	€€€€	Fail
EA11	Mobile detection equipment (drones)	🟡	🔴	🟡	€€	Fail
EL3	Liaison with security experts in other fields	🟢	🟡	🔴	€	Fail
SR4	Staff physical screening	🟢	🟠	🟡	~~€€€€~~	Fail
EA7	Road vehicle intrusion protection	🟡	🟠	🟡	~~€€€€~~	Fail
PS2	Awareness promotion among passengers	🟡	🟡	🟢	€	Pass
RP3	Drills and exercises	🟡	🟢	🟢	€	Pass
EA9	Facial and behaviour recognition technology	🟡	🟠	🟡	€€€	Pass
EA10	Static detection equipment	🟡	🟡	🟡	€€€	Pass
EA4	Station duplicate access routes and walkways	🟢	🟠	🟡	€€€€	Pass
EA3	Facilitation of emergency egress at stations	🟢	🟠	🟡	€€€€	Pass
EA1	Blast-resistant stations and trains	🟢	🟠	🟡	€€€€	Pass
SR3	Staff vetting	🟢	🟠	🟡	€€	Pass
EA2	Minimisation of unseen areas	🟢	🟠	🟡	€€€	Pass
EA14	Resistant radio and communications systems	🟢	🟡	🟡	€€€	Pass
EA15	Contingency IT and communications systems	🟢	🟡	🟡	€€€	Pass
SR5	Staff deployment	🟢	🟡	🟡	€€	Pass
EA6	Recording of vulnerabilities in asset register	🟢	🟡	🟡	€	Pass
PS3	Targeted storage of contingency reserves	🟢	🟡	🟡	€	Pass
PS4	Inspection regimes	🟢	🟡	🟡	€	Pass
SR1	Training in risk and behaviour monitoring	🟢	🟡	🟢	€	Pass
RP1	Threat level protocols	🟢	🟢	🟢	€	Pass
EL1	Partnerships with third parties	🟢	🟢	🟡	€	Pass
SR2	Training in incident response	🟢	🟢	🟡	€	Pass
RP4	Post-incident recovery	🟢	🟢	🟡	€	Pass
EL2	Liaison with emergency services	🟢	🟢	🟢	€	Pass
RP2	Contingency planning	🟢	🟢	🟢	€	Pass

Source: Steer Davies Gleave analysis, see preceding text for details of criteria

Security interventions rejected on multiple grounds

6.17 We rejected five security interventions which failed our sift on multiple grounds (more than one red ● in Table 6.8):

- (EA5) blast-resistant storage areas on stations and trains;
- (EA13) ticket barriers on stations;
- (EA12) passenger and baggage screening equipment on stations;
- (EA8) queuing systems at stations;
- (PS1) identity checks at stations, including checking against a nominative ticket.

6.18 All of these security interventions would have a major effect on passengers, were unproven or rarely used on railways, were considered impracticable by at least some stakeholders and appeared, at least from our initial estimates of the associated capital and operating costs, likely to be extremely expensive to implement for all high-speed and international rail services.

6.19 All of these interventions were also, in themselves, likely to cause queuing and hence crowds, creating an additional opportunity for terrorist attack at queuing points, as seen in the attacks on Brussels airport on 22 March 2016.

6.20 We discuss each intervention in turn briefly below.

Rejected security intervention EA5: blast-resistant storage areas on stations and trains

6.21 Many interviewees commented on the issue of suspect packages including luggage left unattended, but none mentioned the storage of luggage on either trains or stations which could, in principle, be made blast-resistant.

Luggage storage on stations

6.22 On stations we noted on a site visit that the left luggage office at Köln Hauptbahnhof does not search or scan left luggage, which is common in the UK, or ask users to identify themselves.

6.23 At stations which have luggage storage facilities, it would in principle be possible to ensure that these were in a blast-resistant storage area. We have not, however, identified any examples of this approach being adopted in practice in any mode of transport, although blast resistant windows are fitted at some stations (see also 4.85).

Luggage storage on trains

6.24 On trains, we noted that existing large floor-to-ceiling luggage racks could be used by terrorists to stack cases containing several hundred kilograms of explosive. A possible security intervention would therefore be to require dedicated storage areas on trains for luggage above a certain size (such as with airline hand baggage), with the aim that any explosion could be remote from passengers and, ideally, contained.

6.25 It would in principle be possible to arrange that all luggage was stored in a single part of the train, analogous to an airline baggage hold, although we note that airline baggage is also screened first and the hold is immediately below the passengers. On long-distance services in North America there is an established convention that passengers have the option, but not the obligation, to check-in baggage which is not required during the journey. Segregated space for

baggage which has already been checked in has also been provided on some point-to-point city to airport rail shuttle services[49].

6.26 However, we identified a number of potential major difficulties with having dedicated baggage areas on trains, summarised in Table 6.9.

Table 6.9: Rejected security intervention EA5: secure luggage storage on trains

Issue	Direct effect	Impact
Dedicated baggage area requires space on train	Less space for passenger accommodation within a given train length, particularly if constrained by platform lengths and track layouts	Existing fleets would need to be modified or replaced.
		Higher capital and operating costs per passenger space.
		Lower capacity from a given number of train paths.
Transfer to and from baggage area takes passenger time	Passengers must arrive earlier and depart later	Longer effective journey times for passengers with baggage.
Baggage must be loaded and unloaded at intermediate stations	Extended dwell times at intermediate stations	Longer on-train times for all through passengers.
		Loss of railway capacity.
Fast loading and unloading requires baggage staff at all stations	Additional staff required	Higher operating costs per train.

Source: Steer Davies Gleave analysis

6.27 In addition, this security intervention would require new or modified rolling stock, probably with lower passenger capacity, and supporting investment, processes and staff at stations.

6.28 Even without providing any blast-resistance, and merely relying on the luggage being remote from passengers, this security intervention would require major changes in operating practice, particularly with the loading and unloading of baggage at intermediate stations:

- If passengers carried their baggage to and from the baggage vehicle, the station dwell time would need to be sufficient for them to walk from the baggage vehicle to their seat or vice versa. Brief dwell times at intermediate stations would no longer be possible, which could extend overall journey times by several minutes per stop and, in some cases, reduce effective capacity. Deutsche Bahn, for example, informed us that high-speed and international trains using Köln Hauptbahnhof cannot be stopped for more than two minutes.
- If special staff carried baggage to and from the vehicle, passengers would need to deposit it after departure and collect it after arrival. In addition, a train might make over 30 stops (see Figure 2.7), implying over 500 possible combinations of luggage origin and destination to be identified and, ideally, segregated and ready for unloading at each intermediate stop.

6.29 If applied to all international services, baggage handling staff would be required to meet all arriving and departing trains at stations such as Ulrichsbrücke-Füssen (see Figure 2.2). In

[49] SBB in Switzerland provides a luggage and flight service, but this requires passengers to drop their baggage at the station in advance of flying. Passenger and their baggage may travel on different trains.

addition, at major terminal stations, delivering several hundred bags per train could require the equivalent of an airport baggage hall, which might require additional construction.

6.30 We conclude that this intervention could, at best, be adopted on dedicated point-to-point trains with no intermediate stops, analogous to the airline model of baggage drop, hold and reclaim.

Rejected security intervention EA13: ticket barriers

6.31 Ticket barriers require that every passenger entering a platform or group of platforms within a station is in possession of a ticket for a journey valid either from that station, or from that station to a destination served from the platforms to which the barriers provide access. While ticket barriers are used in many stations, particularly in the large commuter network around London, many rail networks have a policy that their stations should be open, and many operators, such as Westbahn, offer a pay-on-the-train service. Ticket barriers therefore have a number of disadvantages:

- They impose at least some delay on all passengers.
- They preclude offering a "pay-on-the-train" service which is used in many networks, and is a key part of the offer of some operators.
- They require all access to and from the platform area to be via the ticket barrier line, which may require extensive works to close gaps in the station layout.
- It would not be practicable to introduce them at stations which are both open and unstaffed, such as at Ulrichsbrücke-Füssen (see Figure 2.2).
- They can be evaded by buying a ticket.

6.32 In addition they can result in queues, and hence the artificial creation of crowds, which may create a potential terrorist target. At some major commuter stations, queuing behind the barriers is common at peak periods when the arrival rate of passengers exceeds the processing rate of the barriers. Figure 6.1 illustrates the problem at Brighton in Great Britain on 8 May 2016. Brighton is a busy day trip destination, where closed ticket barriers (left) regularly lead to large crowds waiting to board trains.

Figure 6.1: Rejected security intervention EA13: ticket barriers: crowds at Brighton station

Source: Mark Lee on Twitter, reported in Brighton and Hove News

Rejected security intervention EA12: passenger and baggage screening

6.33 Unlike ticket barriers, which require only that a passenger entering a platform area has a ticket, passenger and baggage screening using scanning technologies to detect objects such as explosives and weapons. Screening can be applied on a sample, random or intermittent basis.

6.34 Baggage screening equipment typically requires a large area and requires staff both to assist passengers and to monitor images, and effective arrangements for responding to a positive detection. At airports, baggage screening is accompanied by passenger screening to ensure that passengers cannot conceal weapons or other forbidden items within their clothing. Equipment may include fixed metal-detecting arches or hand-held devices, but even manual searches require adequate space and staffing.

While screening is near-universal in air travel, our research (see Table 4.7) shows that its use is limited in rail:

- Eurostar, which carries one in six of the passengers crossing EU borders[50], applies passenger and baggage screening, but uses mainly dedicated station facilities designed to comply with the security requirements of the Channel Tunnel.
- AVE in Spain screens baggage, except at some interchanges, and this appears to cause less disruption than would be required for dedicated luggage storage on trains, rejected above (see Table 6.9). However, it requires sufficient security staff available in advance of each station call to process all baggage before departure.
- Thalys and SNCF have initiatives to introduce some checks on a limited number of services in Belgium and France, although this is difficult at stations where different types of train share a platform, as is the case at Brussels Midi (see 4.69) means that such initiatives are likely to be limited.

6.35 Many stakeholders commented that the core Eurostar network is a very unusual system. Trains operate mainly between dedicated platforms in purpose-built terminals, and Eurostar, which has no land transport competitor for passengers without vehicles, described its operation as “an airline that happens to run on rails”. Most high-speed and international rail services are very different from Eurostar, as the following examples show.

6.36 First, stakeholders asked to comment on the practicability of passenger and baggage screening pointed out that most stations would require major works to separate high-speed and international rail passengers from others. Even where this is practicable, it could take many years to plan, design, build and commission the associated infrastructure changes. A number commented that the arrangements at Paris Gare du Nord for Thalys were merely for show, and that last-minute arrivals were allowed onto trains without being scanned, undermining their effectiveness and rationale. We were told that the staff cost €2.5 million per annum for the operation at one platform, and that this could never become the norm for high-speed and international rail services.

6.37 Second, it is not clear how baggage screening could be applied on rural international services. The Außerfernbahn linking Germany and Austria is a minor rural line but serves 30 stations, some of them, like Ulrichsbrücke-Füssen, unstaffed and open (see Figure 2.2). At many similar stations a platform is shared by trains to and from the border. Illustratively, providing for

[50] Eurostar carries 13 million of the estimated 78 million passengers crossing EU borders, see Figure 2.6.

passenger and baggage screening would require comprehensive reconstruction of all stations as enclosed spaces with screening staff at all entry points, and might require the equivalent of around 150 full-time security staff, at a cost of around €7.5 million per annum[51], although this estimate appears much lower than the reported cost at Gare du Nord.

6.38 Second, it is not clear how baggage screening could be applied on suburban and regional international services. The Öresundståg regional network between Denmark and Sweden, shown in Figure 2.7, carries nearly 12 million cross-border passengers per year between 56 stations over nearly 1,000 route-kilometres, dominated by 8-9,000 regular commuters between Malmö and Copenhagen across the Öresund bridge. To provide dedicated platforms for all passengers travelling towards the border would require all 56 stations to have a dedicated platform, each with appropriate security checks. If passengers travelling away from the border were also to be screened, all 56 stations would require two dedicated platforms.

6.39 Studies of passenger identity checks at the Öresund link have suggested that the easiest way to segregate international passengers for any screening process would be to withdraw through international trains and to force all passengers to interchange at a new station with screening checks. This suggests that a permanent requirement to screen passengers at this one border crossing, even if in only one direction, would result in the ending of 15% of European cross-border rail journeys (see paragraph 2.33). Similarly, on the Außerfernbahn it would in practice probably be much cheaper, and less disruptive to passengers, to break the international service at the borders, which would only affect cross-border passengers, than to introduce any form of passenger screening, which would also affect domestic passengers.

6.40 Finally, and as with ticket barriers (see 6.32), passenger and baggage screening can result in the artificial creation of crowds, which may create a potential terrorist target.

Rejected security intervention EA8: queuing systems

6.41 As discussed in relation to the last two rejected security interventions, EA13 and EA12, our literature review noted, and stakeholders confirmed, that the clustering of passengers at stations creates a target in itself. A possible mitigation would be to modify flows around a station to ensure that queuing happens in a controlled manner and that the density of crowds at any given location is as low as possible.

6.42 Many stakeholders emphasised the need to avoid interventions which could cause, or exacerbate, queueing. A number mentioned that the screening of Thalys passengers at the Gare du Nord in Paris had led to queuing, which also occurs regularly at the Eurostar terminals in London, Paris and Brussels, as well as at many other stations with barriers (see Figure 6.1). In interviews we discussed the practicability of holding passengers away from the main concourse nearer to the outside of the station, ideally leaving them at a lower overall density, until close to the time of departure. We were told that this would only push passengers outside the station area into the public areas where they could be the victims of drive-by or similar attacks.

6.43 Paris Gare du Nord station, shown in Appendix D, Figure D.5), handles up to 190 million passengers a year or 500,000 per day. Stations with such high passenger numbers, which might represent the most attractive target , would also be among the most difficult at which

[51] Assuming five employees per station at a total cost of €50,000 per employee, as in paragraph 6.14.

to avoid gatherings of people. A large proportion of those passengers are commuters who either use high frequency suburban services or time their journeys to arrive just before departure. Particularly at PM peak periods, flows into the station may exceed 1,000 persons per minute, arriving by a number of routes, including from metro services, and it would be impractical to prevent any crowd from forming.

6.44 Stakeholders in Germany also pointed out that at large city-centre stations such as Köln Hauptbahnhof, preventing crowding within the station might merely divert it to adjoining properties and streets. Major events in the city had attracted up to 1 million people (see Appendix E, **Error! Reference source not found.**).

6.45 In summary, we found no evidence from our researches that the formation of crowds, particularly in city centres, could be prevented by changes within the boundary of the railway.

Rejected security intervention PS1: identity checks and/or nominative ticketing

6.46 The Terms of Reference required us to examine the measures that would have to be taken to introduce nominative ticketing for all cross-border and high-speed rail services, including consequences for current operating practices. Table 6.10 sets out our understanding of the steps that would be necessary so that the identity of a passenger could be made known to the security forces and confirmed before they were allowed to start their journey.

Table 6.10: Rejected security intervention PS1: identify checks and/or nominative ticketing

Step	Impact on industry	Impact on passenger
Passenger must book in advance	Not possible to offer "pay-on-the-train", or possibly either "pay-at-the-station" or even "pay-on-the-day".	Barrier to travel at short notice, depending on the notice period required by the security services.
Booking medium must allow passenger to specify train and passenger name	Booking requires an alphabet keyboard. Ticket machines must be modified to include a full keyboard. More ticket machines required, because transaction times will be longer.	Transaction times will be longer.
Passenger information must be sent to security services in advance of travel.	Secure data exchange from booking system or machine to security agencies.	Barrier to travel at short notice.
Access to platform area must be restricted to passengers boarding a specific train.	Stations must be configured to make this possible, in principle with separate checks for each train.	Checks, physical barriers, delays and potential crowding.
Passenger must present ticket on arrival at station.	Tickets must be printed or stored for display on a mobile device.	Barrier to "pay-on-the-train".
Passenger must possess and carry an identity card.	Not possible where identity cards are not issued. Not possible for passengers who have no acceptable means of identifying themselves.	Barrier to travel.
Security staff must check passenger identity matches ticket and ticket matches train	Costs of security staff. Possible capacity reductions if checks are at train doors.	Delay. Possible longer journey times if checks are at train doors.
Security staff may deny the passenger the right to travel.	Secure data exchange from security agencies to station security staff.	Privacy. Barrier to travel.

6.47 Some railway undertakings now issue some tickets on a "nominative" basis, on the condition that a proof of identity is presented, as a means of preventing user-printed tickets being transferred or duplicated. However, capturing identity information at the time of ticket sale requires either that passengers have a personal travel account, or that they pay by a credit or debit card linked to their name, or that their name and/or other identity information are entered into the booking system. If commercial means of identification (such as credit cards) were used, it would be necessary to restrict the types of card used, for instance prohibiting pre-paid debit cards which are not tied to a named individual. Eurostar advised us that they have already banned the use of cash to buy turn-up-and-go tickets between Brussels and Lille.

6.48 In addition the passenger's name must be printed on, or at least linked in a reservation system to, their ticket. Major changes to ticket machines and booking office equipment, longer transaction times, and consequently more ticket machines and/or booking office staff, would be required if tickets were to include the passenger name.

6.49 Subsequent identity checking requires systems and data exchanges to be in place, and legal provision for this data to be used. Such arrangements do not yet exist, but the aviation sector is leading the way following the April 2016 European Parliament's adoption of the Passenger Name Record (PNR) Directive. Eurostar informed us that it had actively lobbied for PNR data to be gathered in the rail sector, although it stated that a key objective was to establish a

passenger manifest that could be used following an incident. We note, however, that identity checks require data exchange, which can be difficult to achieve given the sensitivity of data held by national security agencies.

6.50 If this intervention were adopted, checks would also be made that the passenger is the person for whom the reservation was made. It might also be difficult to implement such checks for domestic high-speed travel in Member States which do not issue, or require citizens to acquire or carry, identity documents.

6.51 Stakeholders agreed that if nominative ticketing was to be employed as a counter-terrorism intervention, identity checks would need to be before boarding. This could be a time-consuming process, likely to require an increase in existing station dwell times and hence potentially both extend effective journey times and reduce the number of services operated within existing capacity constraints (see also Table 6.9).

6.52 Sweden has imposed a requirement for one element of the nominative ticketing process, checks on passenger identity, as a requirement for passengers entering from Denmark across the Öresund bridge, which carries around one in six of all passengers crossing EU borders. The arrangement is achieved through Sweden making railway undertakings responsible for ensuring that passengers have the right to enter Sweden, and the railway undertakings in turn making production of valid identity documents a condition of carriage. The estimated cost to the regional economies of checks in one direction, into Sweden, affecting one in twelve of all passengers crossing EU borders, is €150 million each year (see Table 4.6).

6.53 On open stations such as Ulrichsbrücke-Füssen (see Figure 2.2), it would in principle be possible to implement nominative ticketing by requiring all passengers to enter the train through a single door controlled by a member of staff performing an identity check. In addition to requiring security staff at each train departure, this might also result in extended journey times.

6.54 Alternatively, and instead of full nominative ticketing, the security intervention could be limited to a check on passengers' identity documents. However, it is not clear either what purpose this would serve, or how it would work where citizens do not have, or are not required to carry, identity documents.

6.55 We understand that draft legislation has been introduced in the Belgium parliament to extend the PNR system to all international trains crossing Belgian borders[52]. Operators would be required to collect and submit information on passengers 24 hours in advance.

Security interventions rejected on other grounds

6.56 We also rejected four potential security interventions on other grounds:

- mobile detection equipment (drones);
- liaison with security experts in other fields;
- staff physical screening; and
- road vehicle intrusion protection.

[52] Railway Gazette, 21 September 2016. Railway Gazette also suggested that the PNR requirements would make it impossible for SNCB or its neighbouring railways to operate cross-border regional trains.

Rejected security intervention EA11: mobile detection equipment (drones)

6.57 We conceived this security intervention as a means of monitoring the extensive infrastructure used by high-speed and international rail services. We did not attempt to estimate the length of line involved but note, for instance, that the European high-speed network alone extends to nearly 7,500 kilometres (see 3.26). Even with a strategy of prioritising weak points for monitoring, it would not be possible to monitor all locations continuously, and even periodic examination by patrolling has significant cost.

6.58 Railways have in the past mandated patrolling by track workers, briefed to report signs of unusual activity, although such reports may only be made some time after the unusual activity is observed. Patrolling can also be extended to include a wider examination of threats to the infrastructure. High Speed 1 in the UK told us it employs a security company to patrol the entire length of its infrastructure, engage with local communities and look for signs such as attempts to breach the protective barrier, but its network is only just over 100 kilometres long.

6.59 Until recently, it would be expensive to carry out more than infrequent patrols, but drones now available can in principle be used for continuous supervision of the network and monitored from a central location. We did not identify examples of their use specifically for security purposes, but they are demonstrating their value in wider infrastructure management. SNCF, for example, reports in a press release that they are being used for surveillance and inspections of tracks, catenary, trackside, structures, depots and stations, including roofs.

6.60 However, the practicality and value of patrolling by drones might depend on whether patrolling remained possible, or was effective, in conditions of night, rain, snow or fog. With no proven use of drones at present, and no clear industry consensus on what security role they would play, and hence how this could be defined and set in standards, we rejected them from the sift.

Rejected security intervention EL3: liaison with security experts in other fields

6.61 We considered an intervention of regular liaison and exchange of information between security experts in the rail sector and those in industries facing similar challenges, such as air, maritime and road transport, retail and hotel and catering. Such liaison might help determine best practice and identify interventions deployed or trialled in other sectors that might be applicable to rail. Some stakeholder reported that they had discussions with experts from other sectors, often in collaboration with the police/security agencies. However, a number expressed concern at the suggestion that it would be practicable to adopt approaches similar to aviation, and asserted that the rail is very different from air. A further issue (see 6.15) is that landlocked Member States may have few or no experts on maritime safety, and smaller Member States may have a single airport and no dedicated expertise in aviation safety.

6.62 In practice we rejected this potential security intervention, as it did not appear likely to be practicable to draft legislation at the European level which could specify at the national level which rail sector bodies should carry out liaison, which bodies in which other sectors should be required to liaise with them, or what information they should be required to exchange.

Rejected security intervention SR4: staff physical screening

6.63 Where security interventions rely on restricting access to specific areas of railway property to certain staff, it may be necessary to identify and/or to screen them to ensure that they are not

carrying weapons or devices. This intervention could be applied in circumstances where passengers are being screened in security intervention EA12, which we have already rejected. It could also be applied on a more limited basis where staff enter secure areas such as signalling equipment rooms.

6.64 We did not consider it likely to be practicable to draft European legislation requiring such screening, for a number of reasons:

- The number and nature of the secure locations involved will vary from Member State to Member State, and would ideally be based on a detailed risk assessment.
- Without first identifying the locations, it is not clear what national bodies are responsible for them: these might include the infrastructure manager, railway undertaking, station manager, or potentially other bodies such as police forces with premises on stations.
- The identity, role and employer of personnel permitted to enter might vary widely.
- Various means of screening might be appropriate, including unattended access with a security such as smartcard and PIN or biometric data, remote CCTV check on identity, identity check by staff already in the area, and pre-entry screening by permanent security staff.

6.65 More widely, stakeholders commented that it would be disproportionately expensive to retain screening equipment and staff at any location where it was not already provided to screen passengers.

Rejected security intervention EA7: road vehicle intrusion projection

6.66 The infrastructure used by high-speed and international trains extends over thousands of kilometres (see 3.26), and much of it is either unfenced or protected only by a light fence designed to prevent intrusion by people and animals. Much of the network is therefore vulnerable to incursion by a road vehicle, particularly if this hit a train. However, as the incident at Great Heck shows, it can be argued that barriers should be used to contain vehicles within the road network, rather than to exclude them from the rail network[53].

6.67 A number of stakeholders mentioned the risks associated with vehicle incursion, but the only systematic programme referred to was that in the UK, where vehicles have been used in previous attacks on rail services, whether to carry an explosive device or to travel to and enter stations and other locations. This highlights the fact that various means of attack are possible:

- “ram-raiding” railway premises, with the intention of stealing goods or cash;
- driving up a ramp onto a platform to run down waiting passengers, as has happened on the light rail system in Jerusalem, although it might be difficult to do so without the passengers having sufficient warning to escape;
- conveying explosives into station areas, which might be made easier by knocking down a wall or fence, or driving down the track, especially where the railway runs at ground level through an urban area and roads parallel it on one or both sides; and

[53] On 28 February 2001 a light vehicle and trailer left a motorway and came to rest on the East Coast Main Line at Great Heck in Great Britain. The vehicle derailed a high-speed passenger train which then collided with a freight train travelling in the other direction with a closing speed of 229km/h. Ten people were killed and a number of rail vehicles were destroyed in the incident. Studies have suggested that the accident would best have been prevented by better barriers on the road, rather than on the railway.

- bringing explosives into contact with a train, which would often be easy on remote sections of infrastructure.

6.68 The scale of the security intervention therefore depends on the means of intrusion to be excluded:

- Preventing direct incursions into stations from the adjacent road network can be achieved by bollards and similar structures and restrictions on parking and drop-off.
- Preventing incursions into stations from the road network at level crossings or goods areas is more difficult: vehicles with adequate ground clearance, including most trucks and 4x4 vehicles, can be drive along a railway track.
- Preventing incursions into any part of the rail network, as would be needed to eliminate accidents such as Great Heck, would require thousands of kilometres of barriers designed to stop relatively large vehicles[54].

6.69 However, we note three potential difficulties with attempting to seal the high-speed and international railway infrastructure against all possible vehicle incursions:

- A decision would be needed on whether the highway infrastructure manager should contain vehicles or the railway infrastructure manager should exclude them.
- If barriers were built along the railway infrastructure, it might become more difficult to gain access to carry out routine maintenance and renewal work and in emergencies.
- In either case, the likely extremely high cost and time required to enclose thousands of kilometres of infrastructure, much of it remote and unattended.

6.70 We therefore rejected road vehicle exclusion as a security intervention.

Security interventions retained

6.71 Table 6.11 summarises the security interventions retained after our sifting process.

[54] The truck used in the attack on the Promenade des Anglais in Nice on 14 July 2016, killing 86 people and injuring 434, was a Renault Midlum with a gross vehicle weight of up to 19 tonnes.

Table 6.11: Potential security interventions retained

Intervention Notes: ● = primary objective addressed + = secondary objective addressed		Terms of Reference	Potential scope			May address objectives?			
			Infrastructure	Stations	Trains	Shared EU understanding	Reflect EU-wide benefits	Consistent risk assessment	Coordinated approach
Communications and external liaison									
EL1	Partnerships with third parties							●	+
EL2	Liaison with emergency services	4	●	●	●			●	+
Assets and equipment design									
EA6	Recording of vulnerabilities in asset register		●	●		+		●	
EA4	Station duplicate access routes and walkways			●			●		
EA3	Facilitation of emergency egress at stations			●	●		●		
EA1	Blast-resistant stations and trains	8		●	●		●		
EA2	Minimisation of unseen areas			●	●				●
EA9	Facial or behaviour recognition technology			●	●				●
EA10	Static detection equipment (CCTV)	10		●	●				
EA14	Resistant radio and communications systems		●		●			●	+
EA15	Contingency IT and communications systems		●		●			●	+
Staff and training									
SR1	Training in risk and behaviour monitoring	6	●	●					●
SR2	Training in incident response	7	●	●				●	+
SR3	Staff vetting		●	●	●	●			●
SR5	Staff deployment		●	●	●				●
Risk assessment and planning									
RP1	Threat level protocols	1				●		●	+
RP2	Contingency planning	2	●	●	●			●	+
RP3	Drills and exercises	3	●	●	●			●	+
RP4	Post-incident recovery	5	●	●	●			●	+
Procedures and systems									
PS2	Awareness promotion among passengers		●						●
PS3	Targeted storage of contingency reserves		●	●				●	+
PS4	Inspection regimes		●	●	●			●	

Source: Steer Davies Gleave analysis, see text for details

Best practice, guidelines and mandatory requirements

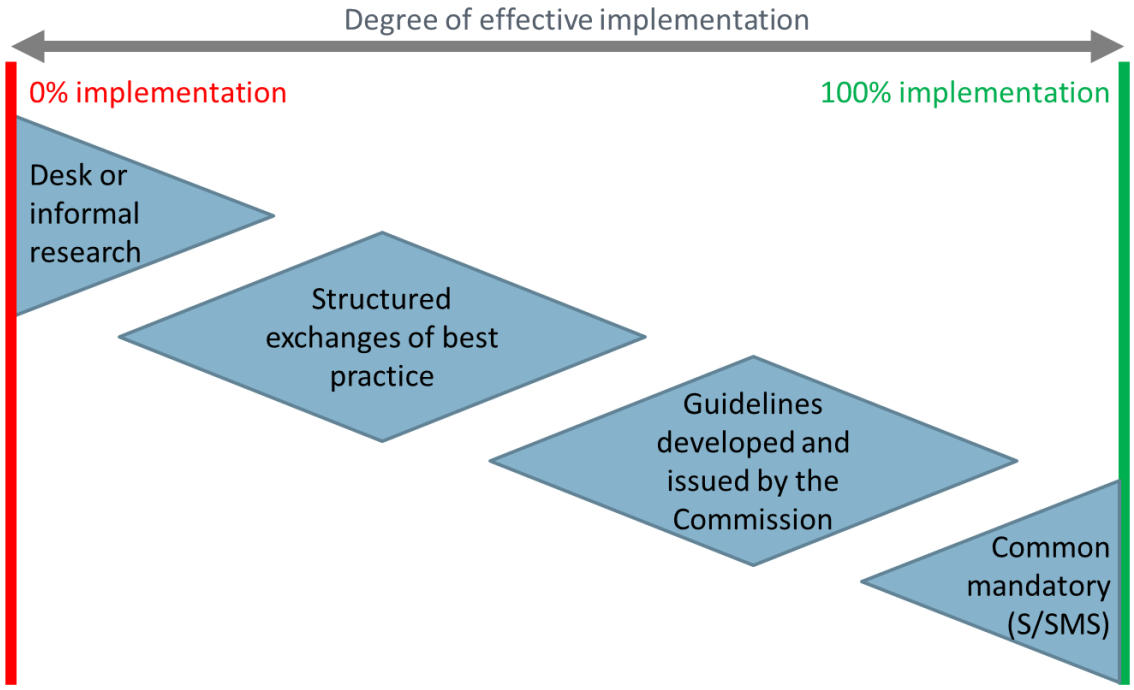
6.72 The Terms of Reference noted that that intervention could in principle be:

- common mandatory requirements set at EU level;
- guidelines to be developed and issued by the Commission; or
- exchanges of best practices among EU Member States and rail transport operators.

6.73 We assume that exchange of best practices might also be by other bodies such as infrastructure managers, station managers and local, regional and national police forces and emergency services.

6.74 Figure 6.2 sets out a possible interpretation of the effectiveness of these different approaches, which we discuss below.

Figure 6.2: Effectiveness of best practice, guidelines and mandatory requirements



Source: Steer Davies Gleave analysis, horizontal axis is not to scale, see text for details

No implementation

6.75 An industry body or individual might be unaware of a potential security intervention, or might not have sought information on how it could be implemented. This position is represented by the extreme left of Figure 6.2.

Desk or informal research

6.76 An industry body or individual might be aware of a potential security intervention, and carry out limited informal research, reading online information such as that we found in our Literature Review (see Appendix A), studies published by the Commission, or holding informal discussions with colleagues and suppliers. This approach appears unlikely to result in an effective adoption of the intervention, although in a small infrastructure manager, railway undertaking or station manager, a single individual carrying out desk research and discussing the findings with a small number of relevant colleagues, might prove effective. Checking that a station had no or minimal unseen areas (EA2), for example, might be completed by a station manager in minutes.

Structured exchanges of best practice

6.77 A more formal approach to applying best practice would be to intervene to have formal processes for identifying best practice, including direct contact with relevant comparators in the rail and other industries. While desk or informal research relies on an individual or

department being proactive, creation of a formal exchange mechanism such as conferences, meetings, internet fora or bulletins ensures that best practice comes to the attention of even passive staff.

Guidelines developed and issued by the Commission

6.78 A second level of intervention would be for the Commission to develop and issue guidelines on a particular security intervention. In the example of minimising unseen areas (EA2), for example, these might include guidelines on how to identify such areas and/or how often to check them[55].

Common mandatory requirements

6.79 A third level of intervention would be for the Commission to introduce common mandatory requirements through a Regulation or Decision. These would, in principle, ensure near-100% implementation of the requirements, particularly if cascaded through the industry, and relevant parties within it, through a Safety and/or Security Management System (S/SMS).

6.80 We stress that Figure 6.2 is illustrative, for at least two reasons. First, the degree of effective intervention might vary widely between actors, and even informal research and internal discussion might be effective in small organisations[56]. Second, the horizontal axis is not to scale and is not intended to show the actual effectiveness of either exchange of best practice or Commission guidelines.

The effectiveness of Commission guidelines

6.81 We also sought evidence of the effectiveness of Commission guidelines from previous stakeholder comments, and in particular the effect of interpretative guidelines concerning Regulation 1370/2007, which also deals with the provision of public passenger transport, including by rail[57]. In February 2016 we completed an assessment of the impact of the Regulation and the associated guidelines[58], in which stakeholders were invited to describe any guidelines of which they were aware and, where they mentioned them, their view of the Commission's interpretative guidelines. The small sample of nine clear responses is summarised in Table 6.12.

[55] For example, London Underground Limited carries out frequent checks that cupboards and equipment spaces have not been tampered with or used to conceal materials or devices.

[56] After drafting this observation, we were told a case where members of one infrastructure manager's staff had proactively read the detailed reports of an incident on another network, identified the implications for their organisation, and arranged to have relevant changes implemented, without any formal publication of either "best practice" or "guidelines".

[57] Communication from the Commission (2014/C 92/01) on interpretative guidelines concerning Regulation (EC) No 1370/2007 on public passenger transport services by rail and by road.

[58] Study on economic and financial effects of the implementation of Regulation 1370/2007 on public passenger transport services, Final Report, February 2016.

Table 6.12: Evidence of the use of guidelines

	No reference to guidelines	Has internal guidelines	Aware of and uses EU guidelines	Aware of and critical of EU guidelines
Number of respondents	5	1	1	2

Source: Steer Davies Gleave. Study on economic and financial effects of the implementation of Regulation 1370/2007 on public passenger transport services, Final Report, February 2016.

6.82 In practice only one of the nine respondents was both aware of the guidelines and made use of them. By contrast, two respondents were aware of the guidelines but were critical of them.

6.83 While we acknowledge that this is an extremely small sample, this suggests that Commission guidelines may only be seen, and taken into account, by around 10% of the industry. In the absence of processes to require that they are consistently applied, the effective level of implementation may be much lower. We assume, by analogy, that the extent of both awareness of, and adherence to, best practice publicised only by the means listed in paragraph 6.77 may be even lower.

The effectiveness of exchange of best practice

6.84 Stakeholders made a number of comments on best practice, with two main themes:

- First, fora already exist for the exchange of best practice, whether in the form of regular meetings, or websites on which ideas can be shared, or academic literature of the type we have examined (and see also footnote 56).
- Second, parties must proactively make use of the best practice information available.

6.85 In Belgium, IM Infrabel referred to studies of vulnerabilities for soft targets, including high-speed services, which are seen as iconic. It is actively seeking to learn from best practice elsewhere, and in particular is adopting the approach of a Security Management System (see Appendix D, **Error! Reference source not found.**).

6.86 In the Netherlands, IM ProRail informed us that it is active in working with other IMs through the PRIME platform and through its membership of EIM. There is a lively exchange of best practice. There are also informal contacts with other networks, notably Infrabel. ProRail and RU NS also share experience and best practice on security at international level, such as within EIM, UIC, CER and COLPOFER. The Netherlands Ministry of Infrastructure and Environment participates in the EU LANDSEC meetings and in EU Transport Council (including working groups) (see Appendix D, **Error! Reference source not found.**-**Error! Reference source not found.**).

6.87 In Sweden, IM Trafikverket emphasised the Swedish consensus on the importance of sharing best practice, which it has discussed at LANDSEC and at a recent UITP meeting. It also expressed concern that the European Union Agency for Railways (the Agency, formerly the European Railway Agency (ERA)) collects large volumes of technical data from the railways and may not always consider the detailed security implications of making this available (see Appendix D, **Error! Reference source not found.**).

6.88 In the UK, operator body ATOC publishes best practice in station incident response plans, but expressed a concern that while local plans exist they are not always adequate. A working group (the Emergency Planning Group) had examined the plans for three of the largest stations and found that they are little more than evacuation plans. Their limitations had been

illustrated by how flooding at Gatwick Airport had led to a loss of power with major consequence. A key risk not currently covered is a marauding shooter. (see Appendix D, **Error! Reference source not found.**).

6.89 We concluded that a range of fora already exist for exchanging best practice, and the principal issue was not the availability of information, or fora, but of the willingness of stakeholders to seek and apply information on best practice which is already available.

6.90 Accordingly, we adopted an assumption that wherever possible interventions should be specified in common mandatory requirements, such as through a Regulation or Decision. We note that Regulations may include both positive permissive ("may") and positive imperative ("shall")[59]. This means that common "mandatory" requirements may still include security interventions which are permitted but not mandatory, or mandatory only under certain defined circumstances.

The effect of mandatory, guidelines or best practice relative to the current position

6.91 A further practical issue in assessing the effect of best practice, guidelines and mandatory requirements is illustrated in Figure 6.2: without a means of quantifying the extent to which existing best practice, guidelines and even mandatory guidelines are already implemented, there is no means of quantifying the effect of any further interventions. We discuss this further in Chapter 9.

Summary

6.92 The analysis above has reduced the long list of 30 potential security interventions, shown in Table 6.3, to 21. Table 6.13, which repeats Table 6.11, lists the potential security interventions retained.

[59] English Style Guide, A handbook for authors and translators in the European Commission, Eighth edition: January 2016, Last updated: October 2016.

Table 6.13: Potential security interventions retained

Intervention Notes: ● = primary objective addressed + = secondary objective addressed		Terms of Reference	Potential scope			May address objectives?			
			Infrastructure	Stations	Trains	Shared EU understanding	Reflect EU-wide benefits	Consistent risk assessment	Coordinated approach
Communications and external liaison									
EL1	Partnerships with third parties							●	+
EL2	Liaison with emergency services	4	●	●	●			●	+
Assets and equipment design									
EA6	Recording of vulnerabilities in asset register		●	●		+		●	
EA4	Station duplicate access routes and walkways			●			●		
EA3	Facilitation of emergency egress at stations			●	●		●		
EA1	Blast-resistant stations and trains	8		●	●		●		
EA2	Minimisation of unseen areas			●	●				●
EA9	Facial or behaviour recognition technology			●	●				●
EA10	Static detection equipment (CCTV)	10		●	●				
EA14	Resistant radio and communications systems		●		●			●	+
EA15	Contingency IT and communications systems		●		●			●	+
Staff and training									
SR1	Training in risk and behaviour monitoring	6	●	●					●
SR2	Training in incident response	7	●	●				●	+
SR3	Staff vetting		●	●	●	●			●
SR5	Staff deployment		●	●	●				●
Risk assessment and planning									
RP1	Threat level protocols	1				●		●	+
RP2	Contingency planning	2	●	●	●			●	+
RP3	Drills and exercises	3	●	●	●			●	+
RP4	Post-incident recovery	5	●	●	●			●	+
Procedures and systems									
PS2	Awareness promotion among passengers		●						●
PS3	Targeted storage of contingency reserves		●	●				●	+
PS4	Inspection regimes		●	●	●			●	

Source: Steer Davies Gleave analysis, see text for details

6.93 We rejected one of the security interventions suggested in the Terms of Reference, nominative ticketing (PS1), and the more restricted intervention of passenger identity checks. As we set out in Table 6.10, either intervention would raise both practical difficulties for operators and barriers to travel for passengers.

6.94 The remaining security interventions address issues associated with stations (subject to how the boundaries of a station should be defined for security purposes), trains and infrastructure (noting that not all the infrastructure need be "secure" to protect the travelling public).

6.95 The remaining security interventions also cover all stages of activity: communication and external liaison (EL), asset and equipment design (EA), staff and training (SR), risk assessment and planning (RP) and procedures and systems (PS).

6.96 Few of the interventions, strictly defined, require coordination across borders or at the European level. In general, they can be introduced on an individual station, train, service, route or Member States, or bi- or multi-laterally between Member States who have chosen to coordinate their approaches.

6.97 While interventions could be introduce through approaches such as exchange of best practice or Commission guidelines, evidence from recent studies is that awareness of, and adherence to, Commission guidelines may be low (see Table 6.12). We therefore assume that, to the extent possible, interventions should be specified in common mandatory requirements, noting that these may be permissive, rather than imperative, in certain areas where this is appropriate.

6.98 There is therefore a need to devise policy measures which could ensure that some or all of these security interventions were applied in a consistent manner across the EU, with the aim of meeting some or all of the objectives set out in Table 5.1.

7 Potential policy measures

Introduction

7.1 In this chapter we describe a number of potential policy measures, in some cases based on one or more of the retained security interventions, which might contribute to one or more of the specific objectives.

Specific objectives

7.2 Table 7.1 below restates the specific objectives developed in chapter 5 and listed in Table 5.1.

Table 7.1: Specific objectives to be addressed by policy measures

Problem drivers (See Figure 4.2)	Specific objective	Rationale/comment
Insufficient understanding of the threat	**Shared EU understanding** Ensure relevant stakeholders have a more thorough and shared understanding of the security threat across the EU.	While the problem is partly the result of underlying data limitations, more could be done to ensure that rail industry and other stakeholders across the EU share a better understanding of the threat.
Inadequate response to the threat	**Reflect EU-wide benefits** Ensure that the response to the threat adopted by the industry takes full account of the economic and social benefits of security interventions across the EU.	There is a need to address externalities, in the form of security benefits that are not taken into account in commercial decision-making. At the same time, the economic and social benefits of security interventions need to be fully considered by public sector decision-makers determining investment priorities.
Different approaches to mitigation in Member States	**Consistent risk assessment** Ensure that mitigation of the security threat in different Member States is based on a consistent assessment of underlying risks.	While the specific security interventions adopted in different Member States will vary according to circumstances, it is important that common risks are assessed using the best methodologies available to the industry.
Fragmentation and gaps in security coordination	**Holistic and coordinated approach** Ensure that the security threat to high-speed and international rail services is addressed in a holistic and coordinated manner.	Mitigation measures should be applied consistently and coherently to an entire service or group of services, so that measures employed on one part of a journey cannot be circumvented or undermined by perpetrator actions taken on another part.

Source: Steer Davies Gleave analysis

Potential policy measures

7.3 Table 7.2 below restates the security interventions retained in Chapter 7 and listed in Table 6.13.

Table 7.2: Potential security interventions retained

Intervention Notes: ● = primary objective addressed + = secondary objective addressed		Terms of Reference	Potential scope			May address objectives?			
			Infrastructure	Stations	Trains	Shared EU understanding	Reflect EU-wide benefits	Consistent risk assessment	Coordinated approach
Communications and external liaison									
EL1	Partnerships with third parties							●	+
EL2	Liaison with emergency services	4	●	●	●			●	+
Assets and equipment design									
EA6	Recording of vulnerabilities in asset register		●	●		+		●	
EA4	Station duplicate access routes and walkways			●			●		
EA3	Facilitation of emergency egress at stations			●	●		●		
EA1	Blast-resistant stations and trains	8		●	●		●		
EA2	Minimisation of unseen areas			●	●				●
EA9	Facial or behaviour recognition technology			●	●				●
EA10	Static detection equipment (CCTV)	10		●	●				
EA14	Resistant radio and communications systems		●		●			●	+
EA15	Contingency IT and communications systems		●		●			●	+
Staff and training									
SR1	Training in risk and behaviour monitoring	6	●	●					●
SR2	Training in incident response	7	●	●				●	+
SR3	Staff vetting		●	●	●	●			●
SR5	Staff deployment		●	●	●				●
Risk assessment and planning									
RP1	Threat level protocols	1				●		●	+
RP2	Contingency planning	2	●	●	●			●	+
RP3	Drills and exercises	3	●	●	●			●	+
RP4	Post-incident recovery	5	●	●	●			●	+
Procedures and systems									
PS2	Awareness promotion among passengers		●						●
PS3	Targeted storage of contingency reserves		●	●				●	+
PS4	Inspection regimes		●	●	●			●	

Source: Steer Davies Gleave analysis, see text for details

7.4 We next describe the proposed policy measures in greater detail. For each we describe in turn the information summarised in Table 7.3.

Table 7.3: Description of policy measures

Characteristic	Details
Definition	How the policy measure might be defined, and in particular on which parties it would impose obligations
Security interventions	What security interventions listed in Chapter 6 could be included within the scope of the policy measure.
Parties required to take action	What parties might be affected, or acquire obligations, as a result of the policy measure, such as: • Government involved in rail transport at national, regional or local level • Industry bodies such as infrastructure managers (IMs), station managers (SMs) and railway undertakings (RUs) • Third parties including supplier and contractors, and tenants and others working on railway premises
Objectives met	What additional objectives, if any, this larger package of security interventions might address.
Scope and coverage	Whether the policy measure could be limited to staff, stations, rolling stock or infrastructure directly used in the provision of high-speed and international rail services, and hence the proportion of the railway to which it might be applied.
Mandatory, guidelines or best practice	Whether, given practical issues, the policy measures should be mandatory.
Contingency	Whether, given the interaction between policy measures, this measure would only be introduced as part of a package with another measure contributing to the same objective.

Source: Steer Davies Gleave analysis

Policy measures to contribute to objective 1: shared EU understanding

7.5 We devised two policy measures to contribute to objective 1, shared EU understanding:

- Policy measure 1A would establish a format for reporting, and a framework for monitoring, national level data relevant to security of high-speed and international rail services.
- Policy measure 1B would establish a framework for researching and disseminating information on relevant security incidents around the world.

7.6 We stress that neither policy measure, in itself, would completely meet objective 1. We propose, however, that policy measure 1B would not be introduced without policy measure 1A. We discuss this contingency further in our discussion of policy options in Chapter 8.

Policy measure 1A: reporting and monitoring national security data

Table 7.4: Policy measure 1A: reporting and monitoring national security data

Characteristic	Details
Definition	The policy measure would mean: • To define national level data which should be monitored • To identify or establish a body to be responsible for monitoring • To vest that body with duties and powers necessary to them • To define national level data that should be reported • To define reporting formats for the data • To identify national bodies who would be required to collate and provide the data • To set protocols for dissemination of the data
Security interventions	None of the potential security interventions retained in Table 7.2 would be associated with this policy measure.
Parties required to take action	We consider that this policy measure would require action primarily by national, regional and local government departments responsible for transport and the rail industry to plan the collection and reporting of monitoring data. In addition, the provision of data might need to extend to some or all of infrastructure managers (IMs), station managers (SMs), railway undertakings (RUs) and third parties such as contractors
Contribution to objective(s)	This policy measure was devised to contribute to objective 1, shared EU understanding. It could also support: • Objective 2: reflect EU-wide benefits • Objective 3: consistent risk assessment
Scope and coverage	This policy measure, by its nature, would not naturally be restricted to particular parts of the rail system, although reporting and monitoring could be limited to stations, trains and infrastructure used by high-speed and international rail services.
Mandatory, guidelines or best practice	We consider that this policy measure would need to be mandatory. However, we are aware of cases where even mandatory reporting is not carried out by the many national, regional and local bodies required to do so[60].
Contingency	The policy measure could be introduced independently of other policy measures.

Source: Steer Davies Gleave analysis

[60] Article 7 of Regulation 1370/2007 requires that "Each competent authority shall make public once a year an aggregated report on the public service obligations for which it is responsible, the selected public service operators and the compensation payments and exclusive rights granted to the said public service operators by way of reimbursement". When we examined compliance with this mandatory requirement for the Commission we found that few competent authorities had made public data which met these requirements. Study on economic and financial effects of the implementation of Regulation 1370/2007 on public passenger transport services, Final Report, February 2016.

Policy measure 1B: researching and disseminating worldwide security data

Table 7.5: Policy measure 1B: reporting and disseminating worldwide security data

Characteristic	Details
Definition	The policy measure would mean: • To define information which should be researched and disseminated • To identify national bodies to whom the information should be disseminated • To define protocols for when dissemination should be limited on security grounds
Security interventions	None of the potential security interventions retained in Table 7.2 would be associated with this policy measure.
Parties required to take action	We consider that this policy measure would require action primarily by national, regional and local government departments responsible for transport and the rail industry to plan the reporting and dissemination of worldwide security data. In addition, some or all of infrastructure managers (IMs), station managers (SMs), railway undertakings (RUs) and third parties such as contractors might be recipients of the data.
Contribution to objective(s)	This policy measure was devised to contribute to objective 1, shared EU understanding. It could also support: • Objective 2: reflect EU-wide benefits • Objective 3: consistent risk assessment
Scope and coverage	This policy measure, by its nature, would not be restricted to particular parts of the EU rail system and would involve reporting and dissemination of any relevant data from any sector.
Mandatory, guidelines or best practice	We consider that this policy measure could take the form of guidelines because it would, in practice, be difficult to describe in advance what worldwide information would be relevant to the security of high-speed and international rail services.
Contingency	We consider that this policy measure should only be introduced if policy measure 1A was also introduced, establishing the communication channels on which it would rely.

Source: Steer Davies Gleave analysis

Policy measures to contribute to objective 2: reflect EU-wide benefits

7.7 We devised four policy measures to contribute to objective 2, reflect EU-wide benefits:

- Policy measure 2A would focus on providing egress and access routes to stations, in particular to allow continued operation if one route was closed for security reasons.
- Policy measure 2B would relate to providing blast-resistant features in stations.
- Policy measure 2C would relate to providing blast-resistant features on trains.

7.8 We stress that no one policy measure, in itself, would completely meet objective 2, and so any or all of the four policy measures could be introduced independently (giving, in theory, 15 possible combinations). We discuss this contingency further in our discussion of options in Chapter 9.

Policy measure 2A: emergency egress and access to stations

Table 7.6: Policy measure 2A: emergency egress and access to stations

Characteristic	Details
Definition	The policy measure would mean: • To define standards for emergency egress and access to stations • To identify bodies responsible for implementing the standards
Security interventions	The following potential security interventions retained in Table 7.2 could be associated with this policy measure: • EA3: facilitation of emergency egress from stations • EA4: duplicated access routes and walkways in stations
Parties required to take action	We consider that this policy measure would require action primarily by infrastructure managers and station managers, depending on how responsibility for stations is allocated. Station managers in some Member States may be railway undertakings, local bodies or private parties.
Contribution to objective(s)	This policy measure was devised to contribute to objective 2, reflect EU-wide benefits. It does not appear to contribute to any other objectives.
Scope and coverage	This policy measure, by its nature, would be restricted to stations, and could be restricted to stations called at (rather than passed through or stopped in) by high-speed and/or international rail services. Excessive compliance costs might result in station calls on high-speed trains being withdrawn, or international services being broken at borders or shortened (in extremis to cross-border shuttles).
Mandatory, guidelines or best practice	We consider that this policy measure could take the form of guidelines because it would, in practice, be difficult to mandate in advance standards which would be both implementable and sufficiently inexpensive to result in the withdrawal or services.
Contingency	The policy measure could be introduced independently of other policy measures.

Source: Steer Davies Gleave analysis

Policy measure 2B: blast-resistant features on stations

Table 7.7: Policy measure 2B: blast-resistant features on stations

Characteristic	Details
Definition	The policy measure would mean: • To define standards for blast-resistance on stations • To identify bodies responsible for implementing the standards
Security interventions	The following potential security interventions retained in Table 7.2 could be associated with this policy measure: • EA1: blast-resistant stations
Parties required to take action	We consider that this policy measure would require action primarily by infrastructure managers and station managers, depending on how responsibility for stations is allocated. Station managers in some Member States may be railway undertakings, local bodies or private parties.
Contribution to objective(s)	This policy measure was devised to contribute to objective 2, reflect EU-wide benefits. It does not appear to contribute to any other objectives.
Scope and coverage	This policy measure, by its nature, would be restricted to stations, and could be restricted to stations called at (rather than passed through or stopped in) by high-speed and/or international rail services. Excessive compliance costs might result in station calls on high-speed trains being withdrawn, or international services being broken at borders or shortened (in extremis to cross-border shuttles).
Mandatory, guidelines or best practice	We consider that this policy measure could take the form of guidelines because it would, in practice, be difficult to mandate in advance standards which would be both implementable and sufficiently inexpensive to result in the withdrawal or services.
Contingency	The policy measure could be introduced independently of other policy measures.

Source: Steer Davies Gleave analysis

Policy measure 2C: blast-resistant features on trains

Table 7.8: Policy measure 2C: blast-resistant features on trains

Characteristic	Details
Definition	The policy measure would mean: • To define standards for blast-resistance on trains • To identify bodies responsible for implementing the standards
Security interventions	The following potential security interventions retained in Table 7.2 could be associated with this policy measure: • EA1: blast-resistant trains
Parties required to take action	We consider that this policy measure would require action primarily by railway undertakings in the first instance. However, where rolling stock is not owned by the railway undertaking, responsibility might lie with rolling stock manufacturers or leasing companies.
Contribution to objective(s)	This policy measure was devised to contribute to objective 2, reflect EU-wide benefits. It does not appear to contribute to any other objectives.
Scope and coverage	This policy measure, by its nature, would be restricted to trains, and could be restricted to trains used to provide high-speed and/or international rail services. Excessive compliance costs might result in high-speed services being withdrawn, or international services being broken at borders or shortened (in extremis to cross-border shuttles).
Mandatory, guidelines or best practice	We consider that this policy measure could take the form of guidelines because it would, in practice, be difficult to mandate in advance standards which would be both implementable and sufficiently inexpensive to result in the withdrawal or services.
Contingency	The policy measure could be introduced independently of other policy measures.

Source: Steer Davies Gleave analysis

Policy measures to contribute to objective 3: consistent risk assessment

7.9 We devised six policy measures to contribute to objective 3, consistent risk assessment:

- Policy measure 3A would include arrangements to ensure exchange of information by relevant agencies in a Security Management System (SMS).
- Policy measure 3B would require vulnerabilities to be identified in the asset register, with an appropriate inspection regime, in a Security Management System (SMS).
- Policy measure 3C would include contingency planning and incident recovery in a Security Management System (SMS) (in Terms of Reference, see Table 6.1).
- Policy measure 3D would include contingency communication systems and reserves, such as first aid equipment and spare cable, in a Security Management System (SMS).

7.10 Policy measure 3E would be a system of threat level protocols, whereby a European, national, regional or local threat level would result in specified security activities (in Terms of Reference, see Table 6.1).

7.11 Policy measure 3F would be a system of liaison with relevant bodies, including the emergency services, supported by training in incident response, drills and exercises (in Terms of Reference, see Table 6.1).

7.12 We stress that no one policy measure, in itself, would completely meet objective 3, and so many of the six policy measures could be introduced independently. However, we conclude that:

- Policy measure 3D, relating to contingency reserves, could only be implemented if policy measure 3C, setting out contingency plans, was also implemented.
- Policy measure 3F, relating to liaison, incident response, drills and exercise, should only be implemented if policy measure 3E, a system of threat level protocols, was also implemented.

7.13 We discuss this contingency further in our discussion of options in Chapter 8.

Policy measure 3A: S/SMS ensure exchange of information by relevant parties

Table 7.9: Policy measure 3A: S/SMS ensure exchange of information by relevant parties

Characteristic	Details
Definition	The policy measure would mean: • To define parties required to have a Security Management System (SMS) • To require the inclusion of arrangements to ensure exchange of information with relevant agencies
Security interventions	None of the potential security interventions retained in Table 7.2 would be associated with this policy measure.
Parties required to take action	We consider that this policy measure would require action by any or all of infrastructure managers, station managers and railway undertakings, and indirectly by a potentially wide range of stakeholders including government, emergency services and "neighbours" of the railway.
Contribution to objective(s)	This policy measure was devised to contribute to objective 3, consistent risk assessment. It does not appear to contribute to any other objectives.
Scope and coverage	This policy measure, by its nature, would not be restricted to particular parts of the EU rail system and would involve exchanging information with relevant parties from any sector.
Mandatory, guidelines or best practice	We consider that this policy measure could be a mandatory part of an S/SMS.
Contingency	The policy measure could be introduced independently of other policy measures.

Source: Steer Davies Gleave analysis

Policy measure 3B: S/SMS recording of vulnerabilities and inspection regimes

Table 7.10: Policy measure 3B: S/SMS recording of vulnerabilities and inspection regimes

Characteristic	Details
Definition	The policy measure would mean: • To define parties required to have a Security Management System (SMS) • To require the inclusion of recording of vulnerabilities and inspection regimes
Security interventions	The following potential security interventions retained in Table 7.2 could be associated with this policy measure: • EA6: recording of vulnerabilities in asset register • PS4: inspection regimes
Parties required to take action	We consider that this policy measure would require action primarily by infrastructure managers but to a lesser extent by station managers.
Contribution to objective(s)	This policy measure was devised to contribute to objective 3, consistent risk assessment. It could also support: • Objective 1: shared EU understanding
Scope and coverage	This policy measure, by its nature, would not naturally be restricted to particular parts of the rail system, although recording of vulnerabilities and inspection regimes could both be limited to stations and infrastructure used by high-speed and international rail services.
Mandatory, guidelines or best practice	We consider that this policy measure could be a mandatory part of an S/SMS.
Contingency	The policy measure could be introduced independently of other policy measures.

Source: Steer Davies Gleave analysis

Policy measure 3C: S/SMS contingency planning and incident recovery

Table 7.11: Policy measure 3C: S/SMS contingency planning and incident recovery

Characteristic	Details
Definition	The policy measure would mean: • To define parties required to have a Security Management System (SMS) • To require the inclusion of contingency plans and plans for incident recovery
Security interventions	The following potential security interventions retained in Table 7.2 could be associated with this policy measure: • RP2: contingency planning • RP4: post-incident recovery
Parties required to take action	We consider that this policy measure would require action primarily by infrastructure managers and railway undertakings, and to a lesser extent by station managers, particularly at staffed or complex stations (see examples in Appendix D, Appendix Figures D.4-D.7), and third parties.
Contribution to objective(s)	This policy measure was devised to contribute to objective 3, consistent risk assessment. It could also support: • Objective 4: coordinated approach
Scope and coverage	This policy measure, by its nature, would not naturally be restricted to particular parts of the rail system, although contingency planning and incident recovery plans could be limited to high-speed and international rail services.
Mandatory, guidelines or best practice	We consider that this policy measure could be a mandatory part of an S/SMS.
Contingency	The policy measure could be introduced independently of other policy measures.

Source: Steer Davies Gleave analysis

Policy measure 3D: S/SMS contingency IT, communications and spares

Table 7.12: Policy measure 3D: S/SMS contingency IT, communications and spares

Characteristic	Details
Definition	The policy measure would mean: • To define parties required to have a Security Management System (SMS) • To require the inclusion of contingency plans and plans for incident recovery (as in 3C) • To include contingency communication systems, reserves and spares
Security interventions	The following potential security interventions retained in Table 7.2 could be associated with this policy measure: • EA14: resistant radio and communications systems • EA15: contingency IT and communication systems • PS3: targeted storage of contingency reserves
Parties required to take action	We consider that this policy measure would require action primarily by infrastructure managers, and to a lesser extent by station managers and railway undertakings. We would not expect that third parties would be required to have contingent systems or targeted storage of spares.
Contribution to objective(s)	This policy measure was devised to contribute to objective 3, consistent risk assessment. It could also support: • Objective 4: coordinated approach
Scope and coverage	This policy measure, by its nature, would not naturally be restricted to particular parts of the rail system, and it might be difficult to restrict resistant radio and communications systems, and contingency IT and communications systems, to parts of the network related to high-speed and international trains. It might, however, be possible to restrict the provision of contingency reserves to parts of the network related to high-speed and international trains.
Mandatory, guidelines or best practice	We consider that this policy measure could be a mandatory part of an S/SMS.
Contingency	We consider that this policy measure should only be introduced if policy measure 3C was also introduced, putting in place contingency and incident recovery plans and hence defining the need for communications and spares.

Source: Steer Davies Gleave analysis

Policy measure 3E: S/SMS threat level protocols

Table 7.13: Policy measure 3E: S/SMS threat level protocols

Characteristic	Details
Definition	The policy measure would mean: • To define parties required to have a Security Management System (SMS) • To require protocols for responding to threat levels defined at European, national, regional or local level
Security interventions	The following potential security interventions retained in Table 7.2 could be associated with this policy measure: • RP1: threat level protocols
Parties required to take action	We consider that this policy measure would require action primarily by infrastructure managers, station managers and railway undertakings.
Contribution to objective(s)	This policy measure was devised to contribute to objective 3, consistent risk assessment. It could also support: • Objective 4: coordinated approach
Scope and coverage	This policy measure, by its nature, would not naturally be restricted to particular parts of the rail system, although in principle the protocols could be limited to threats affecting high-speed or international rail services.
Mandatory, guidelines or best practice	We consider that this policy measure could be a mandatory part of an S/SMS.
Contingency	The policy measure could be introduced independently of other policy measures.

Source: Steer Davies Gleave analysis

Policy measure 3F: S/SMS liaison, incident response, drills and exercises

Table 7.14: Policy measure 3F: S/SMS liaison, incident response, drills and exercises

Characteristic	Details
Definition	The policy measure would mean: • To define parties required to have a Security Management System (SMS) • To require a system of liaison with relevant bodies, including the emergency services, supported by training in incident response, drills and exercises
Security interventions	The following potential security interventions retained in Table 7.2 could be associated with this policy measure: • EL1: partnership with third parties • EL2: liaison with emergency services • SR2: training in incident response • RP3: drills and exercises
Parties required to take action	We consider that this policy measure would require action primarily by infrastructure managers, station managers and railway undertakings, but also by third parties, such as emergency services and "neighbours" of the railway, who needed to take part in, or cooperate with, drills and exercises.
Contribution to objective(s)	This policy measure was devised to contribute to objective 3, consistent risk assessment. It could also support: • Objective 4: coordinated approach
Scope and coverage	This policy measure, by its nature, would not naturally be restricted to particular parts of the rail system, although in principle the requirements could be limited to threats affecting high-speed or international rail services.
Mandatory, guidelines or best practice	We consider that this policy measure could be a mandatory part of an S/SMS.
Contingency	We consider that this policy measure should only be introduced if policy measure 3E was also introduced, putting in place the threat level protocols to which the measure was intended to respond.

Source: Steer Davies Gleave analysis

Policy measures to contribute to objective 4: coordinated approach

7.14 We devised six policy measures to contribute to objective 4, coordinated approach:

- Policy measure 4A would installing CCTV on stations, with recording functionality and, where appropriate, facial recognition software and monitoring by train staff (in Terms of Reference, see Table 6.1).
- Policy measure 4B would installing CCTV on trains, with recording functionality and, where appropriate, facial recognition software (in Terms of Reference, see Table 6.1).
- Policy measure 4C would focus on deploying station staff, and to a lesser extent infrastructure staff, where they could observe behaviour on the railway.
- Policy measure 4D would focus on training station and on-train staff in risk and behaviour monitoring (in Terms of Reference, see Table 6.1).
- Policy measure 4E would focus on awareness promotion among passengers to encourage them to observe and report suspicious behaviour.
- Policy measure 4F would focus on minimising the risks associated with railway and third party staff, including combinations of staff vetting and access controls to sensitive areas.

7.15 We stress that no one policy measure, in itself, would completely meet objective 4, and that policy measures 4A and 4B related to CCTV could be introduced independently. However, we conclude that:

- Policy measure 4C, relating to deploying station and infrastructure staff, should only be implemented if policy measure 4A, installing CCTV on stations, was also implemented.
- Policy measure 4D, relating to training station and on-train staff in risk and behaviour monitoring, should only be implemented if policy measure 4C (and by implication 4B), was also implemented.
- Policy measure 4E, relating to awareness promotion among passengers, should only be implemented if policy measure 4D (and by implication 4C and 4B), was also implemented.

7.16 We discuss this contingency further in our discussion of options in Chapter 8.

Policy measure 4A: CCTV on stations, with recording and facial recognition

Table 7.15: Policy measure 4A: CCTV on stations, with recording and facial recognition

Characteristic	Details
Definition	The policy measure would mean: • To define standards for CCTV on stations including for recording and, optionally, for facial recognition and real time monitoring • To define responsibilities for each of these activities
Security interventions	The following potential security interventions retained in Table 7.2 could be associated with this policy measure: • EA2: minimisation of unseen areas (by ensuring that they were covered by CCTV) • EA9: facial or behaviour recognition technology • EA10: static detection equipment (CCTV)
Parties required to take action	We consider that this policy measure would require action primarily by infrastructure managers and station managers, although it is possible that bodies such as the police might be involved in any real time monitoring of CCTV.
Contribution to objective(s)	This policy measure was devised to contribute to objective 4, coordinated approach. It does not appear to contribute to any other objectives.
Scope and coverage	This policy measure could be restricted to stations served by high-speed or international trains, although except where these services use segregated areas it might not be practicable to limit CCTV, recording, recognition and any monitoring to high-speed and international passengers.
Mandatory, guidelines or best practice	We consider that this policy measure could be mandatory, although it would be possible to have a situation in which elements of the policy were optional but, if included, were subject to mandatory standards (such as the format of recordings or of facial recognition information).
Contingency	The policy measure could be introduced independently of other policy measures.

Source: Steer Davies Gleave analysis

Policy measure 4B: CCTV on trains, with recording and facial recognition

Table 7.16: Policy measure 4A: CCTV on stations, with recording and facial recognition

Characteristic	Details
Definition	The policy measure would mean: • To define standards for CCTV on trains including for recording and, optionally, for facial recognition (but not real time monitoring, for which bandwidth might not be available) • To define responsibilities for each of these activities
Security interventions	The following potential security interventions retained in Table 7.2 could be associated with this policy measure: • EA2: minimisation of unseen areas (by ensuring that they were covered by CCTV) • EA9: facial or behaviour recognition technology • EA10: static detection equipment (CCTV)
Parties required to take action	We consider that this policy measure would require action primarily by railway undertakings in the first instance. However, where rolling stock is not owned by the railway undertaking, responsibility might lie with rolling stock manufacturers or leasing companies.
Contribution to objective(s)	This policy measure was devised to contribute to objective 4, coordinated approach. It does not appear to contribute to any other objectives.
Scope and coverage	This policy measure could be restricted to trains used to provide high-speed or international service.
Mandatory, guidelines or best practice	We consider that this policy measure could be mandatory, although it would be possible to have a situation in which elements of the policy were optional but, if included, were subject to mandatory standards (such as the format of recordings or of facial recognition information).
Contingency	The policy measure could be introduced independently of other policy measures.

Source: Steer Davies Gleave analysis

Policy measure 4C: deploying staff where they can observe

Table 7.17: Policy measure 4C: deploying staff where they can observe

Characteristic	Details
Definition	The policy measure would mean: • To deploy staff, to the extent possible, in locations where they could observe behaviour on and around stations
Security interventions	The following potential security interventions retained in Table 7.2 could be associated with this policy measure: • SR5: staff deployment
Parties required to take action	We consider that this policy measure would require action by any parties whose staff were located on stations, including infrastructure managers, station managers and railway undertakings.
Contribution to objective(s)	This policy measure was devised to contribute to objective 4, coordinated approach. It does not appear to contribute to any other objectives.
Scope and coverage	This policy measure could be restricted to stations served by high-speed or international trains, although in practice staff deployed on stations would in many cases have access to, and be able to observe, all parts of a station.
Mandatory, guidelines or best practice	We consider that this policy measure could take the form of guidelines because it would not, in practice, be possible anyone other than the relevant employer to identify whether and how individual staff, in distinct roles, could be deployed in this way.
Contingency	We consider that this policy measure should only be introduced if policy measure 4A was also introduced, putting in place CCTV on stations as an initial measure before seeking to change staff roles and working practices.

Source: Steer Davies Gleave analysis

Policy measure 4D: training station and on-train staff in risk and behaviour monitoring

Table 7.18: Policy measure 4D: training staff in risk and behaviour monitoring

Characteristic	Details
Definition	The policy measure would mean: • To deploy staff, to the extent possible, in locations where they could observe behaviour on and around stations
Security interventions	The following potential security interventions retained in Table 7.2 could be associated with this policy measure: • SR5: staff deployment
Parties required to take action	We consider that this policy measure would require action by any parties whose staff were located on stations, including infrastructure managers, station managers and railway undertakings.
Contribution to objective(s)	This policy measure was devised to contribute to objective 4, coordinated approach. It does not appear to contribute to any other objectives.
Scope and coverage	This policy measure could be restricted to stations served by high-speed or international trains, although in practice staff deployed on stations would in many cases have access to, and be able to observe, all parts of a station.
Mandatory, guidelines or best practice	We consider that this policy measure could take the form of guidelines because it would not, in practice, be possible anyone other than the relevant employer to identify whether and how individual staff, in distinct roles, could be deployed in this way.
Contingency	We consider that this policy measure should only be introduced if policy measure 4A and 4C were also introduced, putting in place CCTV on stations, and deploying staff as observers, before giving staff training on risk and behaviour monitoring.

Source: Steer Davies Gleave analysis

Policy measure 4E: awareness promotion among passengers

Table 7.19: Policy measure 4E: awareness promotion among passengers

Characteristic	Details
Definition	The policy measure would mean: • To have campaigns to promote awareness of security among passengers • To identify standards for what information such campaigns should include
Security interventions	The following potential security interventions retained in Table 7.2 could be associated with this policy measure: • PS2: awareness promotion among passengers
Parties required to take action	We consider that this policy measure would probably need to be specified and led by national, regional or local governments, but might require the support of infrastructure managers, station managers and railway undertakings to display material or play announcements.
Contribution to objective(s)	This policy measure was devised to contribute to objective 4, coordinated approach. It does not appear to contribute to any other objectives.
Scope and coverage	This policy measure could be restricted high-speed or international trains, and stations served by them, although in practice an effective awareness campaign might make use of a wide range of media including advertising channels.
Mandatory, guidelines or best practice	We consider that this policy measure could take the form of guidelines because the most sensitive and effective means of promoting awareness may vary between Member States and between locations within a Member State.
Contingency	We consider that this policy measure should only be introduced if policy measure 4A and 4C were also introduced, putting in place CCTV on stations, deploying staff as observers, and giving staff training on risk and behaviour monitoring, before expecting passengers to become involved.

Source: Steer Davies Gleave analysis

Policy measure 4F: staff vetting and access controls

Table 7.20: Policy measure 4F: staff vetting and access controls

Characteristic	Details
Definition	The policy measure would mean: • To put in place measures for the vetting of some or all staff working on, or having access to, railway infrastructure, stations and trains • At secure or sensitive locations, to ensure that entry was limited to authorised staff
Security interventions	The following potential security interventions retained in Table 7.2 could be associated with this policy measure: • SR3: staff vetting
Parties required to take action	We consider that this policy measure might need to be applied to some or all staff employed by infrastructure managers, station managers and railway undertakings and by third parties having access to secure or sensitive areas of infrastructure, stations or trains.
Contribution to objective(s)	This policy measure was devised to contribute to objective 4, coordinated approach. It does not appear to contribute to any other objectives.
Scope and coverage	This policy measure could be restricted to staff working on, or with access to, high-speed or international trains, or to infrastructure and stations used by them, although in practice this might need to include a large proportion of all railway industry employees and a large number of third parties including those stocking, maintaining and repairing stations and trains.
Mandatory, guidelines or best practice	We consider that this policy measure could take the form of guidelines because the vetting processes and identification protocols might need to reflect local identity databases, documents and procedures.
Contingency	We consider that this policy measure should only be introduced if policy measure 4A and 4C were also introduced, putting in place CCTV on stations, deploying staff as observers, and giving staff training on risk and behaviour monitoring, before expecting passengers to become involved.

Source: Steer Davies Gleave analysis

Summary

7.17 Table 7.21 summarises the mapping of security interventions to policy measures and also identifies which of the specific objectives in Table 5.1 each measure was intended to address (●) and would also address as a by-product (+). The Commission instructed us that we were to identify a preferred policy option which must contain measures which contribute to all specific objectives, which has two implications:

- We do not assess any individual security interventions, or policy measures, because none of them contribute to all the specific objectives.
- It is necessary for us to assemble policy options, which do contribute to all the specific objectives, from a number of different security interventions, or policy measures.

7.18 We discuss how we assembled the policy measures into policy options next, in Chapter 8.

Table 7.21: Summary: mapping of security interventions to policy measures

Policy measures	Contingent on	Approach		Security interventions from Chapter 6	Parties required to take action					Other objectives addressed			
		Mandatory	Guidelines		Government	Infrastructure manager	Station manager	Railway undertaking	Third parties	Shared EU understanding	Reflect EU-wide benefits	Consistent risk assessment	Coordinated approach
1: shared EU understanding													
1A	-	M		-	●	+	+	+		●	+	+	
1B	1A		G	-	●	+	+	+		●	+	+	
2: reflect EU-wide benefits													
2A	-		G	EA3, EA4		●	●				●		
2B	-		G	EA1 (stations)		●	●				●		
2C	-		G	EA1 (trains)				●	●		●		
3: consistent risk assessment in an S/SMS													
3A	-	M		-	+	●	●	●	+			●	
3B	-	M		EA6, PS4		●	+			+		●	
3C	-	M		RP2, RP4		●	+	●	+			●	+
3D	3C		G	EA14, EA15, PS3		●	+	+				●	+
3E	-		G	RP1		●	●	●				●	+
3F	3E		G	EL1, EL2, SR1, RP3		●	●	●	●			●	+
4: coordinated approach													
4A	-	M		EA2, EA9, EA10 (stations)		●	●						●
4B	-	M		EA2, EA9, EA10 (trains)				●	●				●
4C	4A		G	SR5		●	●	●					●
4D	4C		G	SR1		●	●	●					●
4E	4D		G	PS2	●	+	+	+					●
4F	-		G	SR3		●	●	●	●				●

Source: Steer Davies Gleave analysis.
Note ● shows the objective the measure was intended to address, + shows other objectives it would help address.

8 Potential policy options

Introduction

8.1 Tool #14 of the Better Regulation "Toolbox", "How to identify policy options", opens with a statement that:

*Identifying **alternative** policy options is, in most cases, an iterative process. The aim is to consider as many realistic alternatives as possible and then narrow them down to the most relevant ones for further analysis.*

8.2 We have emphasised the word "alternative", which implies that policy options must be mutually exclusive alternatives, unlike the policy measures described in Chapter 7, all of which could in principle be implemented.

8.3 We therefore adopted an approach of packaging the policy measures into three distinct options, with progressively greater degrees of intervention:

- Option 1: a minimal package, designed to make at least some contribution to addressing each objective.
- Option 2: intermediate package, incorporating additional policy measures, including some which we had identified as contingent on the policy measures in Option 1.
- Option 3: a comprehensive package, incorporating all the policy measures in Table 7.21.

8.4 Each successive Option should result in an incremental improvement in security of high-speed and international rail services relative to the baseline, but even Option 3, incorporating all the policy measures we have devised, would not eliminate all the many security issues identified in the baseline.

8.5 Our proposed options are set out in Table 8.1.

Table 8.1: Policy options

Option 1: minimal	Option 2: intermediate	Option 3: comprehensive	Policy measure		Mandatory/guidelines	Security interventions from Chapter 6
●	●	●	1A	Reporting and monitoring national security data	M	
		●	1B	Researching and disseminating worldwide security data	G	
●	●	●	2A	Emergency egress and access to stations	G	EA3, EA4
		●	2B	Blast-resistant features on stations	G	EA1
		●	2C	Blast-resistant features on trains	G	
●	●	●	3E	S/SMS threat level protocols	G	RP1
	●	●	3A	S/SMS ensure exchange of information by relevant parties	M	
	●	●	3C	S/SMS contingency planning and incident recovery	M	RP2, RP4
	●	●	3F	S/SMS liaison, incident response, drills and exercises	G	EL1, EL2, SR1, RP3
		●	3B	S/SMS recording of vulnerabilities and inspection regimes	M	EA6, PS4
		●	3D	S/SMS contingency IT, communications and spares	G	EA14, EA15, PS3
●	●	●	4A	CCTV on stations, with recording and facial recognition	M	EA2, EA9, EA10
●	●	●	4B	CCTV on trains, with recording and facial recognition	M	
	●	●	4C	Deploying staff where they can observe	G	SR5
	●	●	4F	Staff vetting and access controls	G	SR1
		●	4D	Training station/train staff in risk and behaviour monitoring	G	PS2
		●	4E	Awareness promotion among passengers	G	SR3

Source: Steer Davies Gleave analysis

8.6 Table 8.2 shows how Options 2 and 3 build incrementally on Option 1.

Table 8.2: Policy option increments

Policy measures included		Mandatory/guidelines	Security interventions from Chapter 6
Option 1: minimal includes …			
1A	Reporting and monitoring national security data	M	
3E	S/SMS threat level protocols	G	RP1
2A	Emergency egress and access to stations	G	EA3, EA4
4A	CCTV on stations, with recording and facial recognition	M	EA2, EA9, EA10
4B	CCTV on trains, with recording and facial recognition	M	
Option 2: intermediate also includes …			
3A	S/SMS ensure exchange of information by relevant parties	M	
3C	S/SMS contingency planning and incident recovery	M	RP2, RP4
3F	S/SMS liaison, incident response, drills and exercises	G	EL1, EL2, SR1, RP3
4C	Deploying staff where they can observe	G	SR5
4F	Staff vetting and access controls	G	SR1
Option 3: comprehensive also includes …			
1B	Researching and disseminating worldwide security data	G	
3B	S/SMS recording of vulnerabilities and inspection regimes	M	EA6, PS4
3D	S/SMS contingency IT, communications and spares	G	EA14, EA15, PS3
2B	Blast-resistant features on stations	G	EA1
2C	Blast-resistant features on trains	G	
4D	Training station/train staff in risk and behaviour monitoring	G	PS2
4E	Awareness promotion among passengers	G	SR3

Source: Steer Davies Gleave analysis

8.7 In Chapter 9 we describe our approach to assessing the impact of these Options.

9 Approach to impact assessment

Introduction

9.1 This chapter describes in detail our approach for analysing the impacts of the three options listed in Chapter 8.

9.2 Our approach to assessment took into account a number of challenges arising from the nature of railway security, the options we have put forward to assess, and the availability of evidence, which we summarise in Table 9.1 below.

Table 9.1: The assessment challenge

Section	Issue	Example of issue or outcome
2	Lack of data on the scale of high-speed and international rail services.	Scale of existing services has been estimated with varying degrees of confidence (see Table 2.3).
	Lack of segregation between rail services in scope and out of scope.	High-speed and international rail services are not normally segregated from other services, with rare exceptions such as Eurostar (see paragraph 4.16), making it difficult to restrict security interventions to these services.
	Risk that major security interventions will result in service cutbacks.	For example, identity checks at Sweden have already resulted in around one in sixteen (6%) of all cross-border services being withdrawn (see paragraph 2.29).
	Further uncertainty if options include flexibility to avoid disproportionate interventions.	Flexibility, for example linked to a risk assessment, could reduce the costs of options but also their effectiveness. In an extreme case, measures might only apply in full to Eurostar, which carries one in six passengers across EU borders.
3	Extremely small scale of historic terrorism on high-speed and international rail services.	Cost-Benefit Analysis (CBA) based on historic data would not support any major intervention.
	Lack of data on other rail services.	We have not investigated the large majority of rail services which are out of scope, or the cost or effectiveness of extending security interventions to the whole network.
	Lack of data or evidence on other security failures, other than metal and cable theft, vandalism and graffiti.	Interventions intended to reduce terrorism would probably also reduce other crime (see Table 3.1 for examples) but we have no data on either the cost of such crime or the effectiveness of terrorist-focused interventions in reducing it.
4	Difficulty of defining a problem, or drivers, which cover all aspects of crime on the railway.	The problem tree set out in Figure 4.2 is necessarily generic, given the large number of security failures found on the railway.
	Heterogeneity of security risks and security interventions between and within Member States, which cannot readily be quantified as a "baseline".	It is difficult to characterise the effectiveness of existing or potential interventions, or the net difference between them (see Figure 6.2 and paragraph 6.91).
6-8	Difficulty of identifying what security interventions and policy measures are currently in place.	We have not been able to discuss all the security interventions with stakeholders in all Member States and, even if we had, it would be difficult to quantify the extent to which they are currently applied .
	Difficulty of defining security interventions, policy measures and policy options in sufficient detail to enable assessment.	We have described security interventions, policy measures and policy options at a conceptual level, but this is insufficient to identify exactly how they would be defined and implemented.
	Absence of evidence of the costs of interventions.	Stakeholders provided little information on the costs of interventions, many of which are highly specific to the exact location and approach to implementation.
	Absence of evidence of the impacts of interventions.	Stakeholders provided almost no information on the effectiveness of existing or potential interventions, except where these were demonstrably ineffective (such as with requiring terrorists to put a ticket through a barrier, see 6.31).
8	Policy options must contribute to all specific objectives.	Assessment cannot be based on a single security intervention or policy measure, no matter how strong the evidence for it, if it does not contribute to all the specific objectives in Table 5.1.

Source: summary of analysis earlier in this Report.

9.3 We discuss those issues that have proved particularly difficult to resolve in turn below.

Lack of data on the scale of high-speed and international rail services

High-speed rail services

9.4 The Terms of Reference refer to "security interventions for high-speed passenger railway services within Europe", and by implication to "the existing EU definition of high-speed" (see Figure 2.8). However, we concluded that this definition is both too broad and too easy to evade to be workable, and instead suggested two working definitions of high-speed (see paragraph 2.48):

- Greater than 260 km/h, sufficiently high to exclude 250 km/h services in Austria, but sufficiently low to include all operation at 300 km/h or more by the Alstom TGV and Siemens ICE families of trains.
- Greater than 210 km/h, sufficient also to include 250 km/h services in Austria, 225 km/h services in the UK with Hitachi "Javelin" trains, and 220 km/h services in Finland and Portugal with Fiat (now Alstom) "Pendolino" trains.

9.5 Even with this clarification of the definition, however, it is not clear whether the definition of high-speed services include:

- all services operated by stock capable of these speeds;
- only services scheduled to pass, at some part of the journey, over infrastructure supporting these speeds; or
- only station-to-station arcs over infrastructure supporting these speeds.

9.6 Unless the first definition was adopted, actors might be able to limit the definition of high-speed services merely by subdividing existing end-to-end train services into different train numbers. Actors might also limit the impact of interventions by "de-rating" stock so that it was no longer officially capable of speeds at which a requirement would be triggered.

International rail services

9.7 The Terms of Reference refer to "security interventions for international passenger railway services within Europe", but the definition of an international passenger railway service also seems both problematic and open to manipulation. We assumed in our analysis that international rail services include any service, operated with a single train number, which crosses one or more international borders. However, this need not be the case. As we noted above (see 2.19):

- If this definition was adopted, railway undertakings could change train numbers so as to limit the scope of "international services" to the journey between stations immediately before and after the border.
- A definition could be adopted that a service ceases to be international once it has entered the last state in its journey. For example, some Eurostar services from London to Paris are treated as domestic French services between Lille and Paris. In this case we would expect that approximately half of all current "international" station calls estimated in Table 2.3 would be, or could be, redefined as domestic.
- In addition, some trains are not considered "international" before the last stop before the border. This is the case where "services" into Sweden, carrying one in twelve are now effectively domestic-only services within Denmark (see Table 4.6).

9.8 This imprecision in the definition of international services would be important if railway actors were required to apply additional security to "international" trains, because in many cases it

would be possible to adopt a more limited definition of the international service, with the objective of reducing compliance costs, without any reduction in the underlying security risk.

Open networks and unstaffed stations

9.9 Many rail networks are open systems, in some cases specifically to allow passengers to board and pay on the train (such as with open access operator Westbahn). Others specifically welcome those who have no intention of travelling, including those seeing of or meeting passengers, and those buying tickets for or making enquiries about future travel, but also those using toilets, restaurants, shops and other facilities, or even using the station as a right of way. Many stakeholders were reluctant to change the existing extent of open access.

9.10 In addition, and as shown in Figure 2.1 and Figure 2.2, many stations served by high-speed and international rail services are remote, unattended and open much or all of the time, and it is not clear what security interventions could be applied at them. Similarly, many trains, including a number of trains operating at more than 200 km/h, are unstaffed except for the driver. Others, as we noted above, may operate from open stations with a "pay on board" facility. Either arrangement constrains the scope to implement security interventions on trains.

9.11 More generally, we did not attempt to estimate the length of infrastructure used by high-speed and international trains but, as with stations, much of it may be remote and rarely supervised. Even relatively intensively-used infrastructure in France suffers from frequent incidents of objects being placed on the track. Despite patrolling and research into drones, much infrastructure is unsupervised for most of the time, and vulnerable to attack from objects or vehicles being placed on the track.

Lack of segregation of between rail services in scope and out of scope

9.12 Neither international services nor high-speed services are routinely segregated from other services, and it would often be impracticable or at least extremely costly to do so:

- In Belgium, Denmark and Portugal, we were told that further segregation was impossible, on capacity grounds.
- In Sweden, we were told that further segregation was impossible in the short to medium term, and expensive in the longer term.
- In Slovenia, further segregation was described as very difficult.
- In Hungary, further segregation was described as inefficient.

9.13 This means that many options or measures intended to improve security for international or high-speed services might necessarily also need to be applied to a range of other services, which we have not been able to quantify. Apart from the additional costs of a poorly-targeted measure, we anticipate that this could lead to legal issues in some Member States. For example, the proposal in Option 1 that those boarding international trains were recorded on CCTV, and identifiable or identified through facial recognition software, might be legally problematic if domestic passengers using the same platform were also identifiable or identified.

9.14 In the absence of detailed studies of individual services, however, we have no basis on which to predict the extent to which any of the policy options would either require new measures to segregate services, or require that some or all of the security interventions in the policy option would be extended to other services.

Risk that security interventions will result in service cutbacks

9.15 Railway undertakings, or competent authorities contracting services under a PSO, which were required to implement, or pay for others to implement, security measures related to trains defined as "high-speed" or "international" (9.4 to 9.8), or other services from which they could not be segregated (9.14) would have incentives to minimise the range of services subject to the costs of these interventions. This could be achieved by mechanisms such as those listed in Table 9.2:

Table 9.2: Strategies for evading requirements for high-speed or international rail services

High-speed service	International service
Withdraw services	Withdraw services
De-rate rolling stock to evade definition of high-speed	
	Treat trains as domestic after crossing the (last) border
Renumber trains at start and end of high-speed line	Renumber trains at start and end of cross-border arc
Impose connection at start and end of high-speed line	Impose connection at start and end of cross-border arc
	Impose connection at a border station

Source: Steer Davies Gleave analysis.
Note: "Arc" refers to a journey between consecutive station calls on the same train service.

9.16 Similar issues would also arise in relation to any measures applied to rolling stock or staff, including third party staff, who fell within the scope of security interventions because they were used to provide (or had access to infrastructure, stations and trains used to provide) high-speed or international rail services. We would expect IMs, station managers, RUs and other parties to exploit any scope to limit additional interventions to a pool of rolling stock and staff dedicated to high-speed and international rail services. The extent to which this would prove practicable would depend on the practicability and cost of creating separate pools of "in scope" and "out of scope" rolling stock and staff.

9.17 In the absence of detailed studies of individual services, however, we have no basis on which to predict the extent to which any of the policy options we have devised would result in reductions in high-speed or international rail services.

Uncertainty if there is flexibility to avoid disproportionate interventions

9.18 Some of the retained policy measures include a degree of flexibility that would allow the relevant delivery body to implement the measure in a proportionate and context-specific manner. For example, implementation of S/SMS recording of vulnerabilities and inspection regimes (policy measure 3B) could involve a site-specific risk assessment to identify which elements of the railway estate are most susceptible to security breaches, and a regime designed to ensure that the frequency, rigour and visibility of inspection is proportionate to the likelihood and impact of a security breach.

9.19 In the absence of detailed information regarding the extent of flexibility that may be permitted, and the willingness of delivery bodies to identify proportionate, context-specific actions in response to new requirements, it is not possible to identify with any precision the costs and benefits associated with such policy measures.

The small scale of historic terrorism

9.20 We estimated in paragraph 3.44 how, on a strict definition of terrorism and high-speed and international rail services, the average annual cost of terrorism on high-speed and international rail services over the 40-year period ending in 2015 has been around €0.2 million. On this basis, security interventions to reduce the cost of terrorism further would only pass a cost-benefit test unless they were both relatively cheap and effective[61]. To support intervention at the EU level, it would therefore be necessary either:

- To identify benefits from terrorism-related interventions in other security areas, such as reduction in metal and cable theft, vandalism and graffiti, or other crime.
- To demonstrate that terrorism-related security interventions would result in increased confidence and increased travel.
- To demonstrate that extension of interventions from high-speed and/or international rail services to other services would add create sufficient benefits to outweigh the costs.
- To use an alternative to cost-benefit analysis which takes better account of the small risk of a high impact terrorist attack.

9.21 Tool 12 of the Better Regulation Toolbox ("Risk Assessment and Management") provides some guidance on how to take account of risk[62], and notes that risk assessments are carried out in a wide range of policy areas including security. It states that such risk assessments can support different types of policy decisions or actions taken by the Commission, either on a standalone basis or by feeding into the Impact Assessment process. It also states that the significance of risk can be determined by the so-called risk (or tolerability) criteria, which may range from scientifically identified tolerable thresholds to societal values (for example related to equity or personal freedom considerations). The risk criteria may be defined by the existing legal basis or, more generally, by an existing risk management approach and past experience.

9.22 Another approach to the management of risk is ALARP or "As Low As Reasonably Practicable", mentioned by stakeholders in the Netherlands (see D.324) and Germany (see D.472), and also used in rail safety in Great Britain. One extreme interpretation of this principle would be that any security interventions which has been deemed reasonably practicable anywhere in the EU should be adopted throughout the EU, as has happened, for example, with many security interventions for aviation, such as limited fluids taken airside at airports to 100 millilitres per passenger. In practice, ALARP can be tied to a risk assessment which takes into account the proportionality of applying an intervention in any particular situation. However, ALARP necessarily depends on a definition of "reasonable" which is inevitably a societal judgement.

9.23 Notwithstanding these challenges, we have concluded that there is sufficient information available, including from published sources and stakeholder consultation responses, to enable an assessment of the impacts of policy options based on cost-benefit analysis (CBA). Given the lack of relevant quantified data, however, we also combined a number of qualitative assessments and combined them with the quantified analysis in a Multi-Criteria Analysis (MCA). More generally, we note that in order to assess all of the impacts included in the Terms of Reference it has been necessary to make assumptions that cannot be based on

[61] To achieve a benefit-cost ratio of 1, a measure which halved the economic impact of terrorism on high-speed and international rail services would have to cost on average no more than €4,000 per annum per Member State.

[62] "Risk" in the context of risk assessment explained here presents a result of natural or manmade hazards. We have assumed that terrorism and crime can be considered to be manmade hazards.

independent, documented sources. These, together with our other assumptions, are identified in Appendix E.

The lack of data on other security failures

9.24 Table 3.1 illustrates how security, broadly-defined, covers an extremely wide range of violent and non-violent crime on the railway. The problem tree shown in Figure 4.2 is not specifically limited to the problem of terrorism, and policy options intended to address the objectives we have derived from it might also provide benefits in reduction of non-terrorist crime. However, we have found no consistent data either on the overall level of crime on the railway or on the extent to which security interventions aimed at one type of crime would reduce the frequency or impact of other types of crime.

The cost of interventions

9.25 A further issue for impact assessment is determining the costs of individual security interventions. We discussed costs with stakeholders during the workshop in Germany, but they pointed out that organisation charts do not show a "Terror Department" and budgets do not show a "Terrorism prevention" line, and that awareness is important but does not appear as a cash item (see Appendix D, D.235).

9.26 We have sought other evidence of the costs of particular security interventions, but in practice these vary widely with the local environment and approach to implementation. As examples:

- We were told that passenger and baggage screening staff cost €2.5 million per annum for the operation at one platform at Paris Gare du Nord (see 6.36). However, we have seen screening achieved by a single individual at stations on RENFE's AVE network, and would expect that associated cost is a small fraction of this amount, and have also made our own lower estimates of the costs of screening on the Außerfernbahn (see 6.37).
- Network Rail's Long Term Charge for stations, which can be seen as a broad proxy for the complexity of the station, varies by a factor of over 2,000 between stations[63].

9.27 In consequence we stress that, even where we have been able to obtain cost estimates, they must be seen as subject to a wide variation with location and purpose.

9.28 A related issue is the consequential costs, for RUs and/or passengers, of introducing security interventions, particularly where these restrict operational flexibility. Stakeholders pointed out that many elements of the railway are already at their operational limits and rely, in particular, on flexibility for different types of train to share a platform (as at Brussels Midi, see 4.69), or on both trains and passengers passing through stations as quickly as possible (as at the Köln Hauptbahnhof, see 6.28). Even a few additional seconds delay may disrupt or prevent the operation of the current timetable, with the immediate impact of a loss of capacity, as the imposition of identity checks on passengers entering Sweden shows (see Table 4.6).

The impacts of interventions

9.29 To carry out an impact assessment of options also requires estimates of the impacts of security interventions. In practice, it is relatively easy to estimate the large impacts on passengers of interventions which delay them. For example:

[63] CP5 Long Term Charges for Franchised Stations - Network Rail, for the period 2014 to 2019. Highest charge is £1,310,910 and lowest charge is £627.

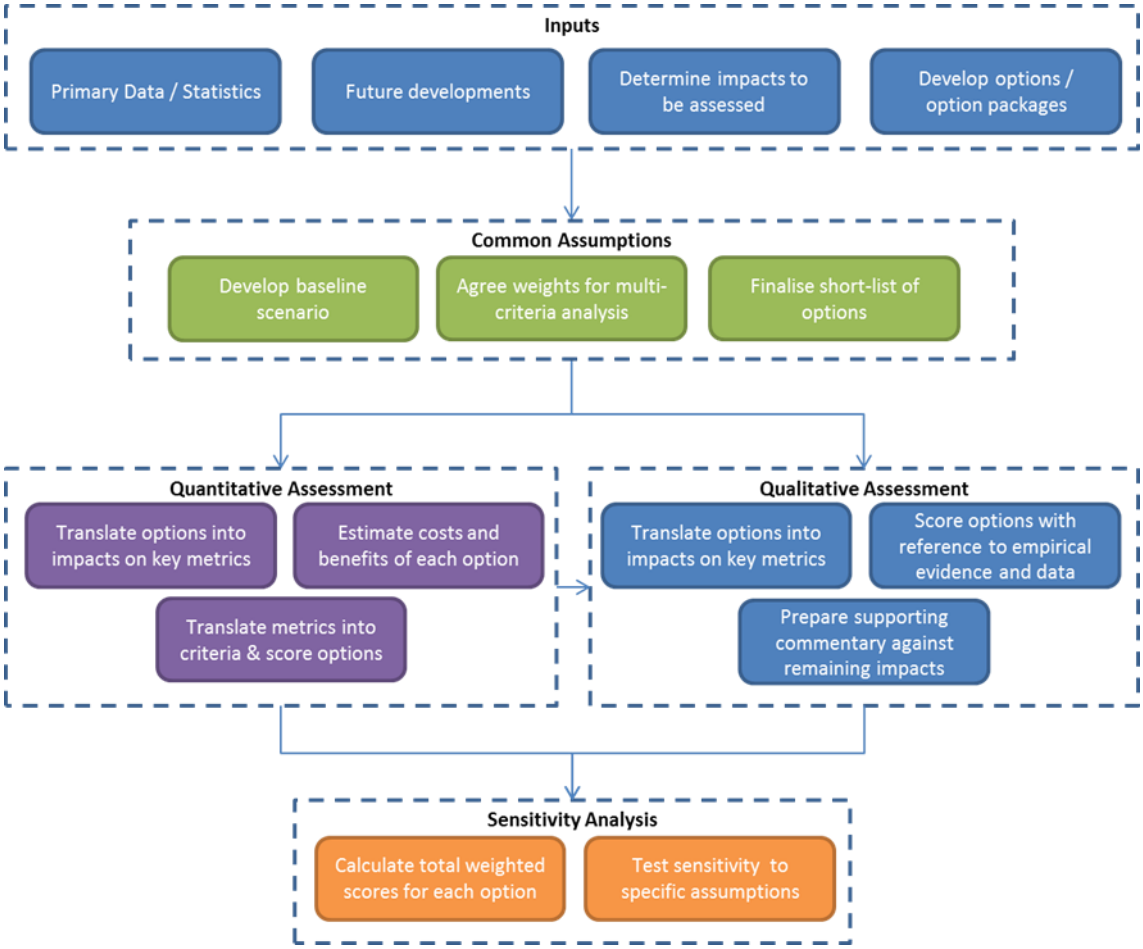
- Tools exist to estimate how passengers are delayed and deterred by station ticket barriers or passenger and baggage screening, but both these measures were rejected in our initial sift (see Table 6.8).
- Tools exist to estimate how passengers are delayed and deterred by RUs replacing through services by connections (see Table 9.2), but not whether any particular RU would choose, or be permitted, to do so with any given service.

9.30 We have, however, been offered no evidence on the effectiveness of any individual security measure in detecting, deterring or mitigating the impact of terrorist crime, which is in any case only a small average annual cost, as we identified above. We discussed the effectiveness of security interventions with stakeholders in Germany, who informed us that they could provide statistics on rates of crime, and their interpretation of how security interventions had affected them, but did not collect sufficient data to assess the social or economic costs of the crimes prevented, deterred or mitigated by interventions.

Overview of our approach

9.31 Our approach to assessing the costs and benefits of policy options is summarised in Figure 9.1.

Figure 9.1: Overview of assessment methodology



9.32 Notwithstanding the challenges presented in the previous section, and where the evidence permits, we have sought to quantify as many impacts of policy options as possible. In some cases, it has then been possible to place a monetary value on a subset of those impacts.

Where there is insufficient evidence to quantify impacts, we have carried out a qualitative assessment of the scheme impacts. Again, where the evidence permits we have sought to codify the qualitative assessment by allocating a 'score' to distinguish the relative impact of policy options. Where there is insufficient evidence to determine a relative score a simple commentary regarding the relative performance of policy options is provided.

9.33 The range of impacts to be assessed was specified within the Terms of Reference for the study. Following a review of the 30 separate economic, social and environmental impacts suggested in the Terms of Reference we concluded these to be sufficiently comprehensive for the purpose of this Impact Assessment. We then screened the impacts to determine how they should be assessed and drew conclusions regarding the most appropriate methodology on the basis of the proportionality principle described in the Better Regulation Toolbox (Tool #9) and with reference to[64]:

- the significance of the expected (intended and unintended) impacts;
- the nature of the options under consideration;
- the maturity of the markets through which options will be delivered, such as security equipment suppliers, enterprise-level risk assessments, staff training; and
- the availability of reliable evidence regarding monetary valuations for non-market impacts (such as travel time savings), direct and indirect behavioural responses and contextual data to inform the qualitative assessment.

9.34 Table 9.3 below presents the results of this exercise and describes the methodology used to assess each of the impacts.

Table 9.3: Assessment methodology by impact

Impact		Quantitative		Qualitative	
		Monetised	Quantified	Objective Score	Commentary
Economic Impacts					
1	What impact (positive or negative) does the option have on the free movement of goods, services, capital and workers?	✓			
2	Will it lead to a reduction in consumer choice, higher prices due to less competition, the creation of barriers for new suppliers and service providers, the facilitation of anti-competitive behaviour or emergence of monopolies, or market segmentation?			✓	
3	Does it affect the nature of information obligations placed on businesses (for example, the type of data required, reporting frequency, the complexity of submission process)?		✓		
4	What is the impact, if any, on Small and Medium Enterprises?		✓		
5	Does it bring additional governmental administrative burden and costs?	✓			

[64] The proportionality principle involves setting an appropriate scope and depth for the overall analysis, including the resources and time allocated to the Impact Assessment process, the relative effort required to answer each of the Impact Assessment key questions, and the specific focus of each step of the analysis

Impact		Quantitative		Qualitative	
		Monetised	Quantified	Objective Score	Commentary
6	Does the option require the creation of new or restructuring of existing public authorities?				✓
7	Does the option stimulate or hinder research and development?			✓	
8	Does it facilitate the introduction and dissemination of new production methods, technologies and products?			✓	
9	Does the option affect the prices consumers pay for the service?	✓			
10	Does it impact on consumers' ability to benefit from the internal market?		✓		
11	Is there a single Member State or region which is disproportionately affected?		✓		
12	What are the impacts on third neighbouring countries with which the EU has close trade, transport or free movement i.e. Schengen links?			✓	
13	Does the option concern an area in which international standards, common regulatory approaches or international regulatory dialogues exist?				✓
14	Does it have overall consequences of the option for economic growth and employment?	✓			
Social Impacts					
15	Does the option directly or indirectly facilitate new job creation or loss of jobs?	✓			
16	Does it have specific consequences for particular types of workers or does it affect particular groups or people such as the disabled or of different ages?			✓	
17	Does the option impact on job quality or affect the access of workers to vocational or continuous training?				✓
18	Will it affect workers' health, safety and dignity?			✓	
19	Does the option directly or indirectly affect workers' existing rights and obligations, in particular as regards information and consultation within their undertaking and protection against dismissal?				✓
20	Does it directly or indirectly affect employers' existing rights and obligations?				✓
21	Does the option facilitate or restrict restructuring, adaptation to change and the use of technological innovations in the workplace?				✓
22	Does the option affect the right of citizens to move freely within the EU?		✓		
23	Does the option impact on cultural diversity?				✓
24	Does the implementation of the proposed measures affect public institutions and administrations, for example in regard to their responsibilities?				✓
25	Can the security effectiveness of the options be measured in respect to deterring or even detecting crime or terrorism?	✓			
26	Are there any unintended negative consequences of introducing such options that may detrimentally impact upon either the safety or privacy of the passenger or staff?			✓	
27	What are the additional resources that the introduction of such an option would require both in terms of people (railway staff, law enforcement capacity) and associated cost?	✓			
28	Does the introduction of such an option impact on the rights to liberty, security, defence and a fair trial for individuals, such as victims, witnesses and others using the railways?				✓

Impact		Quantitative		Qualitative	
		Monetised	Quantified	Objective Score	Commentary
Environmental Impacts					
29	Will the option increase or decrease the demand for passenger transport or influence its modal split?		✓		
30	Will the option increase/decrease energy and fuel needs/consumption?	✓			

Source: Steer Davies Gleave analysis

9.35 Regardless of the analytical approach used, each of the three policy options is assessed relative to the baseline described in paragraphs 4.112 to 4.122.

Quantitative assessment

9.36 Security breaches (and terrorism incidents in particular) can have significant consequences for both victims and society in general. Understanding the scale and distribution of these impacts has taken an increasingly prominent role in the literature and can be used to guide policy decisions in order to maximise the benefits derived from the use of financial resources in providing security.

9.37 In developing our approach to quantitative assessment, we have classified these impacts (both costs and benefits) as follows:

- **Direct** impacts are those that take place as an immediate result of an attack or incident, such as damage to buildings and property, loss of life and injuries.
- **User** impacts arise from a change in the behaviour of the economic system as a consequence of the attack, such as changes in travel habits following the introduction of policy options.
- **Non-user** impacts are further indirect effects realised by society, such as emissions reductions arising from mode-shift to less polluting modes such as rail.

9.38 Further detail regarding the analytical framework used to assess impacts in each of these categories is described below.

Direct impacts

9.39 In Chapter 4, we describe the current situation and projected security baseline scenario in terms of the assumed frequency and impact of security failures, and the monetary value placed upon them. Any improvements to security achieved through the implementation of policy options will have a direct impact on the likelihood and/or severity of an attack. In turn, this will produce an estimate of the future pattern of incidents and impacts by train service. The difference between the baseline and 'policy option' impacts therefore provides a measure of the direct impacts of the option, including estimates of:

- reductions in the severity of incidents;
- reductions in the numbers of incidents; and
- reductions in direct costs of repair and recovery.

9.40 Baseline security failure costs in each Member State combine the impact of terrorism incidents, cable theft and vandalism of infrastructure. Our method for calculating each of

these is described in paragraphs 4.115. In summary, we have assumed the cost of vandalism (expressed in real terms(is fixed throughout the assessment period, although the value of a statistical life and the cost of cable theft (which affects journey reliability) is assumed to grow in line with GDP per capita. Turning to the assessment of 'policy options', assumptions regarding the reduction in the frequency and severity of security breaches are presented in Table 9.4 below.

Table 9.4: Reduction in frequency and severity of incidents by security intervention

Ref	Security Intervention	Frequency	Severity	Total
EA1	Resistance to blast	15.0%	33.0%	43.1%
EA2	Minimisation of unseen areas	15.0%	15.0%	27.8%
EA3	Facilitation of emergency egress	-	33.0%	33.0%
EA4	Duplicated access routes and walkways	-	33.0%	33.0%
EA6	Recording of vulnerabilities in asset registers	10.0%	-	10.0%
EA9	Facial and behavioural recognition technology	15.0%	-	15.0%
EA10	Static detection equipment	15.0%	15.0%	27.8%
EA11	Mobile detection equipment	20.0%	-	20.0%
EA14	Resistant radio systems	-	15.0%	15.0%
EA15	Contingency IT and communications systems	-	15.0%	15.0%
EL1	Partnership arrangements with third parties	-	-	0.0%
EL2	Partnership arrangements with emergency services	-	-	0.0%
PS2	Awareness promotion among passengers	15.0%	15.0%	27.8%
PS3	Targeted storage of contingency resources	-	5.0%	5.0%
PS4	Inspection regimes	33.0%	-	33.0%
RP1	Threat level protocols	15.0%	-	15.0%
RP2	Contingency plans	-	25.0%	25.0%
RP3	Drills and exercises	-	25.0%	25.0%
RP4	Post-incident recovery	-	25.0%	25.0%
SR1	Training in risk and behaviour monitoring	33.3%	-	33.3%
SR2	Training in incident response	-	25.0%	25.0%
SR3	Vetting of staff	25.0%	-	25.0%
SR5	Staff deployment	10.0%	10.0%	19.0%

Source: Steer Davies Gleave assumptions

9.41 In the absence of systematic, observed evidence regarding the relative performance of security interventions on reducing the frequency and severity of security breaches, there is no empirical basis for the assumptions in Table 9.4. The relative and absolute performance of some security interventions is, however, informed by the outputs of the SECURESTATION study on *Passenger Station and Terminal Design for Safety Security and Resilience to Terrorist Attack*. In particular, the *Socio Economic Potential Impact* report describes the reduction in direct and indirect costs of a hypothetical terrorist incident associated with packages of countermeasures (or security interventions within the nomenclature of this study).

9.42 In light of the lack of evidence upon which to base the assumptions described in Table 9.4, we have also presented the results of sensitivity tests in which the changes in likelihood and

severity of security breaches is 50% larger and 50% smaller. We have not considered sensitivity tests in which the relative performance of individual security interventions varies.

9.43 We note that some measures might have negative benefits if, for example:

- they artificially created congestion points or crowds which would, potentially, present a more concentrated target than exists in the status quo; or
- they diverted or displaced threats to other locations or activities (such as from a lightly-used international platform to a crowded domestic concourse or pedestrian underpass).

9.44 In our view, none of the policy options identified in the previous section would create a serious risk of either of the above, although the potential impacts of implementation at specific locations would need to be considered case-by-case to eliminate the risk entirely.

9.45 Finally, it was necessary to distinguish between the relative effectiveness of best practice, guidelines and mandatory requirements. Figure 6.2 sets out a stylised interpretation of the effectiveness of these different approaches. However, as reported in Chapter 6, we have identified examples in which mandatory requirements have been ignored, and others in which best practice has been adopted without any external stimulus. In the absence of systematic evidence regarding the effectiveness of different approaches, we have assumed that policy measures implemented as guidance or exchange of best practise level are less likely to be implemented than common mandatory requirements.

9.46 Moreover, some policy measures do not contain any specific security interventions, therefore the direct costs and benefits of these policy measures are likely to be small and spread across a broad cost base. In such cases we have assumed the impacts are equivalent to a small proportion of all security interventions. The assumptions adopted within the quantified assessment are reported in Table 9.5.

Table 9.5: Intervention level multipliers

Intervention Level	Size of Impacts Multiplier	
	All Policy security interventions	Policy measures not containing security interventions
Common Mandatory Requirements	100%	5%
Guidance	50%	2.5%
Exchange of best practise	20%	1.125%

Source: Steer Davies Gleave

User impacts

9.47 User impacts arise as the result of behavioural change among the travelling public. For example, changes to the perceived quality of rail will have an impact on the overall demand for high-speed and international rail services. Policy options are likely to affect the attractiveness of rail services, and hence the demand for rail travel, in three ways:

- passengers may feel more or less 'secure' depending on the specific measures implemented and their visibility to those using rail services and station facilities;

- security interventions may impose changes in journey times and journey time reliability[65]; and
- fares may increase, subject to the funding approach selected.

9.48 In order to place a monetary value on changes to rail demand we have used the standard welfare economics approach adopted in a number of Member States to determine domestic transport spending priorities and as also used by the European Investment Bank to assess value for money. The approach is based upon the premise that transport is a demand that is derived from the opportunities and potential benefits available at destinations. People make trips when the perceived costs of doing so, both in terms of time and money, are outweighed by these opportunities and benefits. There is a considerable body of evidence that provides estimates of changes in travel demand based on the effects of the various options on users' perceptions of transport costs. The calculation of transport user benefits is then based on changes in consumer surplus associated with these changes in costs.

9.49 Consumer surplus is, in essence, a measure of the amount of satisfaction or utility that is taken from consuming a good or service, over and above the amount that someone paid for it. In purely transport terms, this is the sum total of the difference between how much a transport user is willing to pay for an option (measured in terms of money and journey time and referred to as 'generalised cost') and the amount that the user would actually have to pay. The marginal user is only just willing to make the trip at a given perceived cost so their consumer surplus approaches zero.

9.50 The UK Department for Transport's appraisal guidance (WebTAG) explains[66]:

"The surplus associated with making a journey will not be the same for everybody and depends on the benefit each individual derives from making that journey. Transport demand generally responds to changes in cost, with a reduction in cost leading to increased demand. It follows, therefore, that the benefit associated with any new trips will be lower than that for trips that were already being made (or else they would have been made before the reduction in cost). Therefore, transport demand can be represented by a traditional, downward-sloping demand curve where the demand curve shows the benefit associated with an additional trip at different levels of demand."

9.51 The costs of travel can be represented with an upward-sloping supply curve, reflecting increasing congestion as demand increases. The impact of a policy option can be considered as shifting the supply curve, changing the cost of travel. These relationships are shown in Figure 9.2, along with the change in consumer surplus brought about by a change in the transport costs perceived by users.

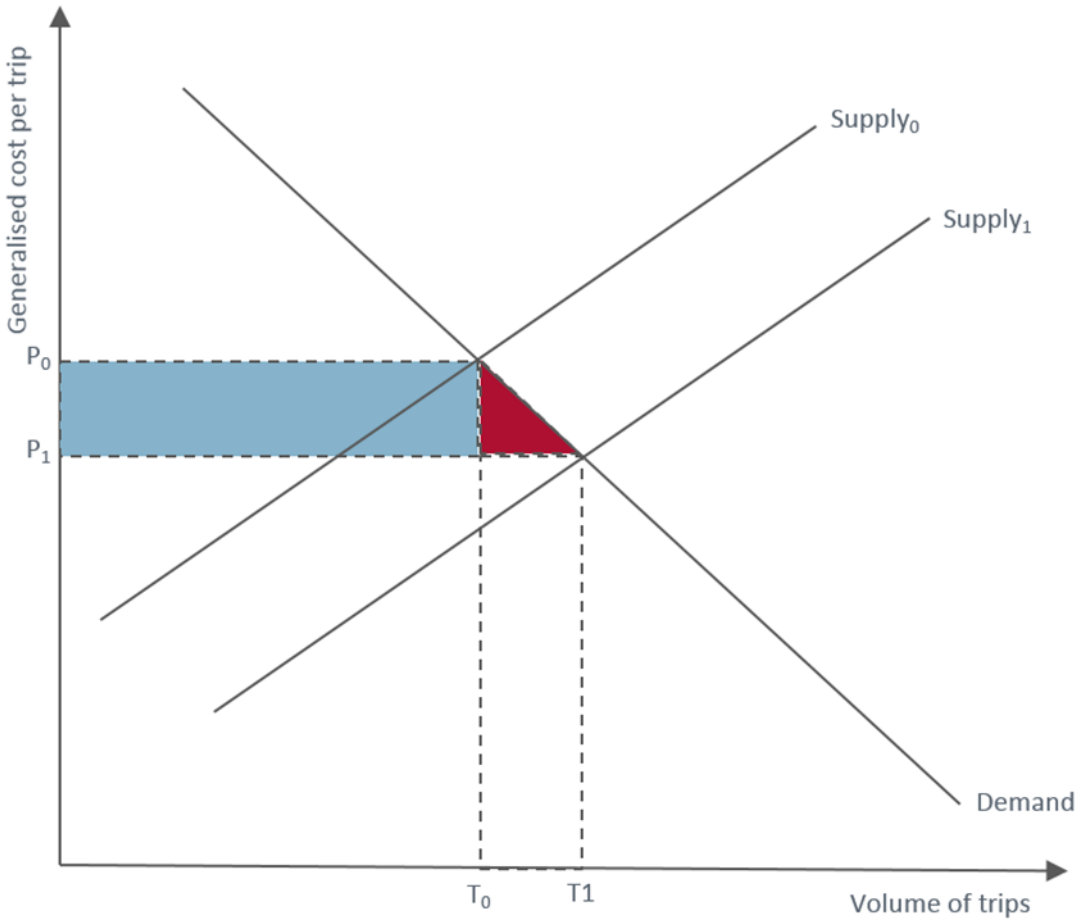
9.52 The change in consumer surplus for existing travellers, who were already making trips in the absence of the scheme, is the full value of the change in cost, represented by the blue rectangle in the diagram. The change in consumer surplus for 'new' travellers, based on the difference between their willingness to pay, represented by the demand curve, and the new cost, is represented by the red triangle. The person represented at T_0 has consumer surplus

[65] In practice, none of the shortlisted security interventions would affect passenger journey times (as would be the case following the introduction of baggage screening measures).

[66] WebTAG Unit A1.3 - User and Provider Impacts (November 2016) p.2

equivalent to $P_0 – P_1$ while the marginal additional traveller at T_1 has a consumer surplus approaching zero. On the assumption that the demand curve is linear, the total value is calculated on the basis of the average change in consumer surplus (i.e. half the difference in cost, multiplied by the number of new trips)[67].

Figure 9.2: Change in consumer surplus arising from a change in generalised costs



9.53 Generalised costs for public transport may take into account fares, access time to station/stop, waiting/boarding/alighting time, in vehicle time and time penalties for crowding and interchange. If generalised cost is measured in units of time, a monetary value can then be placed on the change in consumer surplus (measured as the area beneath the demand curve between the 'baseline' and 'policy option' scenarios) using values of travel time savings taken from Member State appraisal guidelines or, where values are not available, European Investment Bank guidance[68].

9.54 In order to implement the methodology described above, we need information regarding the scale of the change in costs associated with making an international and/or high-speed

[67] The rule of a half formula can be extended to cover network appraisal with many modes and origin/destination pairs.

[68] The Economic Appraisal of Investment Projects at the EIB, EIB (2013) http://www.eib.org/attachments/thematic/economic_appraisal_of_investment_projects_en.pdf.

journey, and evidence on the responsiveness of passengers to changes in those costs. The remainder of this section describes the sources used to undertake the assessment.

9.55 As set out in paragraph 9.47, changes to the generalised cost of travel arising from each policy measure are composed of changes to fare levels, journey times and other factors for which a monetary value is available (including perceived security levels)[69]. **Table 9.6** describes the sources and assumptions used to determine generalised costs in both the baseline and 'policy option' scenarios.

Table 9.6: Generalised cost sources and assumptions

Generalised cost item	Data point/ Assumption	Source
Fare Level	Rail Operating Costs	'Cost & contribution of the rail sector' SDG, 2015
	Typical Fare Level	'Study on the price & quality of rail services' SDG, 2015
	Operating Costs Passed onto Passengers	Estimated
Journey Time	Typical Journey Time	'Study on the price & quality of rail services' SDG, 2015
	Changes to Journey Times	No changes to journey time anticipated
Perceived Security Level	Security Threat Level Score	Estimated based on: UK Foreign Office Threat Level ratings EU Terrorism Situation and Trend Report (TE-SAT) 2016
	Changes to perceived journey times	Passenger Demand Forecasting Handbook version 5.1 Section B

Source: Steer Davies Gleave

9.56 Taking each of the generalised cost items in turn:

- **Fare levels:** we have assumed that the direct costs of implementing policy measures lead to an increase in rail operating costs in each Member State. We have assumed that 20% of the increase in operating costs is passed onto rail passengers through fare increases, only in those circumstances where the implementation costs are expected to be borne by the railway undertaking and where those costs are considered by the railway undertaking as a cost per passenger[70]. In practice, this means that:
  - No third party costs would be passed into fares, as there is no mechanism to do so;
  - No infrastructure costs would be passed into fares, as that is a regulatory decision; and
  - No RU fixed costs would be passed into fares as there would be no rationale to do so.
- **Journey times:** none of the policy options includes policy measures which will materially affect passenger journey times. As previously discussed, we have excluded from the

[69] Generalised costs are defines as 'a weighted sum of time and other costs of travel which can be measured in units of money or (preferably) time'

[70] Long-run cost pass-through assumptions drawn from *Cost pass-through: theory, measurement, and potential policy implications* (2014), Office of Fair Trading

analysis specific security interventions that are likely to adversely affect the passenger journey experience substantially.

- **Perceived security level (on-train):** consistent with UK Passenger Demand Forecasting Handbook (PDFH) guidance, we have assumed that changes to generalised costs arising from policy options are caused by improvements to on-train and at station security. As set out in Table 4.11, each Member State has been assigned a baseline security threat level. Each policy measure is then assumed to reduce the perceived threat level in each Member State to a uniform minimum level (see **Table 9.7**). If a Member State's baseline threat level is above the policy measure minimum, we have assumed that it will fall to this minimum level when a policy measure is introduced. However, if a Member State's base security threat level is at or below the policy measure minimum, we have assumed that it will not change when a policy measure is introduced. The perceived threat level is then converted to a multiplier on in-vehicle time (itself a component of generalised costs) in line with PDFH guidance.
- **Perceived security level (at-station):** where a policy measure affects security at and around station facilities, we have followed a very similar approach to on-train security. However, rather than converting the change in perceived threat levels into a multiplier on journey times, we have drawn on empirical evidence on direct demand responses reported in PDFH.

Table 9.7: Minimum perceived security threat level assumptions by policy measure

Option	Ref	Policy measure	Minimum Threat Level
1	1A	Reporting and monitoring national security data	0
	3E	S/SMS threat level protocols	70
	2B	Emergency egress and access to stations	60
	4A	CCTV on stations, with recording and facial recognition	30
	4B	CCTV on trains, with recording and facial recognition	0
2	3A	S/SMS ensure exchange of information by relevant parties	30
	3C	S/SMS contingency planning and incident recovery	40
	3F	S/SMS liaison, incident response, drills and exercises	50
	4C	Deploying staff where they can observe	40
	4F	Staff vetting and access controls	0
3	1B	Researching and disseminating worldwide security data	0
	3B	S/SMS recording of vulnerabilities and inspection regimes	40
	3D	S/SMS contingency IT, communications and spares	70
	2A	Emergency egress and access to infrastructure	60
	2C	Blast-resistant features on stations	60
	2D	Blast-resistant features on trains	0
	4D	Training station/train staff in risk and behaviour monitoring	60
	4E	Awareness promotion among passengers	60

Source: Steer Davies Gleave assumptions

9.57 As with assumptions regarding the relative performance of security interventions on reducing the frequency and severity of security breaches, there is no systematic, observed evidence regarding the relative performance of security interventions on passengers' perceptions of

security. Depending upon the security interventions included within policy options, these perceptions may differ by Member State. In practice, cultural differences noted will play a role in the impact of each option, a view supported by DB (2012)[71]. In some cases, for instance, implementing visible security interventions such as increased police presence may act as a deterrent as users associate increased police presence with an imminent threat. As a consequence, we have also presented the results of sensitivity tests in which the minimum perceived threat level associated with policy measures is ten points larger and ten points smaller (within an overall range of 0 to 100). We have not considered sensitivity tests in which the relative performance of individual security interventions varies.

9.58 Having established the change in generalised costs, we have then calculated the change in passenger demand (expressed as passenger kilometres) in each Member State arising from those cost changes, and from changes to perceived levels of at-station security. Behavioural responses to these two factors have been subject to extensive study, as reported within the Passenger Demand Forecasting Handbook (PDFH). We have used elasticity values from the most recent version of the handbook (version 5.1) to inform our assessment of policy options. The assumptions and data sources used are set out in Table 9.11

Table 9.8: Passenger demand assumptions

	Data point/ Assumption	Source
Passenger Demand (PKM)	Base Passenger Demand	Eurostat, PRIMES Model
	PKM growth rate	PRIMES Model
	Fare Elasticities	Passenger Demand Forecasting Handbook version 5.1
Passenger Journeys	Typical Journey Length	'Study on the price & quality of rail services' SDG, 2015

Source: Steer Davies Gleave

Non-user impacts

9.59 In addition to direct impacts and those which affect transport users, security options may also have indirect impacts which affect non-transport users. For example:

- impacts on the environment as a result of mode shift;
- impacts on Small and Medium Enterprises (SMEs) as a result of changes to travel patterns; and
- impacts on the economy as a result of productivity changes and the relocation of economic activity.

9.60 Of these three non-user impacts, only environmental impacts have been quantified using the welfare approach described in paragraphs 9.48 to 9.52. It is important to note that some of the policy measures may lead to changes in the demand for high-speed and international rail travel, and those passengers attracted to (or displaced from) travelling by rail may choose to travel less (more) by rail, travel more (less) by other modes, or stop (start) travelling. These changes in travel patterns may therefore affect the environment in the form of increased or decreased greenhouse gas (GHG) emissions.

[71] Position Statement on the Commission Staff Working Paper on Land Transport Security, DB (2012).

9.61 In order to estimate environmental impacts, we took baseline emissions estimates from the European Commission 2011 White Paper on Transport. Using evidence regarding the change in distance travelled by other modes as a percentage of a change in rail passenger kilometres (known in the literature as 'diversion factors') taken from the UK National Transport Model (NTM) and TRANS-TOOLS, we then generated estimates of the changes in passenger kilometres for non-rail modes following the introduction of a policy option[72]. Finally, we monetised the change in emissions using the marginal external costs of emissions provided in the Update of the Handbook of External Costs of Transport (Ricardo-AEA, 2014)[73].

Discounting, appraisal period and timing of policy measures

9.62 Within the monetised appraisal of impacts, we assume that security options are introduced over several years and may take some years for their full effects to be realised. More specifically, we differentiated between the intervention levels identified in the Terms of Reference, assuming that[74]:

- common mandatory requirements would take up to four years from the start of the appraisal period to introduce;
- guidelines could be introduced more quickly since introduction would not require legislation (two years); and
- exchange of best practice could be introduced relatively quickly, with an appropriate forum for exchange established within one year of the start of the appraisal period.

9.63 In general, we assume that the implementation of non-legislative measures will be faster. However, while issuing guidelines or establishing a best practice forum is likely to be relatively fast, the actual changes in security emerging from these are likely to take more time to materialise in the absence of any mandatory framework. A summary of the policy measures included within the assessment and their timing is show in **Table 9.9**. Supporting commentary for 'lead in' timing assumptions is provided in Appendix E.

Table 9.9: Policy measures first impact year and lead in time

Ref	Description	Intervention Level	Includes security interventions?	Costs passed onto passengers?	First impact year	Lead in years
1A	Reporting and monitoring national security data	Common Mandatory requirements	×	×	2020	5
3E	S/SMS threat level protocols	Guidance	✓	×	2018	10

[72] TRANS-TOOLS is a European transport network model covering both passengers and freight, as well as intermodal transport. It combines advanced modelling techniques in transport generation and assignment, economic activity, trade, logistics, regional development and environmental impacts. See http://energy.jrc.ec.europa.eu/transtools/.

[73] See http://ec.europa.eu/transport/themes/sustainable/studies/doc/2014-handbook-external-costs-transport.pdf.

[74] These assumptions have been developed in discussion with the Commission during the preparation of this Impact Assessment

Ref	Description	Intervention Level	Includes security interventions?	Costs passed onto passengers?	First impact year	Lead in years
2B	Emergency egress and access to stations	Guidance	✓	×	2018	20
4A	CCTV on stations, with recording and facial recognition	Common Mandatory requirements	✓	✓	2020	10
4B	CCTV on trains, with recording and facial recognition	Common Mandatory requirements	✓	✓	2020	10
3A	S/SMS ensure exchange of information by relevant parties	Common Mandatory requirements	✓	×	2020	5
3C	S/SMS contingency planning and incident recovery	Common Mandatory requirements	✓	×	2020	5
3F	S/SMS liaison, incident response, drills and exercises	Guidance	✓	×	2018	5
4C	Deploying staff where they can observe	Guidance	✓	×	2018	5
4F	Staff vetting and access controls	Guidance	✓	×	2018	5
1B	Researching and disseminating worldwide security data	Guidance	✓	×	2018	5
3B	S/SMS recording of vulnerabilities and inspection regimes	Common Mandatory requirements	✓	×	2020	5
3D	S/SMS contingency IT, communications and spares	Guidance	✓	×	2018	5
2A	Emergency egress and access to infrastructure	Guidance	✓	×	2018	30
2C	Blast-resistant features on stations	Guidance	✓	✓	2018	60
2D	Blast-resistant features on trains	Guidance	✓	✓	2018	20
4D	Training station/train staff in risk and behaviour monitoring	Guidance	✓	×	2018	5
4E	Awareness promotion among passengers	Guidance	✓	×	2018	5

Source: Steer Davies Gleave

9.64 All monetised impacts are reported as 2016 net present values in 2016 real (constant) prices. We appraised over the period to 2050, the time horizon considered in the 2011 White Paper on Transport *Roadmap to a Single European Transport Area - Towards a competitive and resource efficient transport system* and for which baseline forecasts are available. We applied the standard European Commission social discount rate of 4%.

Reporting impacts

9.65 The following section describes how outputs from the quantitative analysis have been used to inform the assessment of impacts as categorised in Table 9.3. A description of the calculations undertaken, alongside supporting commentary, is provided in Appendix E.

9.66 ***Free movement of goods, services, capital and workers***: we have assumed that any associated benefits are limited to the transport user benefits, or change in consumer surplus, arising from any direct change in generalised costs due changes in journey times. As discussed above, none of the short-listed policy measures are expected to impede passengers or extend journey time. Therefore, there is unlikely to be any effect upon the free movement of goods, services, capital and labour.

9.67 ***Impacts on government administration***: government administration impacts, in the form of government costs, are estimated directly from the direct costs associated with each policy measure. Government costs are assumed to be 10% of direct costs for those policy measures that involve common mandatory requirements, 5% of direct costs for policy measures that introduce guidance and 0% for policy measures which involve the exchange of best practice.

9.68 ***Consumer prices***: again, we have assumed that any associated impacts are limited to the transport user benefits, or change in consumer surplus, arising from any direct change in generalised costs due changes in fare level. As described in paragraph 9.56, the assessment assumes that 20% of operating cost increases are passed onto consumers through fare increases when the costs of implementing security measures are borne by the railway undertaking, and can be directly related to the quantity of journeys made or the distance travelled.

9.69 ***Economic growth and employment***: the impact of security interventions on economic growth and employment are estimated as the quantity of business trips generated multiplied by the annual average trip rate per business passenger to give an estimate of the equivalent number of additional business passengers. This is then multiplied by a fixed proportion (assumed to be 20%) of output (GDP) per worker, to reflect the fact that in the absence of the policy measure that same business person would undertake some alternative, albeit less productive, business activity and therefore the full value of their output should not be captured.

9.70 ***Job creation and destruction***: the monetised impacts of job creation and destruction are estimated as the net change in jobs as a consequence of the implementation of security interventions, taking into account substitution and diversion factors, which are then multiplied by average incomes by Member State. The analysis has been restricted to the direct impacts of the security intervention in order to avoid double-counting of impacts captured under the previous heading.

9.71 ***Deterrence and detection***: the impact upon deterrence and detection of crime or terrorism is composed of two elements:

- the direct benefits associated with reductions in the severity of incidents, the numbers of incidents, and the direct costs of repair and recovery; and

- the change in transport user benefits, or consumer surplus, associated with a change in citizens' perceptions of security levels.

9.72 ***Fuel and energy consumption***: monetised estimates of the impacts on fuel and energy consumption are calculated by applying carbon prices to the net change in carbon emissions arising from a change in the level of car and rail passenger kilometres. For the purpose of this assessment, only the impact of greenhouse gas emissions is measured, since there is insufficient information on the incidence of air pollution (which has localised effects) to generate a meaningful monetised estimate.

9.73 ***Additional resources***: additional resources are assumed to be the cost of implementing each policy measure; this is the direct cost of each policy measure less government administration costs (to avoid double-counting).

9.74 ***Business information obligations***: the additional reporting burden imposed on businesses is calculated by estimating the total yearly employee hours required to meet the reporting levels of each option and translating it into full-time equivalent (FTE) staff numbers based on the average yearly working hours of each Member State.

9.75 ***Consumers' ability to benefit from the internal market***: the change in passenger kilometres split by journey purpose provides a measure that indicates the impact on consumer's ability to benefit from the internal market. Changes in the level of commuter demand provides an estimate of labour market accessibility. In addition, changes in business demand can be used as an estimate of accessibility to the market for goods and services.

9.76 ***Small medium enterprises***: there is no evidence to suggest that SME workers are less likely to travel by rail compared to employees of larger enterprises while on business or commuting. Therefore, the impacts on SMEs across Member States are estimated by multiplying the proportion of SME workers in each Member State by the change in business and commuting travel demand by Member State.

9.77 ***Disproportionate impacts on individual Member States or regions***: the proportion of total transport user benefits captured by the Member State with the largest benefits provides a proxy measure for the extent to which benefits are disproportionately experienced by an individual Member State for each policy measure. The lower the proportion, the more evenly spread are benefits across all Member States.

9.78 ***Demand for passenger transport and modal split***: the impact on the demand for passenger transport is a direct output of the transport appraisal model used to estimate the impact of policy measures. For the purpose of this assessment we have used the change in rail mode share as the preferred assessment metric.

Qualitative assessment

9.79 We carried out a qualitative assessment of those impacts that were unsuitable for quantitative analysis, or for which relevant data was unavailable and/or prohibitively costly to collect. This section summarises our methodology for identifying relevant criteria for each impact, and how we generated qualitative scores for security options against these criteria.

Qualitative scores

9.80 Given the scarcity of evidence regarding the impact of security measures upon a wide range of indicators, it has not been possible to undertake a granular or fine-scale qualitative assessment. We have therefore limited the extent of our assessment to considering whether a

policy measure will have a large, medium or small impact (both positive and negative), or have no perceivable impact whatsoever.

9.81 For each impact, we formalised this by scoring the performance of each policy measure on a seven-point scale from -3 (large negative impact) to +3 (large positive impact). The policy measure considered to have the largest absolute impact in either direction defined the range of scores allocated and, depending on whether the impact was beneficial or detrimental and the expected scale of impact, determined the maximum absolute score that could be assigned to others. Policy measures considered to have small or negligible impacts were assigned scores of zero. All other policy measures were assigned a score between these scores, based on their performance relative to these reference points.

9.82 A qualitative score was assigned to each policy measure, with a simple arithmetic mean then used to aggregate scores across multiple policy measures within a policy option. This approach normalises for the fact that each policy option includes a different quantity of policy measures.

9.83 Our approach to scoring qualitative impacts diverges from that recommended within the Better Regulation Toolbox in that it does not include a "direction" variable to indicate whether the impact is positive or negative. Instead, the direction is implicit within the scale used for impacts, which straddles both positive and negative scores. Doing so allows for the possibility that against a given criterion some policy measures may have a positive impact, while others may have a negative impact. Under these circumstances constraining impacts to be either positive or negative could lead to counterintuitive scores.

9.84 In assigning scores to security options it will be important to note that the impact of any given policy measure may differ between Member States depending on the importance of the rail sector, perceptions of security risks and their tolerability, and the current level of security in the rail sector. However, we have not been able to identify reliable empirical evidence at a sufficiently geographically disaggregate level that would permit such an assessment to be undertaken.

9.85 Therefore, for all quantitative impacts it has been necessary to analyse the performance of each strategy at the EU level. The criteria used to inform the qualitative assessment are described in Table 9.10 below.

Table 9.10: Qualitative assessment criteria

Impact	Criteria
Impacts on consumer choice and competition	Will the measures affect the incentive for anti-competitive behaviour of firms?
	Will the measures affect barriers to entry for new firms?
	Will the measures affect the prices paid by consumers?
	Will the measures affect consumer choice?
	What is the impact on the cost of meeting the regulation?
Impacts on research and development	Would the intervention privilege or prohibit characteristics a new type of good or service could have? Could this even lead in the extreme to preventing a product group or, conversely, leading the market to a single technological solution?
	Does the implementation of the intervention put an administrative burden specifically on introducing new goods, services and production plants on a market or on their demonstration prior to market introduction?
	Does the intervention alter the rewards from innovation (such as the length of patent protection)?
	What is the impact on product development and is there a possibility that some products

Impact	Criteria
	would be taken from the market (i.e. de-selected) or technologies lost?
	Does it impinge on the price, quantity or mobility of human resources with skills appropriate to new technologies and work methods, be it vocationally trained workers or experienced managers?
	Does the proposed intervention impact the generation of new ideas, their adaptation and application, including from the knowledge base to industry?
	Does it affect the co-operation (such as circulation of data, research results or researchers) among public researchers and between public and corporate R&D and with intermediaries that provide advice and support to R&I activities, such as openness to co-operate or the distribution of benefits?
	Does the proposed intervention potentially affect the establishment of, access to and functioning of research and innovation infrastructures?
Impacts on products, production methods and technology	Would the intervention privilege or prohibit characteristics a new type of good or service could have? Could this even lead in the extreme to preventing a product group or, conversely, leading the market to a single technological solution?
	Does the implementation of the intervention put an administrative burden specifically on introducing new goods, services and production plants on a market or on their demonstration prior to market introduction?
	What is the impact on product development and is there a possibility that some products would be taken from the market (i.e. de-selected) or technologies lost?
	Does it impinge on the price, quantity or mobility of human resources with skills appropriate to new technologies and work methods, be it vocationally trained workers or experienced managers?
	Does the proposed intervention impact the generation of new ideas, their adaptation and application, including from the knowledge base to industry?
Impacts on trade and free movement with neighbouring countries	Will the options affect European exports?
	Will the options affect European imports, and value chains in general?
	Does the option affect the potential for trade in services?
	Will the proposal increase or decrease regulatory convergence with the main trading partners?
Social and distributional impacts	To what extent does the option influence the supply of labour of specific groups through labour market participation or labour market mobility?
	Would the option affect the prices, quality, availability or choice of consumer goods and services?
	Would the option affect consumer information, knowledge, trust or protection?
	Would the option impact the safety or sustainability of consumer goods and services?
	Would the option impact vulnerable consumers?
Impacts on workers' health, safety and dignity	Does the option affect health and safety at work?
	Does the option affect workers' fundamental rights?

Assessment of non-scored impacts

9.86 The impacts which we assessed qualitatively are set out in Table 9.3. Where we were able to identify relevant criteria and data to inform the assessment (both the magnitude and the direction), we used the qualitative approach described above. In other cases, where supporting evidence was not available and could not therefore be used to generate a score for each policy measure we provided supporting commentary on the likely impact, without using a scoring system. This commentary was not then taken further within the assessment framework and plays no role in assessing the relative performance of policy options.

Multi-Criteria Analysis (MCA) framework

9.87 We combined the outputs of the quantitative (monetised and non-monetised) and qualitative assessments within a multi-criteria framework. Multi-Criteria Analysis (MCA) can help to establish preferences between options by reference to an explicit set of objectives and supports decision-making through providing measurable criteria to assess the extent to which the objectives have been achieved by the various policy measures under consideration. In simple circumstances, the process of identifying objectives and criteria may alone provide sufficient information for decision-makers. However, in more sophisticated applications such as this study, MCA offers a number of ways of aggregating evidence (including monetary, quantitative, and qualitative information) against individual criteria to provide indicators of the overall performance of options.

9.88 A key feature of MCA is its emphasis on the judgement of the decision-making team in establishing objectives and criteria, estimating relative importance weights and, to some extent, in judging the contribution of each option to each performance criterion. For this study, we used MCA to combine the qualitative and quantitative assessments to judge each option in its totality. To do this, we applied weightings to the various monetised impacts and qualitative assessment criteria, as shown in the table below.

9.89 Our rationale for this distribution is that:

- Criteria that can be assessed by monetising impacts represent the most robust source of information for decision-makers. Therefore, a weighting higher than that of quantitative and qualitative assessed impacts is proposed (50%). Specific weights for individual impacts are implied through the monetisation exercise since all impacts are converted into the same monetary unit of account (€). It is not, therefore, necessary to predetermine weights for monetised criteria.
- Impacts represented quantitatively will receive 30% of the overall weighting. We used a range of weights from 4%to 8% for each impact. We assessed most impacts at 4%, apart from the impact on demand for passenger transport (6%) and SMEs (8%).

9.90 Impacts represented qualitatively will receive 20% of the overall weighting. In a similar manner to quantitative impacts, a broadly uniform distribution of weights is proposed, with a 3% weight for each criterion. Impacts on unintended negative consequences are considered harder to score qualitatively and therefore the lower weight of 2% reflects the uncertainty associated with their assessment.

Table 9.11: Proposed weightings for multi-criteria analysis

	ID	Impact	Individual Weight	Overall Weight
Monetised	1	What impact (positive or negative) does the option have on the free movement of goods, services, capital and workers?	Implicit weighting within monetisation process	50%
	5	Does it bring additional governmental administrative burden and costs?		
	9	Does the option affect the prices consumers pay for the service?		
	14	Does it have overall consequences of the option for economic growth and employment?		
	15	Does the option directly or indirectly facilitate new job creation or loss of jobs?		
	25	Can the security effectiveness of the options be measured in respect to deterring or even detecting crime or terrorism?		
	27	What are the additional resources that the introduction of such an option would require both in terms of people (railway staff, law enforcement capacity) and associated cost?		
	30	Will the option increase/decrease energy and fuel needs/consumption?		
Quantitative	3	Does it affect the nature of information obligations placed on businesses (for example, the type of data required, reporting frequency, the complexity of submission process)?	4%	30%
	4	What is the impact, if any, on Small and Medium Enterprises?	8%	
	10	Does it impact on consumers' ability to benefit from the internal market?	4%	
	11	Is there a single Member State or region which is disproportionately affected?	4%	
	22	Does the option affect the right of citizens to move freely within the EU?	4%	
	29	Will the option increase or decrease the demand for passenger transport or influence its modal split?	6%	
Qualitative	2	Will it lead to a reduction in consumer choice, higher prices due to less competition, the creation of barriers for new suppliers and service providers, the facilitation of anti-competitive behaviour or emergence of monopolies or market segmentation?	3%	20%
	7	Does the option stimulate or hinder research and development?	3%	
	8	Does it facilitate the introduction and dissemination of new production methods, technologies and products?	3%	
	12	What are the impacts on third neighbouring countries with which the EU has close trade, transport or free movement i.e. Schengen links?	3%	
	16	Does it have specific consequences for particular types of workers or does it affect particular groups or people such as disabled or of different ages?	3%	
	18	Will it affect workers' health, safety and dignity?	3%	
	26	Are there any unintended negative consequences of introducing such options that may detrimentally impact upon either the safety or privacy of the passenger or staff?	2%	

Source: Steer Davies Gleave assumptions

10 Results of impact assessment

Introduction

10.1 In this section, we summarise the results of our quantitative and qualitative assessment of the three short-listed policy options described in Chapter 8, using the methodology described in Chapter 9. The Terms of Reference required us to assess 30 separate economic, social and environmental impacts, ranging from economic growth and consumer choice, through employment levels and employee rights, to fuel and energy consumption and environmental emissions. As described in the previous chapter, while some of these can be expressed in monetary terms, others can only be quantified by reference to physical magnitudes such as numbers of employees, and others can only be assessed in qualitative terms.

10.2 Accordingly, in the remainder of this chapter, we describe:

- the overall performance of policy options;
- the results of the monetary, quantitative and qualitative assessment exercises;
- the results of sensitivity tests on the monetary and quantitative assessments; and
- the results of a further qualitative assessment of the remaining impacts, provided in the form of commentary.

Overall performance of policy options

10.3 As discussed in Chapter 9, we used a Multi-Criteria Analysis (MCA) to combine monetary, quantitative and qualitative assessments against individual criteria to provide an indication of the overall performance of policy options, the outputs of which are set out in Table 10.1 below.

Table 10.1: Multi-Criteria Analysis outputs

Option	Multi-Criteria Analysis score	Rank
Option 1	23.3	3
Option 2	49.8	2
Option 3	72.1	1

Source: Steer Davies Gleave analysis

10.4 It is clear from the results that policy option 3 is the best performing package of policy measures. This is in line with expectations given the incremental nature of the policy options, with option 3 being the most comprehensive.

10.5 The final weights assigned to each of the monetised impacts are set out in Table 10.2 below. These reflect the magnitude of monetised benefits/dis-benefits which, by definition, represent relative weights expressed in the same unit of account (€). Monetised benefits constitute 50%

of the total weight assigned in the MCA framework, with the remainder linked to the quantitative (30%) and qualitative (20%) assessments.

Table 10.2: MCA weights for monetised impacts

ID	Impact	Individual Weight	Overall Weight
1	What impact (positive or negative) does the option have on the free movement of goods, services, capital and workers?	0.0%	50%
5	Does it bring additional governmental administrative burden and costs?	0.1%	
9	Does the option affect the prices consumers pay for the service?	2.6%	
14	Does it have overall consequences of the option for economic growth and employment?	29.1%	
15	Does the option directly or indirectly facilitate new job creation or loss of jobs?	0.2%	
25	Can the security effectiveness of the options be measured in respect to deterring or even detecting crime or terrorism?	3.6%	
27	What are the additional resources that the introduction of such an option would require both in terms of people (railway staff, law enforcement capacity) and associated cost?	0.6%	
30	Will the option increase/decrease energy and fuel needs/consumption?	13.8%	

Source: Steer Davies Gleave analysis

Quantitative assessment

Monetised impacts

10.6 Monetised impacts of each of the policy measures investigated under the main policy options are shown in Table 10.3 . The impacts are expressed as present discounted values over the time horizon of the assessment. All values are in 2016 prices.

Table 10.3: Monetised impacts of policy options (€m, 2016 PV and prices)

Option	Free movement of goods, services, capital and workers	Government administration burden	Consumer prices	Economic growth and employment	Job creation and destruction	Deterrence and detection	Additional resources	Fuel and energy consumption
Option 1	-	(650)	(41,070)	114,220	360	54,450	(5,870)	59,080
Option 2	-	(910)	(41,070)	319,670	2,680	55,480	(8,200)	149,360
Option 3	-	(990)	(41,190)	466,960	3,360	58,310	(9,680)	221,770

Source: Steer Davies Gleave analysis
Note: Figures in parentheses are negative i.e. costs or disbenefits

10.7 In line with expectations, the most significant positive impact associated with the introduction of security policy measures is on economic growth and employment. The proportion of individuals travelling in the course of business on high-speed and international rail services is higher than the average across all rail journeys and substantially higher than the average across all journeys (on all modes). These individuals typically have a higher willingness to pay for a range of travel time and quality-related journey attributes (including security), and are

therefore more sensitive to changes in these attributes. The magnitude of the impacts also reflects the cumulative effect of additional growth over an extended period.

10.8 The second most significant monetised impact is on fuel and energy related consumption. These represent a net improvement to the environment as the additional energy consumption needed to accommodate additional rail travel is offset by passengers transferring from other, more carbon-intensive modes.

10.9 Impacts on the deterrence and detection of security threats are unambiguously positive, although the scale of benefits is typically an order of magnitude smaller than the impact on economic growth and employment. An order of magnitude smaller still are the direct impacts upon job creation and destruction associated with the implementation of policy measures, which, while significant, are likely to be limited compared to the broader effects on employment due to economic growth generated through additional travel.

10.10 The impact on consumer prices is modest given our assumption that only 20% of all additional security costs borne by railway undertakings and linked to passenger numbers are passed on to travellers through changes in fares. Finally, no impacts on the free movement of goods, services, capital and workers are observed since any security interventions that involve physical barriers which impede the movement of passengers into, around and from station facilities did not pass the initial sift summarised in Table 6.8.

Other quantified impacts

10.11 Where possible we sought to quantify impacts that cannot be monetised. Table 10.4 below provides a summary of the impacts of each policy measure in 2050, the final year of the assessment period by which we would expect the full effects of a measure to be observed. Table 10.5 presents equivalent values for each policy measure in the year 2030.

Table 10.4: Summary of non-monetised impacts (2050)

Option	Business information obligations	Small and Medium Enterprises	Consumers' ability to benefit from the internal market	Disproportionate impacts on individual Member States or regions	Right of citizens to move freely	Change in rail market share
Units:	FTEs	Million PKM	Million PKM	%	-	%
Option 1	1,180	4,480	6,800	29.9%	-	0.5%
Option 2	8,130	10,980	16,630	31.2%	-	1.3%
Option 3	10,290	16,540	25,120	41.6%	-	2.0%

Source: Steer Davies Gleave analysis

Table 10.5: Summary of non-monetised impacts (2030)

Option	Business information obligations	Small and Medium Enterprises	Consumers' ability to benefit from the internal market	Disproportionate impacts on individual Member States or regions	Right of citizens to move freely	Change in rail market share
Units:	FTEs	Million PKM	Million PKM	%	-	%

Option	Business information obligations	Small and Medium Enterprises	Consumers' ability to benefit from the internal market	Disproportionate impacts on individual Member States or regions	Right of citizens to move freely	Change in rail market share
Option 1	870	2,990	4,530	30.1%	-	0.5%
Option 2	6,000	7,670	11,630	31.1%	-	1.2%
Option 3	7,590	11,200	17,010	41.6%	-	1.7%

Source: Steer Davies Gleave analysis

10.12 The tables highlight that all policy options involve some increase in administrative burden, but those requiring demonstration of compliance with required standards and processes have the greatest impact.

10.13 Impacts on Small and Medium Enterprises and impacts on consumers' ability to benefit from the internal market are both assessed with reference to changes in the absolute quantity of rail demand. As a consequence, those policy options having the greatest impact on demand are considered to have the greatest impact on SMEs (business trips) and consumers (all trips). For example, changes in the level of commuter demand provide a proxy for labour market accessibility. Moreover, changes in business demand can be used as an estimate of accessibility to the market for goods and services.

10.14 Since changes to generalised costs (and therefore the demand for travel) arising from security interventions are the primary drivers of changes to passenger kilometres, the introduction of policy measures which lead to the largest reductions to the perceived security threat level across Member States will result in the largest changes in demand.

10.15 The proportion of total transport user benefits captured by the Member State with the largest benefits provides a proxy measure for the extent to which benefits are disproportionately experienced by an individual Member State for each policy measure. The lower the proportion, the more evenly spread benefits are across all Member States. For each policy option, over 30% of transport user benefits are captured by France or Germany. This is because the majority of high speed and international passenger kilometres in the EU are contained within these two Member States. In turn this means that changes to generalised cost affect a much larger number of passengers compared to other Member States.

10.16 Finally, rail passenger demand may be adversely impacted by generalised cost increases imposed by new security interventions. While this may affect the ability of citizens to move freely within the European Union, it is not expected to have any impact upon the right to travel. As a consequence, we gave all policy measures a score of zero against this criterion.

Sensitivity tests

10.17 Given the time period covered by the analysis (35 years from the base year of 2016) and the extent to which it has been necessary to rely upon key assumptions for which there is no good-quality, systematic evidence available, the results of the quantitative assessment are inevitably subject to significant uncertainty.

10.18 We therefore subjected them to sensitivity analysis, the results of which are reported below. These sensitivities are based on alternative assumptions regarding:

- the reduction in frequency and severity of incidents delivered by short-listed security interventions; and
- the relative performance of security interventions on passengers' perceptions of security.

10.19 In response to the lack of evidence upon which to base assumptions regarding the reduction in frequency and severity of incidences delivered by short-listed security interventions, we have presented the results of sensitivity tests in which the changes in likelihood and severity of security breaches is 50% larger and 50% smaller than the central assumptions presented in Table 9.4. We have not considered sensitivity tests in which the relative performance of individual security interventions varies. The results of these tests are presented in Table 10.6 and Table 10.7 below. Note that the only impact is on deterrence and detection of specific failures.

Table 10.6: Monetised impacts: frequency and severity of security interventions 50% larger (€m, 2016 PV)

Option	Free movement of goods, services, capital and workers	Government administration burden	Consumer prices	Economic growth and employment	Job creation and destruction	Deterrence and detection	Additional resources	Fuel and energy consumption
Option 1	-	(650)	(41,070)	114,220	360	55,060	(5,870)	59,080
Option 2	-	(910)	(41,070)	319,670	2,680	56,600	(8,200)	149,360
Option 3	-	(990)	(41,190)	466,960	3,360	59,890	(9,680)	221,770

Source: Steer Davies Gleave analysis

Table 10.7: Monetised impacts: frequency and severity of security interventions 50% smaller (€m, 2016 PV)

Option	Free movement of goods, services, capital and workers	Government administration burden	Consumer prices	Economic growth and employment	Job creation and destruction	Deterrence and detection	Additional resources	Fuel and energy consumption
Option 1	-	(650)	(41,070)	114,220	360	53,840	(5,870)	59,080
Option 2	-	(910)	(41,070)	319,670	2,680	54,350	(8,200)	149,360
Option 3	-	(990)	(41,190)	466,960	3,360	56,730	(9,680)	221,770

Source: Steer Davies Gleave analysis

10.20 As indicated, the effect of changing the assumption of frequency and severity is relatively small, suggesting that the estimates of monetised impacts of deterrence and detection are robust. We note, however, that changes to the underlying frequency and impact of security failures could be expected to have a more significant impact on the magnitude of the benefits, although we would not expect the relative impacts across options to change.

10.21 We have also presented the results of sensitivity tests in which the minimum perceived threat level associated with policy measures is ten points larger and ten points smaller (within an overall range of 0 to 100) compared to the central assumptions presented in **Table 9.7**. These are reported in Table 10.8 to Table 10.11 below.

Table 10.8: Monetised impacts: minimum perceived threat level +10 points (€m, 2016 PV)

Option	Free movement of goods, services, capital and workers	Government administration burden	Consumer prices	Economic growth and employment	Job creation and destruction	Deterrence and detection	Additional resources	Fuel and energy consumption
Option 1	-	(650)	(41,070)	131,530	360	57,580	(5,870)	65,970
Option 2	-	(910)	(41,070)	364,770	2,680	58,600	(8,200)	164,150
Option 3	-	(990)	(41,190)	549,420	3,360	61,920	(9,680)	249,270

Source: Steer Davies Gleave analysis

Table 10.9: Quantitative impacts: minimum perceived threat level +10 points (2050)

Option	Business information obligations	Small and Medium Enterprises	Consumers' ability to benefit from the internal market	Disproportionate impacts on individual Member States or regions	Right of citizens to move freely	Change in rail market share
Units:	FTEs	Million PKM	Million PKM	%	-	%
Option 1	1,180	5,020	7,590	29.4%	-	0.6%
Option 2	8,130	12,100	18,280	30.7%	-	1.4%
Option 3	10,290	18,690	28,260	39.9%	-	2.2%

Source: Steer Davies Gleave analysis

Table 10.10: Monetised impacts: minimum perceived threat level -10 points (€m, 2016 PV)

Option	Free movement of goods, services, capital and workers	Government administration burden	Consumer prices	Economic growth and employment	Job creation and destruction	Deterrence and detection	Additional resources	Fuel and energy consumption
Option 1	-	(650)	(41,070)	90,390	360	49,070	(5,870)	47,150
Option 2	-	(910)	(41,070)	256,930	2,680	50,100	(8,200)	123,650
Option 3	-	(990)	(41,190)	367,680	3,360	52,330	(9,680)	176,740

Source: Steer Davies Gleave analysis

Table 10.11: Quantitative impacts: minimum perceived threat level -10 points (2050)

Option	Business information obligations	Small and Medium Enterprises	Consumers' ability to benefit from the internal market	Disproportionate impacts on individual Member States or regions	Right of citizens to move freely	Change in rail market share
Units:	FTEs	Million PKM	Million PKM	%	-	%
Option 1	1,180	3,570	5,420	39.4%	-	0.4%
Option 2	8,130	9,050	13,780	32.3%	-	1.1%
Option 3	10,290	13,110	19,980	47.1%	-	1.6%

Source: Steer Davies Gleave analysis

10.22 The perceived threat level is fundamental to the calculation of a number of impacts since it affects passenger demand under each option, and changes to the assumed threat level therefore affect a wider range of results. However, the positive effects of all options on growth and employment, fuel and energy consumption and a number of non-monetised impacts remains substantial even when improvements to the perceived threat level arising from the options are reduced significantly. Moreover, the ranking of options is not affected.

Qualitative assessment

Scored impacts

10.23 As described in Chapter 9, we scored the performance of each policy measure on a scale from ±3. The policy measure considered to have the largest impact defines the range of scores. Policy measures considered to have negligible impacts were assigned a score of zero. All other policy measures were then assigned a score based on their performance relative to these reference points. Impacts for each policy measure were then aggregated into policy options using a simple arithmetic mean.

10.24 The results of this exercise are reported in Table 10.12 below. We provide additional details of the scoring for each policy measure in Appendix F.

Table 10.12: Summary of qualitative scores

Option	Impacts on consumer choice and competition	Impacts on research and development	Impacts on products, production methods and technology	Impacts on trade and free movement with neighbouring countries	Social and distributional impacts	Impacts on workers' health, safety and dignity	Impacts on the safety and privacy of passengers and workers
Option 1	0.2	1.2	1.2	-0.6	1.0	1.2	-0.6
Option 2	0.0	1.1	0.6	-0.7	0.8	0.5	-0.5
Option 3	0.1	1.0	0.9	-0.7	0.5	0.8	-0.4

Source: Steer Davies Gleave analysis

11 Conclusions and recommendations

Introduction

The purpose of this study was to assess the most efficient and effective way of providing for the security of high-speed and international rail services through an assessment of options for policy intervention at the EU level. The study is based on a thorough investigation of security interventions and arrangements currently in place across the EU, drawing on both stakeholder consultation and a review of previous academic work as well as industry information sources. On the basis of the evidence collected, we:

- investigated the problem arising in relation to the security of rail services, identifying the underlying problem drivers and root causes and highlighting the key EU dimensions of the problem;
- defined a general objective for policy intervention at the EU level, as well as a series of specific objectives addressing different aspects of the problem identified, to guide the development of policy measures;
- specified a number of possible policy responses, building on the high level options of common mandatory requirements, guidelines and exchange of best practice described in our Terms of Reference and developing policy measures defined by reference to specific security interventions;
- undertaken a quantitative and qualitative assessment of a wide range of impacts of enhanced rail security, generating results at the EU and Member State level.

11.1 In the remainder of this chapter, we summarise our findings and conclusions and set out a number of policy implications and recommendations.

Problem definition and policy objectives

The problem

11.2 The results of our investigation of the problem were discussed in Chapter 4. In summary, we conclude that high-speed and international rail services across the EU are subject to an unacceptable threat of attack and that the associated railway infrastructure and rolling stock assets are subject to an unacceptably high risk of loss or damage. This has a number of adverse consequences, including risk to the security of passengers leading to the potential for diversion to other modes and a reduction in cross-border travel.

11.3 Our analysis indicates that this problem can be linked to:

- an insufficient understanding of the security threat, broadly defined to include both violent and non-violent crime, partly an inevitable result of the infrequency of certain types of security incident (particularly terrorist attacks) but also due to inadequate reporting and sharing of data;

- an inadequate response to the threat to the EU rail network as a whole, reflecting an understandable focus on specific threats arising at the national level (which vary significantly between Member States) and weak incentives to address ill-defined and poorly understood threats (particularly in the face of strong commercial pressures within railway undertakings and infrastructure managers across Europe);
- different approaches to the mitigation of security risks among rail industry decision-makers in different Member States, driven partly by cultural differences but, more importantly, by the application of inconsistent methodologies for assessing risk; and
- fragmentation of, and gaps in, security arrangements and responsibilities at both the national and EU level, a result of failures to coordinate security interventions on international services and accentuated by the growth of the international rail network.

Objectives

11.4 Given these findings, we defined a general objective, together with supporting specific objectives, providing a focus for the development of policy measures for addressing the problem.

11.5 Our general objective captured the need “to reduce the risk and impact of criminal acts on the European rail network”, recognising both the prevention and mitigation dimensions of the security issue. Note that this objective is broadly drawn to cover the entire European rail network rather than just the high-speed and international rail services that are the focus of this study. This is consistent with the need for decision-makers to consider the implications for other types of services when implementing security interventions on the high-speed and international networks, while reflecting the fact that many measures primarily intended to reduce security risks on one type of service may in practice simultaneously reduce similar risks on others.

11.6 Our specific objectives are aligned to different aspects of the problem definition and are reproduced in the table below.

Table 11.1: Specific objectives

Problem drivers (See Figure 4.2)	Specific objective	Rationale/comment
Insufficient understanding of the threat	**Shared EU understanding** Ensure relevant stakeholders have a more thorough and shared understanding of the security threat across the EU.	While the problem is partly the result of underlying data limitations, more could be done to ensure that rail industry and other stakeholders across the EU share a better understanding of the threat.
Inadequate response to the threat	**Reflect EU-wide benefits** Ensure that the response to the threat adopted by the industry takes full account of the economic and social benefits of security interventions across the EU.	There is a need to address externalities, in the form of security benefits that are not taken into account in commercial decision-making. At the same time, the economic and social benefits of security interventions need to be fully considered by public sector decision-makers determining investment priorities.
Different approaches to mitigation in Member States	**Consistent risk assessment** Ensure that mitigation of the security threat in different Member States is based on a consistent assessment of underlying risks.	While the specific security interventions adopted in different Member States will vary according to circumstances, it is important that common risks are assessed using the best methodologies available to the industry.
Fragmentation and gaps in security coordination	**Holistic and coordinated approach** Ensure that the security threat to high-speed and international rail services is addressed in a holistic and coordinated manner.	Mitigation measures should be applied consistently and coherently to an entire service or group of services, so that measures employed on one part of a journey cannot be circumvented or undermined by perpetrator actions taken on another part.

Source: Steer Davies Gleave

Policy options

11.7 We have developed three policy options on the basis of a "bottom-up" approach involving:

- consideration and selection of specific security interventions that can be expected to reduce the frequency and/or impact of security failures, drawing on industry literature and stakeholder consultation responses;
- packaging of interventions to define a series of policy measures addressing one or more of the specific objectives identified above; and
- in turn, packaging policy measures into three policy options, each of which addresses all of the specific objectives to some degree.

11.8 The options provide for progressively greater degrees of intervention, with each successive option delivering an incremental improvement in the security of high speed and international rail services. They are summarised in the table below, reproduced from Chapter 8.

Table 11.2: Policy options

Option					Mandatory/ guidelines
1: minimal	2: intermediate	3: comprehensive		Policy measure	
●	●	●	1A	Reporting and monitoring national security data	M
		●	1B	Researching and disseminating worldwide security data	G
●	●	●	2A	Emergency egress and access to stations	G
		●	2B	Blast-resistant features on stations	G
		●	2C	Blast-resistant features on trains	G
●	●	●	3E	S/SMS threat level protocols	G
	●	●	3A	S/SMS ensure exchange of information by relevant parties	M
	●	●	3C	S/SMS contingency planning and incident recovery	M
	●	●	3F	S/SMS liaison, incident response, drills and exercises	G
		●	3B	S/SMS recording of vulnerabilities and inspection regimes	M
		●	3D	S/SMS contingency IT, communications and spares	G
●	●	●	4A	CCTV on stations, with recording and facial recognition	M
●	●	●	4B	CCTV on trains, with recording and facial recognition	M
	●	●	4C	Deploying staff where they can observe	G
	●	●	4F	Staff vetting and access controls	G
		●	4D	Training station/train staff in risk and behaviour monitoring	G
		●	4E	Awareness promotion among passengers	G

Source: Steer Davies Gleave analysis

11.9 As indicated, all three options involve a mix of mandatory requirements and guidance. Based on a review of the adoption of Commission guidance, which suggested mixed experience in terms of both awareness of, and adherence to, previous guidance, we consider that policy measures should be specified in mandatory requirements where possible. However, in some cases it will be difficult to specify in advance standards or processes to be applied in a wide range of circumstances, and guidance is likely to be more appropriate. This is particularly true of specific staff-related measures such as training, and measures relating to the design of trains and stations, which will need to vary between networks, routes and even individual locations according to the type of service operated and its use.

Results of the assessment

11.10 As discussed in the previous chapter, on the basis of the MCA we have concluded that Option 3, the most comprehensive of the options, is the preferred choice. This reflects the significant economic growth and employment opportunities and the environmental benefits and energy savings generated by the increase rail travel arising under this option. It also reflects additional benefits captured through the qualitative assessment, including dissemination of new technologies and products and workers' health and safety. We have therefore concluded that

there is a case for intervention at the level of the European Union across a number of aspects of security, in particular:

- monitoring, reporting and exchange of security information;
- the design of trains and stations to mitigate the impact of security failures;
- risk assessment and contingency planning; and
- monitoring and awareness of security risks on the ground.

11.11 We also note that all three options deliver significant benefits, and that as they have been designed to provide for progressively greater levels of intervention, they could be implemented incrementally. Such an incremental approach could begin the introduction of a framework for reporting, coupled with guidance on aspects of station design and threat level protocols, and progress through to the development of standards on CCTV and further guidance on staff training and deployment.

Policy implications and recommendations

11.12 Given the results of the impact assessment, we make the following recommendations for improving the security of high-speed and international rail services operating within the EU.

Recommendation 1: reporting and monitoring of security data

11.13 **We recommend that the Commission establishes a Union-wide framework for reporting and monitoring of data relating to the security of high speed and international rail services.** Such data will include indicators of the incidence and effects of crime by category, and should be reported according to a standard format and common definitions of crime and types of rail service. The Commission should also establish a central capability for monitoring and disseminating data, analogous to the rail market monitoring survey reporting framework.

11.14 **The monitoring framework should be supplemented with guidance on areas for further research and exchange of information on rail security beyond the European Union.** This should identify and, as appropriate, disseminate international sources of data and research likely to inform ongoing discussion of rail security at LANDSEC and other forums and improve understanding of the security threat and ways of addressing it.

11.15 Together, the reporting framework and guidance will provide for more thorough analysis of the scale of the security threat and the impacts of security interventions than we have been able to undertake in this study. In line with the scope of our Terms of Reference, we have restricted this recommendation to data relating to high speed and international train services. However, in view of the difficulties of assessing the scale of the problem in relation to these services in isolation, as reported in Chapter 3, the Commission may wish to consider broadening it to apply to the rail industry more generally.

Recommendation 2: design of trains and stations for added security

11.16 **We recommend that the Commission, in collaboration with relevant international and national bodies, prepares guidance on the design of station access and egress with a view to improving security at stations used by high speed and international services. We also recommend that it prepares guidance on standards for blast-resistance on trains and at stations.** This will ensure that infrastructure managers and railway undertakings have access to information on best practice in these aspects of train and station design.

11.17 This recommendation is for guidance rather than mandatory requirements as we consider that, given the range of station locations and types of train service in operation, and the

different affordability constraints applying in different Member States, it will not be possible to define suitable standards that should apply in all circumstances. Transport authorities, railway undertakings, infrastructure managers and asset owners must have the flexibility to apply the standards or not, taking into account a range of factors, not least the security threat prevailing in the Member State concerned. Nevertheless, access to central guidance on standards applied elsewhere will enable such organisations to more easily assess the costs and benefits of applying best practice.

Recommendation 3: risk assessment and contingency planning

11.18 **We recommend that Member States should be required to ensure that rail organisations 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.**

11.19 **Such systems should be based on an explicit risk assessment process and subject to approval by an appropriate national regulatory body.**

11.20 In our view, the requirement for a Security Management System (SMS) including a number of common processes should be mandatory. This will provide for a minimum level of security on high speed and international services across the European Union. However, rail organisations must have the flexibility to adapt such systems to their particular circumstances, taking account of factors such as station location, types of service operated and the level of the security threat in the Member State concerned.

11.21 **We also recommend that the Commission, in collaboration with relevant national bodies, prepares guidance on:**

- **best practice in relation to the design of relevant information technology and communications systems to withstand attacks and the deployment of reserves and spare equipment for use following a security incident;**
- **appropriate liaison with emergency services and other relevant agencies as well as drills and exercises in incident response; and**
- **protocols for responding to changes in security threat levels identified at the European, national or local level.**

11.22 Again, the introduction of guidance will ensure that railway undertakings, infrastructure managers and other relevant industry organisations have access to information on best practice in relation to contingency planning and incident response while retaining the flexibility to adapt processes to local circumstances. At the same time, we suggest that the guidance could usefully be extended to include rail services more generally, as processes applying in the event of an attack on a high speed or international service are likely to be appropriate following attacks on other types of service.

Recommendation 4: monitoring and awareness of security risks

11.23 **We recommend that the Commission, in collaboration with relevant bodies, prepares common mandatory standards for CCTV on trains and stations, recovering requirements for**

recording capability as a minimum and, optionally, for facial recognition and real time monitoring. In addition, Member States should be required to identify responsibilities for undertaking CCTV monitoring activity. We consider that standards for a minimum level of monitoring should be mandatory, with the introduction of more sophisticated monitoring technology optional to enable rail industry organisations to assess their value case-by-case. However, requirements should be defined to ensure that where optional monitoring arrangements are adopted, mandatory standards for their capability are applied.

11.24 **We also recommend that the Commission should prepare guidance on:**

- **the appropriate deployment of staff for the purposes of observing behaviour on stations, drawing on principles of good practice already adopted;**
- **training of on-train and station staff in security risks and behaviour monitoring;**
- **campaigns promoting awareness of security among passengers; and**
- **processes for vetting of staff and limiting access to particularly vulnerable or sensitive locations.**

11.25 A central repository of guidance on good practice in each of these areas, coupled with proactive dissemination through LANDSEC and other channels, would provide helpful information to rail undertakings and other organisations charged with implementing security management systems. While they would be free to consider whether and how far to apply the guidance according to local circumstances, they could be required to demonstrate awareness and regular review of the guidance as part of their Security Management System SMS).

steer davies gleave

Appendices

A Literature review

Table A.1: Literature sources

	Title	Author(s)	Reference and/or date	High-speed and international rail travel	Terrorist attacks and their consequences	Security interventions	Legislation and acceptability	The costs of security interventions	The benefits of security interventions
1	Global terrorism index	Institute for Economics and Peace	2015		●			●	
2	A study on land transport security regarding high-speed trains	kwink groep	Ares(2014)3340512 - 09/10/2014			●			
3	Passenger station and terminal design for safety, security and resilience to terrorist attack: D7.1 – Socio economic potential impact	ISDEFE	29 November 2013						●
4	EU energy, transport and GHG emissions trends to 2050: Reference Scenario 2013	European Commission	2013						●
5	Terrorism as a strategic challenge for business: crisis management in the German rail travel industry	Sabine Tomasco and Thomas Baumert, Universidad Complutense de Madrid, Facultad de Ciencias Económicas y Empresariales	14 November 2012		●				
6	Commission Decision 2012/286/EU of 31 May 2012 on the creation of an Expert Group on Land Transport Security	European Commission	OJ L 142 of 01 June 2012			●			

	Title	Author(s)	Reference and/or date	High-speed and international rail travel	Terrorist attacks and their consequences	Security interventions	Legislation and acceptability	The costs of security interventions	The benefits of security interventions
7	Commission staff working document on transport security	European Commission	31 May 2012, SWD(2012) 143 final				●		
8	White Paper: Roadmap to a Single European Transport Area – towards a competitive and resource efficient transport system	European Commission	COM (2011) 144 final of 28 March 2011			●			
9	Journeys without borders	Howard Thomas et al, European Passengers' Federation	July 2010	●					
10	Explosives and incendiaries used in terrorist attacks on public surface transportation: a preliminary empirical examination	Brian Michael Jenkins and Bruce Robert Butterworth, Mineta Transportation Institute	March 2010		●				
11	Quantifying individuals' trade-offs between privacy, liberty & security: The case of rail travel in UK	RAND Europe	Transportation Research Part A: Policy and Practice 44(3), pp. 169-181. (10.1016/j.tra.2009.12.006)				●		●
12	Securing America's passenger rails - analysing current challenges and future solutions	Nicholas J. Armstrong et al, Maxwell School of Citizenship and Public Affairs, Syracuse University	04 June 2008			●		●	
13	Terrorism and rail security, testimony presented to the Senate Commerce, Science, and Transportation Committee	Jack Riley, Rand Corporation	23 March 2004	●					

	Title	Author(s)	Reference and/or date	High-speed and international rail travel	Terrorist attacks and their consequences	Security interventions	Legislation and acceptability	The costs of security interventions	The benefits of security interventions
14	Economic consequences of terrorism	OECD	OECD Economic Outlook, Edition 71, 2002		●				
15	The 1995 attempted derailing of the French TGV (High-Speed Train) and a quantitative analysis of 91 rail sabotage attempts	Brian Michael Jenkins, Bruce R. Butterworth, Jean-François Clair	MTI Report 09-12, March 2010		●	●			
16	Protecting surface transportation systems and patrons from terrorist activities: case studies of best security practices and a chronology of attack	Brian Jenkins and Bruce Butterworth, MTI	November 1997			●			
17	TETRIS - Terrorists in Europe Targeting Railway Infrastructure - Key Indicators	TETRIS Consortium	2014		●				
18	Passenger station and terminal design for safety, security and resilience to terrorist attack: D7.2 - Research into the acceptability of security options recommended by Securestation	DAPP	31 January 2014				●		●
19	Passenger station and terminal design for safety, security and resilience to terrorist attack: D7.3 - Gap analysis for current standards and guidelines	USFD	31 January 2014			●			
20	Passenger station and terminal design for safety, security and resilience to terrorist attack: D7.4 - Implementation roadmap	MTRS3 Solution and Services	31 January 2014				●		●
21	Formulating a strategy for securing high-speed rail in the United States	Mineta Transportation Institute	Research Report 12-03, March 2013			●			

	Title	Author(s)	Reference and/or date	High-speed and international rail travel	Terrorist attacks and their consequences	Security interventions	Legislation and acceptability	The costs of security interventions	The benefits of security interventions
22	Passenger station and terminal design for safety, security and resilience to terrorist attack: D2.2 - Scenario definition and user compilation of user requirements for improvements to current systems	InteCo	31 May 2012			●			
23	Passenger station and terminal design for safety, security and resilience to terrorist attack: D2.3 - Compendium for technologies for designing safety and security systems	MTRS3 Ltd	31 May 2012			●			
24	Passenger station and terminal design for safety, security and resilience to terrorist attack: D2.4 - Analysis of presentation of methods for design guidance	John McAslan & Partners	31 May 2012			●			
25	Passenger station and terminal design for safety, security and resilience to terrorist attack: D2.1 - Critical inventory report on threats, design strategies and risk assessment procedures in transport systems	J. Paragreen	30 November 2011			●	●		
26	Passenger station and terminal design for safety, security and resilience to terrorist attack: D3.1 - Evaluation report of the existing risk assessment methodologies and Securestation methodology	MTRS3 Ltd	15 October 2011			●			
27	Passenger station and terminal design for safety, security and resilience to terrorist attack: D8.1 - Dissemination plan	ISDEFE	29 August 2011			●			
28	Effects of the EU rail liberalisation on international rail passenger transport	Hedi Maurer et al	Association for European Transport and contributors, 2010	●					●

	Title	Author(s)	Reference and/or date	High-speed and international rail travel	Terrorist attacks and their consequences	Security interventions	Legislation and acceptability	The costs of security interventions	The benefits of security interventions
29	Terrorist attacks on public bus transportation: a preliminary empirical analysis	Jenkins, Butterworth and Shrum, MTI	MTI Report WP09/01 March 2010		●				
30	Designing and operating safe and secure transit systems: assessing current practices in the United States and abroad	Brian Taylor and others, MTI	MTI Report 04-05 November 2005			●			
31	Position Statement on the Commission Staff Working Paper on Land Transport Security	Deutsche Bahn	September 2012	●	●		●		●
32	Literature Review of London Underground and National Rail (LUNR) High Throughput Passenger Screening	UK Home Office	August 2012	●		●		●	

B Stakeholder questionnaires

Table B.1: Stakeholder questionnaire

		Regulators	Infrastructure managers	Ministries	Railway undertakings	Pan-European
Services operated that are in scope						
1	Does your organisation deal with passenger services that are: • High-speed; • International; • High-speed and international?	√	√	√	√	
2	Do any of the trains in these categories share platforms with other types of services e.g. high-speed with commuter trains, international with domestic? If so, would it be possible either to use separate platforms or to secure and 'sweep' the platforms between services?		√		√	
High level threat assessment						
3	Does your organisation maintain a risk assessment process covering all types of risk which does (or could) include security risks?	√	√	√	√	
Relevant legislation and policy						
4	What legislation governs activity related to rail security in your country?	√	√	√	√	
5	Has the legislation remained unchanged for the last 5 years?			√		
6	Is new legislation being considered? If so, what is being proposed?			√		
Evolution of legislation and policy						
7	What has been the primary driver/motivation for security policy in the rail sector**?**			√		
Roles and responsibilities						

		Regulators	Infrastructure managers	Ministries	Railway undertakings	Pan-European
8	Which organisation (or individual) holds primary responsibility for rail security? What type of organisation is this (governmental/regulatory/police/other)			√		
9	What other organisations are involved in ensuring rail security?		√	√	√	
10	What security obligations does the station manager (organisation) have?	√	√			
11	What security obligations does the railway undertaking have?				√	
12	What security obligations does the infrastructure manager have?		√			
13	Are the security requirements generally prescriptive or output-based?		√	√	√	
Attribution of costs for security activity						
14	Please describe how costs are assigned for: • Patrolling of stations and other infrastructure • Other security activities, as appropriate		√		√	
15	Do you believe that the defined responsibilities within the sector bring together decision-making about what actions is taken and the responsibility for paying for these actions?	√	√	√	√	
Co-operation between different authorities and stakeholders						
16	Was your organisation involved in the development of current policy and legislation?	√	√	√	√	
17	Do you meet with other organisations that are involved in the maintenance of security? If yes then which organisations?		√		√	
18	Are some security policies developed specifically by rail sector actors?	√	√	√	√	
19	Are different approaches adopted for different types of passenger train services (such as high-speed/international/urban)?		√		√	
20	Are there multi-agency security plans in place for interchange stations not operated by a single organisation?		√		√	
Threat levels						

		Regulators	Infrastructure managers	Ministries	Railway undertakings	Pan-European
21	Is there a system for categorising the current level of threat (nationally or more specifically)?			√		
22	If there is such a system, does a change in the threat level lead to a change in the measures that are in place to protect the sector against attack?			√		
International cooperation						
23	Is your organisation involved in discussions/cooperation with similar bodies in neighbouring countries?	√	√	√		
24	Is your organisation involved in discussions/cooperation with any other type of organisation in neighbouring countries?		√	√		
25	How are operational decisions affecting international services taken?		√		√	
Research undertaken						
26	Has your organisation undertaken research into the effectiveness of different approaches to reducing the security threat to rail services?	√	√	√	√	√
27	Are you aware of research undertaken by others in the rail sector into the effectiveness of different approaches to reducing the security threat to rail services?	√	√	√	√	√
Dealing with incidents						
28	Do you have local contingency plans that deal specifically with terrorist attacks?		√		√	
29	Has your organisation been involved in exercises (live or simulated) for dealing with security incidents?		√		√	
30	Are the plans for responding to rail security incidents consistent with those for other types of incidents (rail accidents or non-rail security incidents)?		√		√	
31	Is there a regulatory requirement for staff to receive training related to responding to security threats?	√	√	√	√	
32	Are staff in your organisation given specific training in threat awareness? If so, how many staff are concerned and how much time per staff member is dedicated to this?		√		√	

		Regulators	Infrastructure managers	Ministries	Railway undertakings	Pan-European
33	Are staff in your organisation given specific training in reacting to a terrorist attack? If so, how many staff are concerned and how much time per staff member is dedicated to this?		√		√	
34	Is any training provided to [staff of] third parties (suppliers/station traders etc.)?		√		√	
Specific threats						
35	Does your organisation have plans that deal with the cyber-threats to the rail network? If so, have they been tested?		√	√	√	
36	Are there any plans in place to deal with chemical, biological or radiological weapons (CBR)?		√	√	√	
Adoption of options to be assessed						
37	On your network, are there any stations where access to the station (or parts of it) is restricted to those holding tickets? If 'Yes', please give further information.		√		√	
38	Do you have areas within stations where you take measures to avoid the formation of concentrations of people? If 'Yes', please give further information.		√		√	
39	What activity do you undertake to detect unusual behaviour in stations and trains?		√		√	
40	Do you have any services for which all passengers have to establish their identity in order to be able to travel? If so, what arrangements do you have in place for establishing whether individuals pose a threat to security? Also, please give information about how far in advance passengers must do this, whether it involves extra costs in ticket retailing and what checks are done on their identity when they travel.				√	
41	What procedures have you adopted to minimise the impacts of security alerts (in duration or in connection with evacuation etc.)?		√		√	
42	What training is provided to staff (and, where appropriate, third parties such as traders, cleaners etc.) in recognising unusual or suspicious behaviour or events?		√		√	

		Regulators	Infrastructure managers	Ministries	Railway undertakings	Pan-European
43	What training is provided to staff (and, where appropriate, third parties such as traders, cleaners etc.) in taking appropriate action in the event of a terrorist attack?		√		√	
44	Are there any trains on your network for which passengers and their luggage are screened?		√		√	
45	Is screening of passengers and their luggage undertaken other than for accessing specific trains?		√		√	
46	How is general station patrolling undertaken? Is this under your organisation's control? If not, who controls it? How is it funded?		√		√	
47	Are there security patrols of trains (over and above the normal operational and commercial duties of rail staff)? Is this under your organisation's control? If not, who controls it? How is it funded?				√	
48	Do you identify elements of infrastructure that are particularly vulnerable to attack? If 'Yes', what action is taken to mitigate this?		√			
49	Do you believe that some train services on your network are more susceptible to terrorist attack? If 'Yes', which services are these?	√	√	√	√	
50	What measures are taken to protect remote, vulnerable elements of infrastructure from attack?		√			
Other views of respondents						
51	Please give your views upon the following with respect to your rail network: • how successful security arrangements have been to date in managing the security risk; • to what degree these arrangements have had additional benefits in reducing crime or anti-social behaviour; • the shortcomings of current arrangements; • likely developments; • expected impacts upon passenger behaviour and mode choice; and • what do you think represents best practice for an organisation such as yours?	√	√	√	√	
52	What is your highest priority for improving overall safety and security?	√	√	√	√	√

C Stakeholders contacted

Table C.1: Stakeholders contacted – government ministries

Member State	Organisation	Contact
AT	Federal Ministry for Transport, Innovation and Technology	Brigitte Raicher-Siegl
AT	Federal Ministry of the Interior	Wilhelm Seper
BE	Federal Ministry of Transport	Peter Geens
BE	Federal traffic police - Policy Development Department	Kris Depovere (Hoofdcommissaris/Commissaire Divisionnaire)
BG	Ministry of Transport, IT and Communications	Tsvetelina Ilieva-Yordanova
BG	Ministry of Interior of the Republic of Bulgaria	Stanislav Teofilov
CZ	Ministry of Transport	Jan Ilik
DE	Federal Ministry of Transport and Digital Infrastructure	Erich Schmid (Head of the Crisis Management Taskforce)
DE	Federal Ministry of Transport	Ricardo Liesig
DE	Federal Police Headquarters	Franz Volgl
DE	Federal Ministry of the Interior	Dirk Paulmann
DK	Danish Transport and Construction Authority	Julie Lange
DK	National Police Denmark	Jørn Pakula Andresen
EE	Ministry of Economic Affairs and Communications	Elari Kasemets
EE	Ministry of Interior – Public order and Criminal Policy Department	Einar Lillo
EL	Ministry of Infrastructure, Transport and Networks - Civil Emergency Planning Division	Konstantina Kosmidou
EL	Greek Ministry of Citizen Protection	Ioannis Panoliaskos
ES	Central Services Directorate General of Traffic	Carmen Girón
ES	Major Guardia Civil	Marcos Gomez Romera
IE	Public Transport Regulation Division, Department of Transport Tourism and Sport	Derek Rafferty
FI	Finnish Transport Safety Agency	Une Tyynilä
FI	National Police Board of Finland	Pasi Kemppainen
FR	Department of Transport Security	Pierre Brodin
FR	Ministry of Interior – General Direction of National Police	Julien Dufour

Member State	Organisation	Contact
HR	Ministry of Maritime Affairs, Transport and Infrastructure	Ljiljana Bosak
HR	Ministry of the Interior	Ante Gašpar
HU	Ministry of National Development	Peter Huszka
HU	Hungarian National Police Headquarters	Eva Dudas
IT	Ministry of Infrastructure and Transport	Alfonso Simoni
IT	Ministry of Interior	Paolo Cestra
LT	Ministry of Transport and Communications (NSA section)	Giedrė Ivinskienė
LT	Ministry of the Interior	Rytis Vosylius
LU	Department for Transport, Ministry of Sustainable Development and Infrastructure	Jeannot Poeker
LV	Ministry of Transport	Viktors Līpenīts
LV	The State Police of Latvia	Vineta Mistre
NL	Ministry of Infrastructure and the Environment	Monique Van Wortel
NL	Ministry of Justice	Bastiaan Schuring
PL	Ministry of Infrastructure and Development	Anna Krukowska
PL	Ministry of the Interior and Administration	
PL	Polish Ministry of Infrastructure and Construction	Marcin Rzeszewicz (Strategy Department)
PT	Institute for Mobility and Land Transport	Jose Alberto Franco
PT	Division of Transit and Bus Station Security	Gabriel Chaves Barao Mendes
RO	Ministry of Transport and Infrastructure – Railway Department	Dragos Anoaica
RO	General Inspectorate of Romanian Police	Marin Motoc
SE	Swedish Transport Administration	Carl Silfverswärd
SI	Ministry of Infrastructure	Milos Pregl
SI	Ministry of Interior, Police, Criminal Police Directorate	Albert Cernigoj
SK	Ministry of Transport, Construction and Regional Development	Mikuláš Sedlák
UK	Department for Transport, Land Transport Security	Andrew Cook

Table C.2: Stakeholders contacted – regulators

Member State	Organisation	Contact
AT	Rail Control Commission - Schienen-Control	Yvonne Rab
BE	National/Regulatory Service for Railway Transport And Operation Of Brussels National Airport	Bart Daneels
BG	Railway Administration Executive Agency	Daniela Nikolova
CZ	Office for Regulation of Railway Transport	Michaela Macova
DE	Bundesnetzagentur	Karsten Otte

Member State	Organisation	Contact
DE	The Federal Railway Authority - Eisenbahnbundesamt	
DK	Office for Regulation of Railway Transport	Marianne Bagge
EE	Estonian Competition Authority/Konkurentsiamet	Anvar Salomets
EL	Rail Regulatory Authority (RRA)	Dimitris Apostolinas
ES	Expert of the General Directorate of Railways	Carlos García Salvador
FI	Finnish Transport Safety Agency	Yrjö Mäkelä (Director of Rail Transport Sector)
FR	ARAF	Aude Le Lannier
HU	NKH - Railway Safety Authority	Péter Münnich
HR	ASZ - Railway Safety Agency	Želimir Delač
HR	Hakom (Croatian Regulatory Authority for Network Industries)	Željka Grgec (Head of Railway services)
IT	ART	Stefano Andreoli
LU	ILR	Mathias Behm
LU	ACF (National Safety Organisation)	
LV	State Railway Administration of Latvian Republic	Maris Ankalnins
NL	Netherlands Competition Authority (NMa)	Coen Timmerman
PO	UTK (The Office of Rail Transportation)	Michal Jaworski
PT	IMT/URF	Susanna Pinho
RO	Railway Supervision Council	
SE	Transportstyrelsen (Swedish Transport Agency)	Helene Jarefors
SI	Post and Electronic Communications Agency of the Republic of Slovenia (APEK)	Peter Picelj
UK	Office of Rail and Road	Martin Jones

Table C.3: Stakeholders contacted – railway undertakings

Member State	Organisation	Contact
AT	Association of Railways	Carmen Langer
AT	ÖBB (Österreichische Bundesbahnen)	Peter Blauensteiner (Head of Traffic Safety and Quality, ÖBB Personenverkehr AG) Ralf Mair (Safety Manager)
AT	Westbahn	Rosa Mayer
BE	SNCB	Hendrik Vanderkimpen (Head of Security)
BE	Thalys	Eric Martos (Safety Director)
CZ	České dráhy (ČD)	Ota Zachariáš
CZ	RegioJet	Jan Raym
DE	DB	Thorsten Buhrmester (Senior Consultant, DB security)
DE	Transdev	
DE	VDV	Marcus Gersinke (Head of Railway Business Management)

Member State	Organisation	Contact
DK	Danske Statsbaner (DSB)	Bjarne Lindberg Bak (Deputy Director, International Affairs)
EE	Estonian Railways	Marius Kupper (Head of Security)
EL	TrainOSE	Anna Delilabrou
ES	RENFE Operadora	David López Peinado
FI	VR	Mikael Aro (CEO)
FR	Thello	
FR	SNCF	Guillaume Pepy (CEO)
HU	GYSEV	Szilárd Liska
HU	MAV	Bernadette Kukoda (Director of International Relations)
HR	HŽ Putnički Prijevoz (HZPP)	Zeljko Ukic (Department for Safety and Protection)
IE	Irish Rail	Michael Power
IT	FS/TrenItalia (Italian Rail)	Maria-Cristina Fiorentino (Civil Protection and Anti-Mafia Manager)
IT	NTV	Luigi Celentano
LT	Lithuanian railways (LG)	Stasys Failydka (Director General)
LU	CFL	Christian Antinori (Manager)
LV	Latvian Railway	Lainis Kamaldins (Director of Security Department)
LV	Baltic Express	Juris Linde (Senior Inspector of Security Department)
NL	Nederlandse Spoorwegen (NS)	Frank Reitsma (Security Director)
PL	Polskie Koleje (PKP)	Wlodzimierz Ternawski (International Relations department)
PL	Rail Polska	
PT	CP (Comboios de Portugal)	Artur Jorge Aguiar Cerejo (Director of Security)
RO	CFR	Alexandru Emil Samoilenco (Safety Inspector)
SE	SJ	Jan Sjölund (Head of security)
SE	ASTOC	Björn Westerberg
SI	Slovenske železnice (SZ)	Dragutin Mate
SK	ŽSSK	Lubomir Hradiský
UK	First Group	Steve Montgomery (Managing Director)
UK	Stagecoach	Andrew Levy
UK	ATOC/Rail Delivery Group	Peter Lovegrove (Operational Resilience Manager)
UK	Eurostar International	Gareth Williams (Director of Strategy and Regulatory Affairs)

Table C.4: Stakeholders contacted – infrastructure managers

Member State	Organisation	Contact
AT/HU	GySEV/Raabbahn Raab-Oedenburg-Ebenfurter Eisenbahn AG	Oskar Pichler
AT	ÖBB Infrastruktur AG	Peter Kleinschuster (Head of Quality and Safety)
BE	Infrabel	Josef Decelle (Manager Punctuality and Security)
CZ	SŽDC	Anna Kodysová
DK	Banedanmark	Ole Christensen (Senior advisor Emergency and Security)
EE	AS Eesti Raudtee	
EL	OSE	Theofanopoulos Panagiotis (Chairman and CEO)
ES	ADIF	Antonio Bertomeu Fraisoli (Security Director)
FI	Liikennevirasto	Marko Tuominen (Head of Traffic and Work Safety Unit)
FR	SNCF Réseau	Xavier Epitalon, CSO (Head of Security and Defence)
FR	Lisea	Emmanuel Dalmar (Commercial Director)
FR/UK	Groupe Eurotunnel	Dominique Schmitlin (Security and Fire Safety (FLOR) Director Concession)
HR	HŽ Infrastruktura	Department for Security and Defence
HU	GYSEV Rail Infrastructure Business Division	András Riegler
HU	MAV Hungarian State Railways Co.	Bernadette Kukoda (Director of International Relations)
LV	Latvian Railways	Edvīns Bērziņš (CEO)
NL	ProRail	Justus Hartkamp (Deputy Director Corporate Strategy)
PL	PKP Polskie Linie Kolejowe	Urszula Maszkiewicz
PT	Infraestruturas de Portugal	Rui Fonte (Deputy Director Security)
RO	CFR Infrastructură	Jean Nicolaos (Director for Communication and Foreign Relations)
SE	Trafikverket	Åsa Tysklind
SI	Železnica Srbije (ŽS)	Dušan Garibović (Director General)
SK	ŽSR - Železnice Slovenskej Republiky (ŽSR)	Miroslav Zeman, Security Manager
UK	Network Rail	Guy Huckle (Operational Security and Contingency Planning Manager)
UK	HS1	Chris Lord (Train Operations Assurance Manager)

Table C.5: Stakeholders contacted – pan-European organisations

Organisation	Contact
CER	Alena Havlova (Digital and Security Adviser)
EIM	Bartłomiej (Bartek) Jesionkiewicz, Manager (Security Affairs)
European Organisation for Security (EOS)	Eda Aygen (Communication Manager)
European Passengers' Federation (EPF)	Christopher Irwin
COLPOFER	Maria Cristina Fiorentino

Organisation	Contact
RAILPOL	John Laene
UIC (International Union of Railways)	Grigore Havarneanu (Research Advisor - Security Division)
UITP	Andrea Soehnchen
UNECE	Francesco Dionori

Breakdown of responses

Ministries

Table C.6: Ministries responses

Stakeholder	Form of response		
	Telephone interview	Written response	Workshop/ face to face
Federal Ministry of Transport (BE)	✓		
Federal traffic police - Policy Development Department (BE)	✓		
Ministry of Transport (CZ)	✓		
Federal Ministry of Transport and Digital Infrastructure (DE)			✓
Federal Ministry of Transport (DE)			✓
Federal Police Headquarters (DE)			✓
Federal Ministry of the Interior (DE)	✓		✓
Danish Transport and Construction Authority (DK)			
Greek Ministry of Citizen Protection (EL)		✓	
Public Transport Regulation Division, Department of Transport Tourism & Sport (IE)	✓		
Finnish Transport Safety Agency (FI)	✓		
Department of Transport Security (FR)		✓	
Ministry of Interior – General Direction of National Police (FR)		✓	
Ministry of Maritime Affairs, Transport and Infrastructure (HR)		✓	
Ministry of National Development (HU)		✓	
Ministry of Infrastructure and the Environment (NL)	✓		
Ministry of Justice (NL)	✓		
Polish Ministry of Infrastructure and Construction (PL)	✓		
Swedish Transport Administration (SE)	✓		
Ministry of Infrastructure (SI)	✓		
Ministry of Interior, Police, Criminal Police Directorate (SI)	✓		
Ministry of Transport, Construction and Regional Development (SK)		✓	
Department for Transport, Land Transport Security (UK)	✓		

Regulators

Table C.7: Regulator responses

Stakeholder	Form of Response		
	Telephone Interview	Written Response	Workshop/Face to Face
Office for Regulation of Railway Transport (CZ)		✓	
NKH - Railway Safety Authority (HU)		✓	
Transport Authority (NSAT) (SK)	✓		
Office of Rail and Road (UK)			✓

Railway undertakings

Table C.8: Railway undertakings responses

Stakeholder	Form of Response		
	Telephone Interview	Written Response	Workshop/Face to Face
ÖBB Österreichische Bundesbahnen (AT)	✓		
Westbahn (AT)	✓		
Thalys (BE)	✓		
Bulgarian State Railways (BDŽ) (BG)			✓
České dráhy (ČD) (CZ)		✓	
DB (DE)			✓
VDV (DE)			✓
Danske Statsbaner (DSB) (DK)	✓		
RENFE Operadora (ES)		✓	
SNCF (FR)			✓
GYSEV (HU)		✓	
HŽ Putnički Prijevoz (HZPP) (HR)	✓		
Irish Rail (IE)	✓		
FS/TrenItalia (Italian Rail) (IT)	✓		
JSC "Lithuanian railways"/Lietuvos geležinkeliai (LG) (LT)		✓	
SJ (SE)	✓		
Slovenske železnice (SZ) (SI)	✓		
Železničná spoločnosť Slovensko, a.s. (ŽSSK) (SK)		✓	
ATOC/Rail Delivery Group (grouping of RUs and IMs) (UK)	✓		
Eurostar International (UK)	✓		

Infrastructure managers

Table C.9: Infrastructure managers responses

Stakeholder	Form of Response		
	Telephone Interview	Written Response	Workshop/Face to Face
ÖBB Infrastruktur AG (AT)	✓		
Infrabel (BE)	✓		

Stakeholder	Form of Response		
	Telephone Interview	Written Response	Workshop/Face to Face
National Railway Infrastructure Company (BG)			✓
Banedanmark (DK)	✓		
SNCF Réseau (FR)			✓
GYSEV Rail Infrastructure Business Division (HU)		✓	
MAV Hungarian State Railways Co. (HU)	✓		
ProRail (NL)	✓		
Infraestruturas de Portugal (PT)	✓		
Trafikverket (SE)	✓		
Network Rail (UK)	✓		
HS1 (UK)	✓		

Pan-European organisations

Table C.10: Pan-European organisations responses

Stakeholder	Form of Response		
	Telephone Interview	Written Response	Workshop/Face to Face
CER			✓
EIM			✓
European Organisation for Security (EOS)			✓
European Passengers' Federation (EPF)	✓		
COLPOFER	✓		
RAILPOL	✓		
UIC (International Union of Railways)			✓
UITP	✓		
UNECE		✓	

D Stakeholder consultation findings

This Annex has been removed from open publication in order to protect the data privacy of stakeholders who participated in this study.

E Approach to analysis and assumptions

Introduction

E.1 Assumptions used to estimate the impact of the shortlisted policy interventions have been taken from a variety of sources and are detailed in this appendix. Where possible, we have attempted to use publically available data and studies to inform the impact assessment but this has not always been possible.

E.2 Our assumptions have been informed by:

- Eurostat data;
- the European Rail Timetable January 2016;
- desk research, particularly on the websites of Railway Undertakings (RUs) and Infrastructure Managers (IMs);
- information gathered on other studies we have worked on for Steer Davies Gleave; and
- our professional experience.

General assumptions

Direct benefits – Value of Statistical Life (VSL)

E.3 The benefits of implementing security interventions have been examined to a limited extent, and assumptions on the value of life and injury (ISDEFE (2013)), occupancy of different types of train (Maurer et al (2010)) and international rail passenger numbers (Maurer et all (2010)) are available. Our desk research suggests that the majority of international passenger journeys may take place on a small number of routes, and in some cases be dominated by a small number of regular commuters. We have, as yet, found no consistent source of data on high speed rail passenger numbers and are aware that rail operators may not gather or publish such specific data. As with information on costs, there is nothing approaching a “security benefit manual” which would enable to stakeholders to identify the benefits of individual security measures. ISDEFE have shown how, with sufficient data and assumptions, it is possible to evaluate the benefits of a particular intervention at an individual station, although they conclude that the intervention may fail a strict cost-benefit test.

E.4 For a given change in the frequency and nature of terrorist attacks we have made estimates of:

- the cost of direct damage and values of life and injury;
- first response costs; and
- compensation costs.

Value of a statistical life in the EU (fatalities and injuries)

Degree of injury	Value (at 2012 prices)
Fatality	€1,785,000
Severe injury	€240,000
Slight injury	€19,000

Source: ISDEFE, socio economic potential impact, quoting HEATCO

E.5 We estimated direct benefits by calculating the average yearly loss of life as a result of attacks (between 1975 and 2015, based on RAND database) and dividing it by the total threat level.

Direct benefits by Member State

Member State	Yearly Direct Benefit in 2002 €s (killed)	Yearly Direct Benefit in 2002 €s (Seriously Injured)
BE	€572,557	€380,140
BG	€44,070	€26,192
CZ	€129,690	€76,830
DK	€576,400	€311,784
DE	€580,243	€350,217
EE	€61,483	€35,495
IE	€372,739	€206,176
ES	€293,964	€159,041
FR	€564,872	€344,721
IT	€374,660	€210,337
CY	€122,965	€70,914
LV	€48,033	€28,014
LT	€48,033	€29,007
LU	€610,984	€416,437
HU	€76,853	€45,037
MT	€174,841	€97,554
NL	€622,512	€361,209
AT	€461,120	€275,144
PL	€89,342	€53,243
RO	€51,083	€30,360
SI	€132,572	€75,570
SK	€53,797	€32,136
FI	€455,356	€264,037
SE	€489,940	€312,929
UK	€634,040	€358,919
PT	€140,257	€81,982
EL	€146,021	€83,585
HR	€78,094	€46,414

Staff time

E.6 We estimated the costs of security interventions by estimating the hours required by each staff member taking part and estimating the total number of additional staff required to cover them. To arrive at this estimation we extracted data on railway staff numbers from Eurostat data on employment in principal railway enterprises and estimated the proportion working on high-speed/international services as follows using our professional judgement.

Proportion of staff working on High Speed and / or International services by Member State

Member State	Proportion of Railway Staff working in High Speed / International Services
BE	High
BG	Low
CZ	Medium
DK	Medium
DE	High
EE	Low
IE	Low
EL	Low
ES	High
FR	High
HR	Low
IT	High
CY	–
LV	Low
LT	Low
LU	Medium
HU	Medium
MT	–
NL	Medium
AT	Medium
PL	Medium
RO	Low
SI	Low
SK	Medium
FI	Low
SE	Medium
UK	Medium
PT	Low

E.7 We have estimated that if a high majority of railway staff are likely to work on high-speed and International rail services it should equate to 75% of the total railway staff, medium to 50% and low 25%. The selection has been based on the baseline report whereby an estimate of total high-speed and international rail services by Member State is provided.

Costs passed on to the passenger

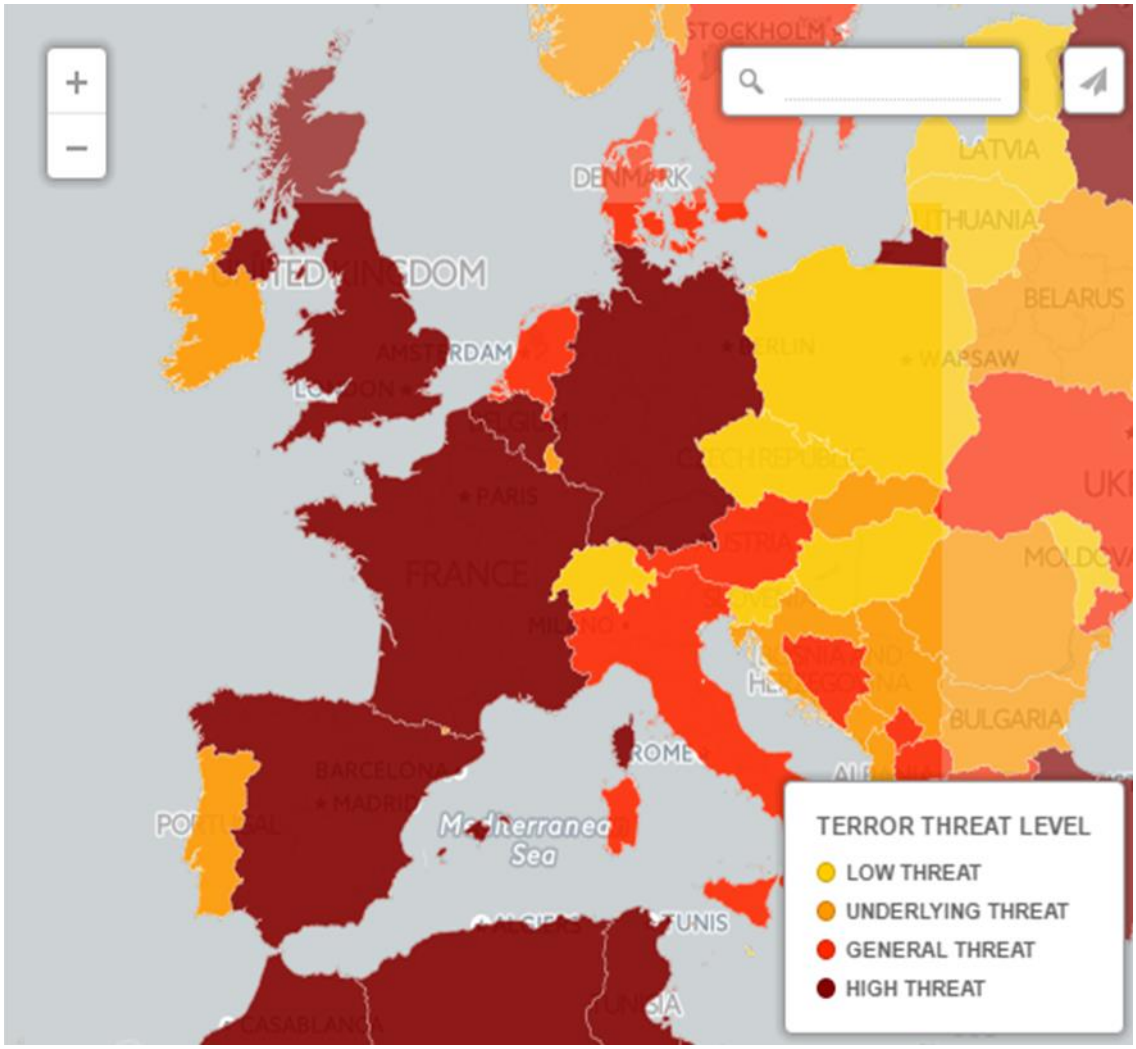
E.8 Based on the majority of the security interventions being addressed to IMs and station managers, we have not factored these costs being passed onto passengers.

E.9 On the security interventions that would affect RUs, while it is possible to make a quantitative assessment of the increase in costs of interventions to RUs, the degree to which this may translate into increases in costs to rail users must be the result of a judgement. Some increases may pass through, particularly where they apply to all competing operators within the mode but the inter-modal competitive pressure will moderate the degree to which this is possible. We are able to make effective qualitative judgements in this domain due to extensive experience in the provision of advice on management of demand and revenue.

RP1: Threat level protocol

E.10 The threat level used in the impact assessment is based on the map of threat levels indicating the likelihood of a terrorist attack provided by the UK Foreign Office (FCO).

European terrorist threat as assessed by the UK Foreign Office



Source: Foreign and Commonwealth Office

E.11 Information is gathered by the FCO via local knowledge from British embassies abroad and intelligence services and leads to the following categorisation:

- A high threat from terrorism: a high level of known terrorist activity.
- A general threat from terrorism: some level of known terrorist activity.
- An underlying threat from terrorism: a low level of known terrorist activity.
- Low threat from terrorism: no or limited known terrorist activity.

E.12 This threat level is reviewed monthly and updated if the FCO become aware of an incident that might affect a particular area.

E.13 Using the threat level categorisation High threat to Low Threat, we have assigned values to Member States and grouped them accordingly.

Threat level by Member State

UK Foreign Office threat level	Scale used in modelling	Member States experiencing indicated threat level
	1	
Low threat	2	Czech Republic, Estonia, Finland, Hungary, Latvia, Lithuania, Poland, Slovenia
	3	
Underlying threat	4	Bulgaria, Croatia, Ireland, Luxembourg, Portugal, Romania, Slovak Republic
	5	
General threat	6	Austria, Denmark, Sweden, Greece, Italy, Netherlands
	7	
High threat	8	Belgium, France, Germany, Spain, UK
	9	
State of emergency	10	

Source: Steer Davies Gleave assessment based on UK Foreign Office information and stakeholder consultation responses

E.14 If the EU introduces legislation requiring rail sector in Member States to have in place documented procedures for responding to the prevailing threat level and any changes in that level that may take place, this measure should be effective almost immediately. We have estimated a 10-year lead-in merely to reflect the fact that there will inevitably be a learning-curve for all parties involved. While most Member States will be able to roll out this measure relatively quickly, we have assumed that a few will prove slow to respond - in large part due to the sensitivities of the agencies concerned and / or legal constraints.

Impact assumptions

Impact	Data / Assumptions used	Source
Free movement of goods, services, capital and workers	Changes to Journey Times	Study on the price & quality of rail services, SDG, 2015 Passenger Demand Forecasting Handbook version 5.1 Section B

Impact	Data / Assumptions used	Source
	Changes to Passenger Journeys	Study on the price & quality of rail services, SDG, 2015 Passenger Demand Forecasting Handbook version 5.1 Eurostat PRIMES Model
Impacts on government administration	Direct Costs	Eurostat
Consumer prices	Changes to Fare Level	Cost & contribution of the rail sector, SDG, 2015 Study on the price & quality of rail services, SDG, 2015
	Passenger Journeys	Study on the price & quality of rail services, SDG, 2015 Passenger Demand Forecasting Handbook version 5.1 Eurostat PRIMES Model
Economic growth and employment	Changes to Passenger Journeys	Study on the price & quality of rail services, SDG, 2015 Passenger Demand Forecasting Handbook version 5.1 Eurostat PRIMES Model
	Journey purpose Split	Based on PDFH guidance based on journey lengths
	GDP per Capita	Eurostat
	GDP Growth	OECD
	Diversion Factors	TRL, the demand for public transport a practical guide, 2004
Job creation and destruction	Direct Jobs	Eurostat
	GDP per Capita	Eurostat
Deterrence and detection	Changes to Perceived Security Level	Passenger Demand Forecasting Handbook version 5.1 Section B UK Foreign Office Threat Level ratings EU Terrorism Situation and Trend Report (TE-SAT) 2016
	Changes to Passenger Journeys	Study on the price & quality of rail services, SDG, 2015 Passenger Demand Forecasting Handbook version 5.1 Eurostat PRIMES Model
	Direct Benefits	RAND Database of Worldwide Terrorism Incidents ISDEFE (2013) EIM Metal Theft Position Papers Graffolution 2014

Impact	Data / Assumptions used	Source
Fuel and energy consumption	Rail and Car Emissions per PKM	EEA, Specific CO2 emissions per passenger-km and per mode of transport in Europe, 2013
	Carbon Cost	EU Reference Scenario 2050
Additional resources	Direct Costs	Eurostat
Business information obligations	Direct Jobs	Eurostat
Consumers' ability to benefit from the internal market	Changes to Passenger Journeys	Study on the price & quality of rail services, SDG, 2015 Passenger Demand Forecasting Handbook version 5.1 Eurostat PRIMES Model
	Journey purpose Split	Based on PDFH guidance based on journey lengths
	Changes to Passenger Journeys	Study on the price & quality of rail services, SDG, 2015 Passenger Demand Forecasting Handbook version 5.1 Eurostat PRIMES Model
Small medium enterprises	Journey purpose Split	Based on PDFH guidance based on journey lengths
	SME Proportion	Eurostat
Disproportionate impacts on individual Member States or regions	Transport User Benefits	UK Department for Transport's Transport analysis guidance: WebTAG contains transport user benefits guidance.
Right of citizens to move freely		
Demand for passenger transport and modal split	Changes to Passenger Journeys	Study on the price & quality of rail services, SDG, 2015 Passenger Demand Forecasting Handbook version 5.1 Eurostat PRIMES Model
	Rail Mode Share	PRIMES Model

Specific assumptions on quantified impacts

1A Reporting and monitoring national security data

E.15 The value to be gained from the data will increase as the number of years for which it has been collected increases. In the very earliest years it will not be known how representative the data is or what the trends are. Once data capture has been underway for 5 years, it will have approached its full value in enabling comparisons over time.

E.16 We are basing this assumption on reported data availability on the basis of data prior to the introduction of these arrangements not being suitable for the purpose because it will not be normalised and hence will not be suitable for undertaking comparative evaluation. We established in 4.29 that reporting is currently limited in nature and that there is a lack of a framework to ensure consistency of approach. Our assumption that full value is achieved after

5 years is a judgement based upon our experience of regulatory economics. Whilst it is valuable after 10 years to have a greater set of data, this will only be marginally more effective in understanding trends and supporting decision-making that the 5-year view.

EA1: Blast resistant stations and trains

Cost to upgrade a station

E.17 We noted from a press release that the recent cost of the recent upgrade station facilities at Lille Flandres station was €18 million. We adopted this a paradigm of the size of station that falls into the category affected by this measure and thus used the €18 million as a working figure for the full cost of a station upgrade, to which the 25% proportion was applied to reflect the marginal cost of introducing measures for blast protection.

Life of rolling stock

E.18 We have assumed that the new requirements are applied not only to new vehicles but also to vehicles at half-life stage when they would have a thorough refurbishment.

E.19 We have reviewed a number of documents that discuss vehicle life-cycles in order to identify the value that we should assume for full-life. While rolling stock may, typically, be ordered on the assumption of a 30 year life, in practice this is often exceeded. The Network Route Utilisation Strategy (RUS) - Passenger Rolling Stock published by Network Rail in 2011 states "Historically the railway has considered commercial asset life as a nominal 30 years for diesel trains, and 35 years for electric trains. In theory, over the next ten years a quarter of the fleet would need to be replaced on this basis. Recent technical research suggests that the life of some rolling stock can be extended considerably."

E.20 Given this, and the fact that the majority of the in-scope trains will be electric, we have adopted a rolling stock life of 36 years.

E.21 Based on this assumption, refurbishment would be at 18 years' life and hence all passenger rolling stock would meet the new standards 20 years after the change in standards.

E.22 European Commission facilitate discussions in the rail sector, including the rolling stock supply sector on how rolling stock can be designed to ensure that trains will be better designed to dissuade or survive security attacks.

E.23 We have assumed that the new requirements are applied not only to new vehicles but also to vehicles at half-life stage when they would have a thorough refurbishment.

E.24 We have again assumed that the new approaches are applied not only to new vehicles but also to vehicles at half-life stage when they would have a thorough refurbishment.

EA2: Minimisation of unseen areas

E.25 The description of this measure given in Table 7.15 states that this would be achieved by means of coverage by CCTV. In this respect, it is a modifying measure, ensuring that CCTV is not only used to supervise normal passenger circulating areas but also to monitor areas that are not normally frequented but which are out of sight. We have assumed a lead time of 5 years.

EA9: Facial or behaviour recognition technology

E.26 Our baselining informed us that, whilst facial or behaviour recognition technology exists, the rail sector stakeholders' view was that it is not yet a mature technology. We noted comments

about the contrast between what could be achieved in a demonstration environment and the difficult conditions that characterise the rail environment, including climatic factors and lighting. This is not to say that there was a negative view of the prospects for the technology and it was suggested to us that in, say, 10 years, it could be expected to play a major part in the mitigation of the security threat. For this reason, we adopted a 10-year lead time for the measure. We considered that it was likely that the technology would only represent a marginal cost increase upon the cost of a normal CCTV installation.

EA14: Resistant radio and communications systems

E.27 There are various ways in which a radio system might be made more resistant. While in practice, a station manager or IM might adopt any of these, in order to quantify the cost of this intervention, we adopted the indicative approach of reducing vulnerability to attack by introducing additional antennae.

- Cost of each antenna -> €2,000;
- Installation cost per antenna -> €3,000;
- Antennae per station -> 4;
- Maintenance costs -> 20% of cost of each antennae, €400 per year per antenna.

E.28 The values used are not based upon any specific equipment but do reflect our experience of the costs of installing external electrical equipment in railway environments.

EA15: Contingency IT and communications systems

E.29 In order to quantify the cost of a contingency IT system we gave consideration to the equipment that might be kept as contingency equipment for use after a security incident. In such a case, it might not be possible for key station management functions to be undertaken from the normal location. In addition, the local area network might also not be functioning. For this reason, it was considered that typical contingency equipment might be ruggedised laptops, 4G dongles, ruggedised printers and emergency power supply.

E.30 The following table sets out what might be provided for the 'average' station.

Itemised Costs

Item	Quantity	Unit-Cost
Ruggedised Laptop	4	€1,500
Pre-paid 4G dongles	4	€100
Rugged printer	1	€300
Emergency power supply	1	€7,500
Anciliaries	1	€1,500

E.31 We assumed that 500 stations would require the above material with the number of stations by Member State distributed based on the proportion of total EU International/high-speed PKM.

EL1: Partnership with third parties

E.32 EU legislates that RUs and IMs must demonstrate in their security management system that suitable arrangements are in place to limit security risks imported to the rail sector by staff, contractors and third parties sharing infrastructure.

E.33 If the changes to arrangements in place in the sector are to make a real impact upon behaviours, they would best made at the time of renewal / replacement of contracts with the third parties concerned.

E.34 For some contracts, such as material supplies, this may be very easy to achieve. For others, there may be many years to run on the contract. Taking one example of contract life, the contact between SNCF Gares et Conexions and Relay, which is responsible for station trading on French stations, lasts for ten years[75].

E.35 Having considered this range of contract lengths, it was evident that it would not be possible to allow for a lead-in time that would always allow for awaiting the next renewal / replacement of the prevailing contracts but by allowing a 5 year transition period, a large proportion of them would be dealt with in this way.

EL2 Liaison with emergency services

E.36 During our baselining it was made clear that Member States recognise the importance of close working between the rail sectors and emergency services in order that the response to emergencies is as effective as possible. While there is always room for improvement, we ascertained that there are well-established arrangements for responding to classic railway incidents, such as collisions and fires. We ascertained that the collaboration was enforced by means of exercises, both live and in the classroom ('table-top').

E.37 Some stakeholders confirmed that they included security incidents in this training but it was clear that there is further work to be done to extend this to be sufficiently frequently to increase the likelihood that any decision-makers that find themselves responding to an incident will have participated in such exercises. Such training needs to be refreshed periodically and we would expect each key member of staff to participate every 5 years. We have used this figure as a proxy for the lead-in time this measure because, after this period, all of the key staff will have had their first set of training.

EA6 Recording of vulnerabilities in asset register

E.38 While the importance of maintaining an asset register may be accepted widely in principle across Member States, our baselining indicated that there remains much to do. Our desktop research included reviewing the UIC "Guidelines for the Application of Asset Management in Railway Infrastructure Organisations" and a presentation from the associated UIC "Asset Management Global Conference 2015", Assessment of your current asset management practices: presentation of the UIC's self-assessment tool". The current position that these documents refer to is one where many states have inherited documentation and processes from their historic railway organisations but there remains a need to apply a systematic new approach.

E.39 One of the presenters of the Conference paper, Andy Kirwan, Head of Asset Policy and Whole Life Costing at Network Rail set out in 2013 the asset management approach taken by Network Rail . This suggested that undertaking a full programme to introduce Asset Management takes 10 years. The development of 'Route asset management plans' is a sub-

[75] (https://www.gares-sncf.com/sites/default/files/field_files/2014-12/dp-nouvelle-offre-relay-en-gare-14-11-13.pdf).

component of this strategy and, given the tasks identified as preceding and following this task, we concluded that it was reasonable to assume that this would be achieved in 5 years.

EA4 Station duplicate access routes and walkways

E.40 The intention of this measure was to create duplicate access routes and walkways at stations that are significantly distinct from those normally used to access the station. The advantage of this would be that if part of the station is taken out of service due to a security incident, the remainder of the station could still be employed. Achieving this would require more than simply adding a door. It might well require, for example, the addition of a footbridge. Our assessment was that this would only be undertaken by station managers when a more general significant change was being undertaken. Based upon this assumption, the lead-in time is inevitably going to be lengthy and we considered 50 years to be appropriate.

EA3: Facilitation of emergency egress at stations

E.41 The work required for this measure is of a lesser scale than for EA4. In general terms it would be more than simply adding additional doors adjacent to those currently used – it would be to provide different points of egress. As they would only be required for emergency use, they would only need to accommodate one-directional flow and it would not be necessary to design them to avoid inconveniencing normal operations. In many cases they would be introduced during wider upgrade work but for many others the work would be an additional task. For this reason, we made the assumption that any in-scope stations for which wider upgrading was not taking place within 20 years would have the work to facilitate emergency egress undertaken and thus that this measure would have a lead-in time of 20 years.

EA10: Static detection equipment (CCTV)

E.42 Our baselining brought to light a significant difference in the extent to which CCTV has been employed in different Member States. This reflects wider cultural issues related to the degree to which surveillance is considered acceptable and national legal controls. Recognising this variability, we assumed a levelling-out of difference, with those Member States that currently have little provision making much more change than those that currently have fairly-comprehensive coverage. The move to the use of Internet Protocol for communications means that the requirement for extensive cabling is much-reduced from the early days of CCTV. Cameras can now be installed much more easily than had been the case.

SR2 Training in incident response

E.43 It is anticipated that the training will need to be given to a large proportion of staff. During baselining, we learnt that the duration of the necessary training is not very long. Our prior experience in supporting the business plans of train operators and station managers has informed us that only a limited number of staff can be trained at any one time due to the need to maintain service levels. We have therefore allowed for this to take a further five years from the completion of legislation to reach complete coverage.

E.44 Our findings during baselining indicated that very many of the procedures required for responding to security incidents are very similar in nature to those that are already in place for other types of incident. The additional task of ensuring that security incidents are addressed expressly is not very onerous. In the absence of legislation, we consider that a proportion of Member States will delay implementation for some while after publication of the guidance and, hence, we have allowed five years to reach complete coverage.

RP2: Contingency planning

E.45 EU legislates that railway undertakings and infrastructure managers must demonstrate in their security management system that security risks have been duly accounted for in contingency planning.

E.46 We consider that it will be necessary to allow a significant time for introduction of the security management systems after passage of the legislation as this will be a significant task. The security management system will not simply be an aggregation of existing material - it will need to reflect a considered, risk-based approach.

E.47 We drew a comparison with the findings of our 'Servrail' report in 2007 which showed that the Network Statements required by the 2001 Rail Directive were still not fully-populated at that time. Based upon this comparator, we consider it reasonable to presume that security management systems would be implemented within five years.

SR1: Training in risk and behaviour monitoring

E.48 It is anticipated that the training will need to be given to a large proportion of staff. During stakeholder consultation we learnt that the duration of the necessary training is not long but only a limited number of staff can be trained at any one time due to the need to maintain service levels.

E.49 In the absence of legislation, we consider that a proportion of Member States will delay implementation for some while after publication of the guidance and, hence, we have allowed five years to reach complete coverage.

SR3: Staff vetting

E.50 We extracted from Eurostat data concerning the number of railway staff in each Member State. Using our judgement we estimated the proportion working on high-speed/international services as follows:

E.51 We used the figure of UK rail employees[76] in addition to the turnover statistics for the UK[77] to estimate the total number of new employees every year. We then normalised this figure with the proportion of high-speed and international rail PKM. We assumed a unit of time to vet staff based on our judgement and then extrapolated it across the rest of the Member States based on total high-speed and/or international PKM.

SR5: Staff deployment

E.52 This is a measure that can be implemented very rapidly. Our assumption is that staff deployment will continue to be arranged such that members of staff can effectively patrol and monitor activity as part of their duties. This role is consistent with other business needs and does not necessarily represent an additional cost, especially for staff who would otherwise have periods of inactivity.

[76] http://www.people1st.co.uk/getattachment/Research-policy/Research-reports/State-of-the-Nation-Passenger-Transport-Travel/SOTN-PT-Summary-Rail.pdf.aspx

[77] http://www.stagecoach.com/~/media/Files/S/Stagecoach-Group/Attachments/pdf/rail-industry-faqs.pdf

RP3: Drills and exercises

E.53 During our baselining exercise, stakeholders confirmed that contingency plans need to be supported by exercises to test their effectiveness and to ensure that staff gain experience of responding to a security threat or incident in a simulated environment. This is consistent with the knowledge of our own rail operations professionals. Stakeholders also confirmed that such exercises play a particularly important in testing the effectiveness of interfaces between multiple agencies and ensuring that their respective plans are consistent. Their responses suggested that this principle is embedded in the rail sector, although there is wide variation in the extent to which exercises are held.

E.54 In a number of Member States we were told that there is scope for the number of exercises of all types to be increased significantly and for ensuring that terrorism is the subject of the some scenarios. One stakeholder stated that it deliberately uses the term “drill” rather than “exercise” to emphasise that this activity forms a part of “business as usual”. Our assumption was that this could be achieved quickly once it was decided to take action.

RP4: Post-incident recovery

E.55 Post-incident recovery is concerned with returning to near-to-normal operations as quickly as possible after an event, whether an accident, attack or false alarm. In each case, the aim is to ensure continued availability of rail services and to reduce any tendency of users to change to other modes. Our baselining confirmed that, in practice, Member States take similar approaches to recovering from other types of incident. For this reason, our assumption is that the lead-time for introducing change will be short.

PS2: Awareness promotion among passengers

E.56 The lead time for implementing this measure is very short. Rail sector actors already have departments that ensure that public safety messages are disseminated. The approaches taken to messages promoting awareness of security issues can be expected to be similar. In general, messages need constant re-enforcement, which indicates that the effects are of short duration and thus there is no lag in the benefits.

PS3: Targeted storage of contingency reserves

E.57 The report text makes mention of resources from megaphones to generators. It seems reasonable to consider that the latter end of the scale would be provided for by having 'call-off' contractors with equipment suppliers and thus there is no cost associated.

E.58 We assumed that each station has a stock of items costing €5,000 (not all items will be replaced each year but there will be a re-stocking requirement even if there are no incidents). Though storage space will be required, this is likely to be marginal to the amount of storage space that any station will inevitably have.

E.59 Based on the Baseline report, there are an estimated 500 stations likely to require this measure. We apportioned these costs to the different Member States pro rata with the estimated total high-speed/International PKMs from Eurostat.

Analysis

E.60 In addition to the central case estimates we have reported sensitivities based on alternative assumptions regarding:

- the reduction in frequency and severity of incidents delivered by short-listed security interventions; and
- the relative performance of security interventions on passengers' perceptions of security.

Calculations

E.61 Unless stated otherwise, all calculations in the table below are for each Member State in each year. All calculations are summed across Member States and growth throughout the assessment period as stated in the table.

Impact calculations – Monetised impacts

Impact	Summary	Calculation	Growth	Comments
Free movement of goods, services, capital and workers	Transport user benefits, or change in consumer surplus, arising only from any direct change in the GC due changes in journey times.	$(Base\ Journeys \times \Delta GC_{JT}) + (0.5 \times \Delta GC_{JT} \times \Delta Journeys_{JT})$	*Journeys* grow with PKM	ΔGC_{JT} Denotes changes in GC due only to changes to journey times. $\Delta Journeys_{JT}$ Denotes changes in journeys due only to changes to journey times.
Impacts on government administration	Proportion of Direct Costs	$Direct\ Costs \times Government\ Admin\ \%$	*Direct Costs* grow with PKM	Government Admin % is assumed to be: 20% for Common Mandatory Requirements, and 10% for Guidance
Consumer prices	Transport user benefits, or change in consumer surplus, arising only from any direct change in the GC due changes in fare level.	$(Base\ Journeys \times \Delta GC_F) + (0.5 \times \Delta GC_F \times \Delta Journeys_F)$	*Journeys* grow with PKM	ΔGC_F Denotes changes in GC due only to changes to fares. $\Delta Journeys_F$ Denotes changes in journeys due only to changes to fares.

Impact	Summary	Calculation	Growth	Comments
Economic growth and employment	The monetary value of the number of extra workers implied by the current level of business journeys per worker.	$\frac{\Delta Journeys \times Business\ \%}{Business\ Journeys\ per\ Worker} \times GDP\ per\ Capita \times$ Displacement	*Journeys* grow with PKM	$Business\ \%$ Denotes the proportion of journeys which are for business purposes Displacement factor (20%) represents the proportion of additional economic activity.
Job creation and destruction	The net change in jobs as a consequence of the implementation of security interventions.	$Direct\ Jobs \times Average\ Wage$	*Direct Jobs* grow with PKM	
Deterrence and detection	The Direct Benefits associated with reductions in the severity of incidents **and** The change in transport user benefits, or consumer surplus, associated with a change in perceptions of security levels.	*Direct Benefits* **+** $(Base\ Journeys \times \Delta GC_S) + (0.5 \times \Delta GC_S \times \Delta Journeys_S)$	*Direct Benefits* grow with GDP *Journeys* grow with PKM	ΔGC_S Denotes changes in GC due only to changes to security perceptions. $\Delta Journeys_S$ Denotes changes in journeys due only to changes to security perceptions.

Impact	Summary	Calculation	Growth	Comments
Fuel and energy consumption	Monetised impact of the net change in carbon emissions	$\boldsymbol{Base\ Emissions\ Cost_{Rail}} = Base\ PKM_{Rail} \times Emissions\ Factor_{Rail} \times Carbon\ Price$ => $\boldsymbol{\Delta Emissions\ Cost_{Rail}} = Base\ Emissions\ Cost_{Rail} \times (1 + \%\Delta PKM_{Rail})$ => $\boldsymbol{\Delta Emissions\ Cost_{Net}} = \Delta Emissions\ Cost_{Rail} \times \left(\frac{Emissions\ Factor_{Road}}{Emissions\ Factor_{Rail}}\right) \times DiversionFactor$	PKM growth based on EU Projections The *Emissions Factor* and *Carbon Price* grow in line with EU projections	The *Diversion Factor* is a substitution factor between road and rail PKM The *Emissions Factor*, for each mode, is the grams of CO2 emissions per passenger kilometre The Carbon Price is the € per gram of CO2 emitted
Additional resources	The Direct Cost of implementing each security intervention	$Direct\ Costs \times (1 - Government\ Admin\ \%)$	*Direct Costs* grow with PKM	*Government Admin %* is assumed to be: 20% for Common Mandatory Requirements, and 10% for Guidance

Impact calculations – Quantified impacts

Impact	Summary	Calculation	Growth	Comments
Business information obligations	The additional FTEs equivalent to the yearly employee hours required to meet new reporting levels	*Direct Jobs*	*Direct Jobs* grow with PKM	
Consumers' ability to benefit from the internal market	The change in business and commuter passenger kilometres	$\Delta PKM \times (Business\ \% + Commuter\%)$	PKM growth based on EU Projections	$Business\ \%\ and\ Commuter\%$ Denote the proportion of PKM which are for business or commuting purposes respectively

Small medium enterprises	The change in SME business and commuter passenger kilometres	$\Delta PKM \times (Business\ \% + Commuter\%) \times SME\%$	PKM growth based on EU Projections	$SME\%$ Denotes the proportion of workers employed in SMEs
Disproportionate impacts on individual Member States or regions	The proportion of total transport user benefits captured by the Member State with the largest benefits	$Max_{MS}(Base\ Journeys \times \Delta GC_T) + (0.5 \times \Delta GC_T \times \Delta Journeys_T))$	*Journeys* grow with PKM	ΔGC_T Denotes total changes in GC. $\Delta Journeys_T$ Denotes total changes in journeys. Max_{MS} Denotes maximum across Member States
Demand for passenger transport and modal split	The change in rail mode share arising from a change in demand	$Base\ Rail\ Mode\ Share \times (1 + \%\Delta PKM_{Rail})$	*Base Rail Mode Share* growth based on EU Projections	

F Qualitative scoring of policy measures

Impacts on consumer choice and competition (repeat for each impact)

Policy measure		Mandatory /guidelines	Qualitative score	Rationale for score
1A	Reporting and monitoring national security data	M	0	Our experience of working on studies involving data collection and analysis, for example, the cost and contribution study (2016) has led us to the informed decision that there is no link between the policy measure, impact and market behaviour. This policy measure: • will not lead to a reduction in consumer choice; • will have no effect on competition; and • will not lead to market segmentation.
1B	Researching and disseminating worldwide security data	G	0	Our experience of working on studies involving data collection and analysis, for example, the cost and contribution study (2016) has led us to the informed decision that there is no link between the policy measure, impact and market behaviour. This policy measure: • will not lead to a reduction in consumer choice; • will have no effect on competition; and • will not lead to market segmentation.
2A	Emergency egress and access to stations	G	0	Our experience of working on studies involving data collection and analysis, for example, the cost and contribution study (2016) has led us to the informed decision that there is no link between the policy measure, impact and market behaviour. This policy measure: • will not lead to a reduction in consumer choice; • will have no effect on competition; and • will not lead to market segmentation.
2B	Blast-resistant features on stations	G	0	Our experience of working on studies involving data collection and analysis, for example, the cost and contribution study (2016) has led us to the informed decision that there is no link between the policy measure, impact and market behaviour. This policy measure: • will not lead to a reduction in consumer choice; • will have no effect on competition; and • will not lead to market segmentation.

Policy measure		Mandatory /guidelines	Qualitative score	Rationale for score
2C	Blast-resistant features on trains	G	1	Our desk research and stakeholder consultation has highlighted that there is a possibility that this measure could have a minor positive impact on consumer choice. Trains with enhanced security features are a more attractive options to some passengers. This policy measure: • will not lead to a reduction in consumer choice; • has the potential to have no effect on competition; and • will not lead to market segmentation.
3E	SMS threat level protocols	G	0	Our experience of working on studies involving data collection and analysis, for example, the cost and contribution study (2016) has led us to the informed decision that there is no link between the policy measure, impact and market behaviour. This policy measure: • will not lead to a reduction in consumer choice; • will have no effect on competition; and • will not lead to market segmentation.
3A	SMS ensure exchange of information by relevant parties	M	-1	Our experience of working on studies involving data collection and analysis, for example, the cost and contribution study (2016) has led us to the informed decision that there could be a possible impact to competition based on the change in market behaviour. The sharing of commercial information could reveal practices that a competitor could make use of to gain a larger portion of the market. This policy measure: • will not lead to a reduction in consumer choice; • will have a minor effect on competition; and • will not lead to market segmentation.
3C	SMS contingency planning and incident recovery	M	0	Our experience of working on studies involving data collection and analysis, for example, the cost and contribution study (2016) has led us to the informed decision that there is no link between the policy measure, impact and market behaviour. This policy measure: • will not lead to a reduction in consumer choice; • will have no effect on competition; and • will not lead to market segmentation.
3F	SMS liaison, incident response, drills and exercises	G	0	Our experience of working on studies involving data collection and analysis, for example, the cost and contribution study (2016) has led us to the informed decision that there is no link between the policy measure, impact and market behaviour. This policy measure: • will not lead to a reduction in consumer choice; • will have no effect on competition; and • will not lead to market segmentation.

Policy measure		Mandatory /guidelines	Qualitative score	Rationale for score
3B	SMS recording of vulnerabilities and inspection regimes	M	0	Our experience of working on studies involving data collection and analysis, for example, the cost and contribution study (2016) has led us to the informed decision that there is no link between the policy measure, impact and market behaviour. This policy measure: • will not lead to a reduction in consumer choice; • will have no effect on competition; and • will not lead to market segmentation.
3D	SMS contingency IT, communications and spares	G	0	Our experience of working on studies involving data collection and analysis, for example, the cost and contribution study (2016) has led us to the informed decision that there is no link between the policy measure, impact and market behaviour. This policy measure: • will not lead to a reduction in consumer choice; • will have no effect on competition; and • will not lead to market segmentation.
4A	CCTV on stations, with recording and facial recognition	M	0	Our experience of working on studies involving data collection and analysis, for example, the cost and contribution study (2016) has led us to the informed decision that there is no link between the policy measure, impact and market behaviour. This policy measure: • will not lead to a reduction in consumer choice; • will have no effect on competition; and • will not lead to market segmentation.
4B	CCTV on trains, with recording and facial recognition	M	1	Our desk research and stakeholder consultation has highlighted that there is a possibility that this measure could have a minor positive impact on consumer choice. Trains with enhanced security features are a more attractive options to some passengers. This policy measure: • will not lead to a reduction in consumer choice; • has the potential to have no effect on competition; and • will not lead to market segmentation.
4C	Deploying staff where they can observe	G	0	Our experience of working on studies involving data collection and analysis, for example, the cost and contribution study (2016) has led us to the informed decision that there is no link between the policy measure, impact and market behaviour. This policy measure: • will not lead to a reduction in consumer choice; • will have no effect on competition; and • will not lead to market segmentation.

Policy measure		Mandatory /guidelines	Qualitative score	Rationale for score
4F	Staff vetting and access controls	G	0	Our experience of working on studies involving data collection and analysis, for example, the cost and contribution study (2016) has led us to the informed decision that there is no link between the policy measure, impact and market behaviour. This policy measure: • will not lead to a reduction in consumer choice; • will have no effect on competition; and • will not lead to market segmentation.
4D	Training station/train staff in risk and behaviour monitoring	G	0	Our experience of working on studies involving data collection and analysis, for example, the cost and contribution study (2016) has led us to the informed decision that there is no link between the policy measure, impact and market behaviour. This policy measure: • will not lead to a reduction in consumer choice; • will have no effect on competition; and • will not lead to market segmentation.
4E	Awareness promotion among passengers	G	0	Our experience of working on studies involving data collection and analysis, for example, the cost and contribution study (2016) has led us to the informed decision that there is no link between the policy measure, impact and market behaviour. This policy measure: • will not lead to a reduction in consumer choice; • will have no effect on competition; and • will not lead to market segmentation.

Impacts on research and development

Policy measure		Mandatory /guidelines	Qualitative score	Rationale for score
1A	Reporting and monitoring national security data	M	1	This option has the potential to stimulate research and development. Current reporting to the European Commission and the European Union Agency for Railways in the area of interoperability has fed into the work of developing Technical Specifications for Interoperability (TSIs). This demonstrates the possibility of a minor positive impact.
1B	Researching and disseminating worldwide security data	G	1	This option has the potential to stimulate research and development. Current reporting to the European Commission and the European Union Agency for Railways in the area of interoperability has fed into the work of developing Technical Specifications for Interoperability (TSIs). This demonstrates the possibility of a minor positive impact.
2A	Emergency egress and access to stations	G	2	This option will stimulate research and development. Any technical change in design will feed into the work of developing TSIs. This demonstrates the possibility of a positive impact.
2B	Blast-resistant features on stations	G	2	This option will stimulate research and development. Any technical change in design will feed into the work of developing TSIs. This demonstrates the possibility of a positive impact.
2C	Blast-resistant features on trains	G	2	This option will stimulate research and development. Any technical change in design will feed into the work of developing TSIs. This demonstrates the possibility of a positive impact.
3E	SMS threat level protocols	G	1	This option has the potential to stimulate research and development. Moreover this can be an opportunity for the European Commission and the European Union Agency for Railways to further develop the area of interoperability, feeding into the work of developing TSIs. This demonstrates the possibility of a minor positive impact.
3A	SMS ensure exchange of information by relevant parties	M	1	This option has the potential to stimulate research and development. Member States currently participate in sharing information via the National Safety Authority (NSA) Network and the Network of National Investigation Bodies (NIB). This has led to the creation of dedicated databases that informs all interested parties and feeds into the work of drafting the TSIs. This demonstrates the possibility of a minor positive impact.
3C	SMS contingency planning and incident recovery	M	1	This option has the potential to stimulate research and development. Member States having a threshold for an SMS could incentivise the investigation of preventative measures and efficient response. This demonstrates the possibility of a minor positive impact.

Policy measure		Mandatory /guidelines	Qualitative score	Rationale for score
3F	SMS liaison, incident response, drills and exercises	G	2	This option has the potential to stimulate research and development. Member States having a threshold for an SMS could incentivise the investigation of an efficient and effective response to a security incident. This demonstrates the possibility of a positive impact.
3B	SMS recording of vulnerabilities and inspection regimes	M	1	This option has the potential to stimulate research and development. Member States would be incentivised to find ways of limiting their vulnerabilities and having more efficient inspection regimes This demonstrates the possibility of a minor positive impact.
3D	SMS contingency IT, communications and spares	G	2	This option has the potential to stimulate research and development. Member States would be incentivised to find ways of having a more efficient communication system in the eventuality of a security incident. The stakeholder consultation and desk research has shown that cyber security is one of the most important concerns to stakeholders. This demonstrates the possibility of a positive impact.
4A	CCTV on stations, with recording and facial recognition	M	1	This option has the potential to stimulate research and development. Our stakeholder consultation and desk research has shown that a large majority of stakeholders already implement CCTV in stations. Facial recognition and advanced security monitoring is being researched already by a portion of stakeholders that we interviewed. This demonstrates the possibility of a positive impact
4B	CCTV on trains, with recording and facial recognition	M	1	This option has the potential to stimulate research and development. Our stakeholder consultation and desk research has shown that a large majority of stakeholders already implement CCTV in stations. Facial recognition and advanced security monitoring is being researched already by a portion of stakeholders that we interviewed. This demonstrates the possibility of a positive impact
4C	Deploying staff where they can observe	G	0	We do not believe that this option has the potential to stimulate research and development. There is no evidence of a link between staff deployment generating any research and development.
4F	Staff vetting and access controls	G	1	This option has the potential to stimulate research and development. In our stakeholder consultation feedback, staff vetting was an area in which stakeholders were interested. This leads us to make the assumption that any outcome of research and development undertaken would influence staff vetting. This demonstrates the possibility of a minor positive impact

	Policy measure	Mandatory /guidelines	Qualitative score	Rationale for score
4D	Training station/train staff in risk and behaviour monitoring	G	1	This option has the potential to stimulate research and development. In our stakeholder consultation feedback, training was an area in which stakeholders were interested. This leads us to make the assumption that any outcome of research and development undertaken would influence staff training. This demonstrates the possibility of a minor positive impact
4E	Awareness promotion among passengers	G	0	We do not believe that this option has the potential to stimulate research and development. There is no evidence of a link between staff deployment generating any research and development.

Impacts on dissemination of new production methods, technologies and products

Policy measure		Mandatory /guidelines	Qualitative score	Rationale for score
1A	Reporting and monitoring national security data	M	0	This measure does not facilitate the introduction and dissemination of new production methods, technologies and products.
1B	Researching and disseminating worldwide security data	G	1	The sharing of security data could lead to new production methods, technologies and products being developed.
2A	Emergency egress and access to stations	G	2	This measure would facilitate the introduction and dissemination of new production methods, technologies and products. It is assumed that any technical developments would be written into the Technical Specifications for Interoperability (TSIs).
2B	Blast-resistant features on stations	G	2	This measure would facilitate the introduction and dissemination of new production methods, technologies and products. It is assumed that any technical developments would be written into the TSIs.
2C	Blast-resistant features on trains	G	2	This measure would facilitate the introduction and dissemination of new production methods, technologies and products. It is assumed that any technical developments would be written into the TSIs.
3E	SMS threat level protocols	G	2	This measure would facilitate the introduction and dissemination of new production methods, technologies and products. The SMS may have to respond with different security technologies based on the threat level.
3A	SMS ensure exchange of information by relevant parties	M	0	This measure does not facilitate the introduction and dissemination of new production methods, technologies and products.
3C	SMS contingency planning and incident recovery	M	0	This measure does not facilitate the introduction and dissemination of new production methods, technologies and products.
3F	SMS liaison, incident response, drills and exercises	G	0	This measure does not facilitate the introduction and dissemination of new production methods, technologies and products.
3B	SMS recording of vulnerabilities and inspection regimes	M	1	This measure would potentially facilitate the introduction and dissemination of new production methods, technologies and products. Based on a vulnerability identified, there would be an incentive to find new technologies that might solve the problem.
3D	SMS contingency IT, communications and spares	G	1	This measure would potentially facilitate the introduction and dissemination of new production methods, technologies and products. There would be an incentive to implement new products and technologies to minimise any risks in the contingency plan.

Policy measure		Mandatory /guidelines	Qualitative score	Rationale for score
4A	CCTV on stations, with recording and facial recognition	M	2	This measure would facilitate the introduction and dissemination of new production methods, technologies and products. There would be an incentive to implement new products and technologies to minimise any risks to security.
4B	CCTV on trains, with recording and facial recognition	M	0	This measure does not facilitate the introduction and dissemination of new production methods, technologies and products.
4C	Deploying staff where they can observe	G	0	This measure does not facilitate the introduction and dissemination of new production methods, technologies and products.
4F	Staff vetting and access controls	G	0	This measure does not facilitate the introduction and dissemination of new production methods, technologies and products.
4D	Training station/train staff in risk and behaviour monitoring	G	2	This measure would facilitate the introduction and dissemination of new production methods, technologies and products. Staff would have to be trained in using the new technology.
4E	Awareness promotion among passengers	G	1	This measure would potentially facilitate the introduction and dissemination of new production methods, technologies and products. Passengers could possibly be updated via electronic applications.

Impacts on third neighbouring countries with which the EU has close trade, transport or free movement i.e. Schengen links

Policy measure		Mandatory /guidelines	Qualitative score	Rationale for score
1A	Reporting and monitoring national security data	M	0	This has no impacts on third neighbouring countries with which the EU has close trade, transport or free movement i.e. Schengen links. The security data will not have an effect on these areas.
1B	Researching and disseminating worldwide security data	G	0	This has no impacts on third neighbouring countries with which the EU has close trade, transport or free movement i.e. Schengen links. The security data will not have an effect on these areas.
2A	Emergency egress and access to stations	G	-1	This may have a minor impact on third neighbouring countries with which the EU has close trade, transport or free movement i.e. Schengen links. An international / cross-border service may have to take into account a European standard.
2B	Blast-resistant features on stations	G	-1	This may have a minor impact on third neighbouring countries with which the EU has close trade, transport or free movement i.e. Schengen links. A station in a third neighbouring country may have to take into account a European or commercial standard for an international / cross-border service.
2C	Blast-resistant features on trains	G	-2	This may have an impact on third neighbouring countries with which the EU has close trade, transport or free movement i.e. Schengen links. An international / cross-border service may have to take into account a European standard.
3E	SMS threat level protocols	G	1	This may have a minor impact on third neighbouring countries with which the EU has close trade, transport or free movement i.e. Schengen links. An SMS will have to take into account all destinations on the operating route. This could be of benefit to a third country that does not have a threat level protocol or threshold. This assumption is based on our stakeholder consultation which identified a difference in establishing threat levels across Member States.
3A	SMS ensure exchange of information by relevant parties	M	-2	This may have an impact on third neighbouring countries with which the EU has close trade, transport or free movement i.e. Schengen links. An SMS will have to take into account all destinations on the operating route and it may be difficult to ensure cooperation with all parties involved. This assumption is based on our stakeholder consultation which identified a potential difficulty in coordinating all parties involved.

Policy measure		Mandatory /guidelines	Qualitative score	Rationale for score
3C	SMS contingency planning and incident recovery	M	-1	This may have a minor impact on third neighbouring countries with which the EU has close trade, transport or free movement i.e. Schengen links. An SMS will have to take into account all destinations on the operating route and it may be difficult to ensure cooperation with all parties involved. This assumption is based on our stakeholder consultation which identified a potential difficulty in coordinating all parties involved.
3F	SMS liaison, incident response, drills and exercises	G	-1	This may have a minor impact on third neighbouring countries with which the EU has close trade, transport or free movement i.e. Schengen links. An SMS will have to take into account all destinations on the operating route and it may be difficult to ensure cooperation with all parties involved. This assumption is based on our stakeholder consultation which identified a potential difficulty in coordinating all parties involved.
3B	SMS recording of vulnerabilities and inspection regimes	M	1	This may have a minor impact on third neighbouring countries with which the EU has close trade, transport or free movement i.e. Schengen links. An SMS will have to take into account all destinations on the operating route. This could be of benefit to a third countries by having a unified and coordinated inspection regime and recording of vulnerabilities. This assumption is based on our stakeholder consultation which identified a difference in contracts across Member States
3D	SMS contingency IT, communications and spares	G	-1	This may have a minor impact on third neighbouring countries with which the EU has close trade, transport or free movement i.e. Schengen links. An SMS will have to take into account all destinations on the operating route and it may be difficult to ensure cooperation with all parties involved. This assumption is based on our stakeholder consultation which identified a potential difficulty in coordinating all parties involved.
4A	CCTV on stations, with recording and facial recognition	M	-2	This may have an impact on third neighbouring countries with which the EU has close trade, transport or free movement i.e. Schengen links. A station in a third neighbouring country may have to take into account a European or commercial standard for an international / cross-border service.
4B	CCTV on trains, with recording and facial recognition	M	-1	This may have a minor impact on third neighbouring countries with which the EU has close trade, transport or free movement i.e. Schengen links. It is assumed that any train crossing the border will already be equipped with the EU specified equipment.

Policy measure		Mandatory /guidelines	Qualitative score	Rationale for score
4C	Deploying staff where they can observe	G	1	This may have a minor impact on third neighbouring countries with which the EU has close trade, transport or free movement i.e. Schengen links. From our stakeholder consultation we have learnt that in the majority of Member States having staff deployed at stations makes passengers feel 'safer'.
4F	Staff vetting and access controls	G	-1	This may have a minor impact on third neighbouring countries with which the EU has close trade, transport or free movement i.e. Schengen links. Staff in these third countries may be subject to vetting procedures that they might not necessarily undergo in their country or it might be repeated.
4D	Training station/train staff in risk and behaviour monitoring	G	-1	This may have a minor impact on third neighbouring countries with which the EU has close trade, transport or free movement i.e. Schengen links. Staff in these third countries may be subject to training procedures that they might not necessarily undergo in their country or it might be repeated
4E	Awareness promotion among passengers	G	-1	This may have a minor impact on third neighbouring countries with which the EU has close trade, transport or free movement i.e. Schengen links. International / cross-border services may require a contractual level of passenger awareness / promotion in the third country. Adding a cost.

Impacts on types of workers or does it affect particular groups or people such as the disabled or of different ages

Policy measure		Mandatory /guidelines	Qualitative score	Rationale for score
1A	Reporting and monitoring national security data	M	0	This impact has no specific consequences for particular types of workers or groups of people that are disabled or of different ages.
1B	Researching and disseminating worldwide security data	G	1	This impact could have an effect on workers or groups or people that are disabled or of different ages. By collecting data that affects passengers that have reduced mobility, you could potentially improve the security measures to offer a better service.
2A	Emergency egress and access to stations	G	3	This impact will have an effect on workers or groups or people that are disabled or of different ages. By considering the access to stations, station managers / infrastructure managers will need to take into account the arrangements for passengers of reduced mobility and the emergency egress procedures.
2B	Blast-resistant features on stations	G	0	This impact has no specific consequences for particular types of workers, groups or people, i.e. disabled or of different ages.
2C	Blast-resistant features on trains	G	1	This impact could have an effect on all workers and passengers regardless of their mobility.
3E	SMS threat level protocols	G	2	This impact will have an effect on all workers and passengers of reduced mobility. The SMS may need to take account of special arrangements for these workers / passengers.
3A	SMS ensure exchange of information by relevant parties	M	0	This impact has no specific consequences for particular types of workers, groups or people, i.e. disabled or of different ages.
3C	SMS contingency planning and incident recovery	M	2	This impact will have an effect on all workers and passengers of reduced mobility. The SMS may need to take account of special arrangements for these workers / passengers.
3F	SMS liaison, incident response, drills and exercises	G	2	This impact will have an effect on all workers and passengers of reduced mobility. The SMS may need to take account of special arrangements for these workers / passengers.
3B	S/SMS recording of vulnerabilities and inspection regimes	M	0	This impact has no specific consequences for particular types of workers, groups or people, i.e. disabled or of different ages.
3D	S/SMS contingency IT, communications and spares	G	0	This impact has no specific consequences for particular types of workers, groups or people, i.e. disabled or of different ages.
4A	CCTV on stations, with recording and facial recognition	M	0	This impact has no specific consequences for particular types of workers, groups or people, i.e. disabled or of different ages.
4B	CCTV on trains, with recording and facial recognition	M	0	This impact has no specific consequences for particular types of workers, groups or people, i.e. disabled or of different ages.

Policy measure		Mandatory /guidelines	Qualitative score	Rationale for score
4C	Deploying staff where they can observe	G	-1	This impact has consequences for particular types of workers. The staff deployed to observe potential security threats could be exposed to a higher level of risk.
4F	Staff vetting and access controls	G	0	This impact has no specific consequences for particular types of workers, groups or people, i.e. disabled or of different ages.
4D	Training station/train staff in risk and behaviour monitoring	G	-1	This impact has consequences for particular types of workers. The staff deployed to observe potential security threats could be exposed to a higher level of risk.
4E	Awareness promotion among passengers	G	0	This impact has no specific consequences for particular types of workers, groups or people, i.e. disabled or of different ages.

Impacts on workers' health, safety and dignity

Policy measure		Mandatory /guidelines	Qualitative score	Rationale for score
1A	Reporting and monitoring national security data	M	0	This impact will not affect workers' health, safety and dignity. There is no evidence of links between the measure and the policy.
1B	Researching and disseminating worldwide security data	G	0	This impact will not affect workers' health, safety and dignity. There is no evidence of links between the measure and the policy.
2A	Emergency egress and access to stations	G	2	This impact will have a positive effect on workers' health, safety and dignity. By factoring in emergency protocols this will support the health and safety of the worker in the event of a security incident.
2B	Blast-resistant features on stations	G	2	This impact will have a positive effect on workers' health, safety and dignity. By factoring in emergency protocols this will support the health and safety of the worker in the event of a security incident.
2C	Blast-resistant features on trains	G	2	This impact will have a positive effect on workers' health, safety and dignity. By factoring in emergency protocols this will support the health and safety of the worker in the event of a security incident.
3E	SMS threat level protocols	G	2	This impact will have a positive effect on workers' health, safety and dignity. By factoring in emergency protocols this will support the health and safety of the worker in the event of a security incident.
3A	SMS ensure exchange of information by relevant parties	M	1	This impact will have a potential positive effect on workers' health, safety and dignity. By factoring in emergency protocols this will support the health and safety of the worker in the event of a security incident.
3C	SMS contingency planning and incident recovery	M	1	This impact will have a potential positive effect on workers' health, safety and dignity. By factoring in emergency protocols this will support the health and safety of the worker in the event of a security incident.
3F	SMS liaison, incident response, drills and exercises	G	1	This impact will have a potential positive effect on workers' health, safety and dignity. By factoring in emergency protocols this will support the health and safety of the worker in the event of a security incident.
3B	SMS recording of vulnerabilities and inspection regimes	M	1	This impact will have a potential positive effect on workers' health, safety and dignity. By factoring in emergency protocols this will support the health and safety of the worker in the event of a security incident.
3D	S/SMS contingency IT, communications and spares	G	1	This impact will have a potential positive effect on workers' health, safety and dignity. By factoring in emergency protocols this will support the health and safety of the worker in the event of a security incident.

Policy measure		Mandatory /guidelines	Qualitative score	Rationale for score
4A	CCTV on stations, with recording and facial recognition	M	0	This impact will not affect workers' health, safety and dignity. There is no evidence of links between the measure and the policy.
4B	CCTV on trains, with recording and facial recognition	M	2	This impact will have a positive effect on workers' health, safety and dignity. By factoring in emergency protocols this will support the health and safety of the worker in the event of a security incident.
4C	Deploying staff where they can observe	G	-2	This impact will have a negative effect on workers' health, safety and dignity. The staff deployed to observe potential security threats could be exposed to a higher level of risk.
4F	Staff vetting and access controls	G	-2	This impact will have a negative effect on workers' health, safety and dignity. By carrying out vetting, you are gaining access to their personal information. Any information gained could be misused if not stored confidentially and correctly.
4D	Training station/train staff in risk and behaviour monitoring	G	2	This impact will have a positive effect on workers' health, safety and dignity. By training staff to recognise risk, you are enhancing their safety.
4E	Awareness promotion among passengers	G	0	This impact will not affect workers' health, safety and dignity. There is no evidence of links between the measure and the policy.

Impacts on the safety or privacy of the passenger or staff due to unintended negative consequences of introducing such options

Policy measure		Mandatory /guidelines	Qualitative score	Rationale for score
1A	Reporting and monitoring national security data	M	-1	The privacy of passengers and / or staff could be compromised as a result of collecting personal data.
1B	Researching and disseminating worldwide security data	G	-1	The privacy of passengers and / or staff could be compromised as a result of collecting personal data.
2A	Emergency egress and access to stations	G	0	The safety or privacy of the passenger and / or staff would not be affected by an unintended negative consequence of introducing this policy measure.
2B	Blast-resistant features on stations	G	0	The safety or privacy of the passenger and / or staff would not be affected by an unintended negative consequence of introducing this policy measure.
2C	Blast-resistant features on trains	G	0	The safety or privacy of the passenger and / or staff would not be affected by an unintended negative consequence of introducing this policy measure.
3E	S/SMS threat level protocols	G	0	The safety or privacy of the passenger and / or staff would not be affected by an unintended negative consequence of introducing this policy measure.
3A	S/SMS ensure exchange of information by relevant parties	M	-1	The privacy of passengers and / or staff could be compromised as a result of collecting personal data
3C	S/SMS contingency planning and incident recovery	M	0	The safety or privacy of the passenger and / or staff would not be affected by an unintended negative consequence of introducing this policy measure.
3F	S/SMS liaison, incident response, drills and exercises	G	0	The safety or privacy of the passenger and / or staff would not be affected by an unintended negative consequence of introducing this policy measure.
3B	S/SMS recording of vulnerabilities and inspection regimes	M	0	The safety or privacy of the passenger and / or staff would not be affected by an unintended negative consequence of introducing this policy measure.
3D	S/SMS contingency IT, communications and spares	G	0	The safety or privacy of the passenger and / or staff would not be affected by an unintended negative consequence of introducing this policy measure.
4A	CCTV on stations, with recording and facial recognition	M	-1	The privacy of passengers and / or staff could be compromised as a result of collecting personal data
4B	CCTV on trains, with recording and facial recognition	M	-1	The privacy of passengers and / or staff could be compromised as a result of collecting personal data
4C	Deploying staff where they can observe	G	0	The safety or privacy of the passenger and / or staff would not be affected by an unintended negative consequence of introducing this policy measure.
4F	Staff vetting and access controls	G	-1	The privacy of staff could be compromised as a result of collecting personal data
4D	Training station/train staff in risk and behaviour monitoring	G	0	The safety or privacy of the passenger and / or staff would not be affected by an unintended negative consequence of introducing this policy measure.
4E	Awareness promotion among passengers	G	0	The safety or privacy of the passenger and / or staff would not be affected by an unintended negative consequence of introducing this policy measure.

CONTROL INFORMATION

Prepared by	Prepared for
Steer Davies Gleave 28-32 Upper Ground London SE1 9PD +44 20 7910 5000 www.steerdaviesgleave.com	European Commission Directorate-General for Mobility and Transport, MOVE A4 Rue de Mot 28 B-1040 Brussels Belgium

SDG project/proposal number	Client contract/project number
22894101	MOVE/A4/SER/2015/637

Author/originator	Reviewer/approver
Jake Cartmell, Dick Dunmore, Simon Ellis	Simon Ellis

Other contributors	Distribution	
Noe Ardanaz Ugalde, Vernon Basely, Angela De Carlo, Helen Jarvis, Daniela Phillips, Mark Scott	*Client:* DG MOVE	*SDG*: Confidential 22894101 files only

Version control/issue number	Date
Final Report to client	9 December 2016