ASSESS

Assessment of the contribution of the TEN and other transport policy measures to the mid-term implementation of the White Paper on the European Transport Policy for 2010

FINAL REPORT
ANNEX XVIII TRANSPORT SECURITY

European Commission
DG TREN
DM 28
1043 Brussels
Belgium

28 October 2005

Preface

This is ANNEX XVIII of the final report for *'Assessment of the contribution of the TEN and other transport policy measures to the mid-term implementation of the White Paper on the European Transport Policy for 2010'*.

Project title: ASSESS

Client: European Commission, Directorate-General for Transport and Energy, Unit B1.

Contract: TREN/04/ADM/S07.38796

Project contractor: Transport & Mobility Leuven

Authors:

      J.F.F. Becker M.Sc., TNO, Netherlands
      Dr. L. Smit, TNO, Netherlands

Version:
Final Version.

Date:
28 October 2005.

Reference:
Becker J., Smit L. (2005), Transport security, Annex XVIII of ASSESS Final Report, DG TREN, European Commission.

Scope

Scope of the ASSESS project

The long name for the ASSESS project is **"Assessment of the contribution of the TEN and other transport policy measures to the mid-term implementation of the White Paper on the European Transport Policy for 2010"**.

The ASSESS study is about the **"Assessment of the contribution of the TEN and other transport policy measures to the mid-term implementation of the White Paper on the European Transport Policy for 2010"**.

The European Commission's White Paper of 12.9.2001 "European transport policy for 2010: time to decide" aims to promote a sustainable transport policy. The White Paper proposes to achieve sustainability by gradually breaking the link between transport growth and economic growth, principally in three ways: changing the modal split in the long term, clearing infrastructure bottlenecks and placing safety and quality at the heart of the transport policy.

As foreseen, the White Paper on Transport undergoes in 2005 an overall **assessment concerning the implementation of the measures it advocates and to check whether its targets** - for example, on modal split or road safety - **and objectives are being attained or whether adjustments are needed.**

ASSESS provides technical support to the Commission services for the above mid-term assessment of the White Paper.

The analysis accounts for the economic, social and environmental consequences of the proposed measures and their contribution to sustainable development objectives. It provides also a detailed analysis of those effects of enlargement likely to affect the structure and performance of the EU transport system.

The study takes a three pillar approach based on the use of analysis, indicators and models. National transport policies are reviewed for compatibility and coherence with the White Paper objectives. The models used allow a detailed analysis of the freight market, the passenger market and their infrastructure networks under a number of scenarios.

Scope of this Annex

In line with the White Paper on a European transport policy, this annex reviews security to the overall policy framework of both traffic and transport. Because of the fact that terrorism has become a supranational policy issue after 9/11/2001, the White Paper on European transport policy could hardly set the security policy actions in this field. However, the European Union has always put a secure society for its residents as one important fundament of the Union. Through a qualitative policy analysis approach, this annex links the policy response for securing Europe against terrorism to the transport policy measures of the White Paper.

Index

Tables

ANNEX XVIII Transport security

Assessment of the possibility of adding security aspects to the White Paper.

Authors:
J.F.F. Becker M.Sc., TNO
Dr. L. Smit, TNO

Preface

The world has changed after September 11th 2001. Before the terrorist attacks in NY, security focused primarily on prevention and mitigation of criminality in traffic and transport. Although terrorism was commonly present (e.g. ETA, IRA, RAF), attacks mainly had the goal to come to the news and highlight the interests of the terrorist group. Their intentions were aimed at being taken seriously in political debate. Since the 9/11 attacks, our society has been confronted with a new kind of risk: the will of terrorists to spark off as much casualties as possible.

The White Paper on European transport policy was published September 12th 2001. It did of course refer to safety as an important policy issue for traffic. Safety measures are aimed at the prevention and mitigation of unintentional acts and minimisation of the consequences. However, the White Paper did not address security. Security measures relate to the prevention and mitigation of intentional acts to disturb social harmony and/or create casualties for mass dismay. The March 11th 2004 and July 2005 attacks proved that Europe is also subject to terrorist attack.

Community policy on transport in Europe needs to include a security strategy. It should *1)* protect travellers, *2)* prevent terrorists taking over a transport unit or gaining access to a loading unit, *3)* prevent smuggling in passenger and freight transport, and *4)* reduce crime.

The European Commission's Directorate-General for Energy and Transport develops and implements policy to ensure security of facilities and infrastructure in both transport and energy to protect citizens, public services and industry.

This report provides a review of European, US and other international security initiatives in the field of transport. Based on the social and strategic need for security, taking actual initiatives into account, this report motivates a Community security strategy for transport.

Abstract

The European Union (EU) has always put a secure society for its residents as one important fundament of the Union. A common counteraction to terrorism is not only necessary because of the actual geographical relations, but unquestionably because of the corresponding democratic ideologies, the intense internal trade relationships and the joint interest for a competitive position worldwide.

The European Commission's Directorate-General for Energy and Transport develops and implements policy to ensure the security of energy and transport services across the European Union. The aim of this policy is to conceive and implement measures to improve security, mainly to protect citizens against terrorism[1].

Security has become as much an element in quality of service as safety or management methods. Security in transport is thus an essential addition to the White Paper. As security policy always centres on *1)* political prevention (by foreign affairs), *2)* intelligence to track terrorism and *3)* protection, Community policy needs to be coordinated along the Directorate-Generates involved. To this purpose, an overall European transport policy should consider all objectives and all interests in an integrative manner. Consequently, it can give the other White Paper's objectives the opportunity to realise their goal.
Common rules and standards for security in energy and transport ensure the same high levels of protection for citizens throughout the Union – and ensure fair competition between operators. An adequate security policy always covers passenger and freight transport from any door to any door. Coordination across the Union enables early identification of threats and gaps in security provision. A common transport security policy should assess these vulnerabilities in any perspective and prioritise the security requirements. Policy can be taken to align and integrate the existing parallel initiatives, and fill the missing policy gaps.

Directorate-General for Energy and Transport undertakes security policy activities on the following areas:
- Aviation
- Maritime transport
- Critical transport infrastructure
- Land passenger transport
- The supply chain
- Transport of dangerous goods
- Energy facilities and infrastructure

This assessment acknowledges and suggests the following relevant policy aspects of Community policy (as valuable for an update of the White Paper) on security in transport:

-	Promoting **international cooperation and coordination,**	see section 3.4,
-	Setting a **security awareness culture** in Europe,	see section 3.5,
-	Deliberating on the **citizen's liberties and (privacy) rights** in respect to security requirements,	see section 3.6,
-	Assuring a **secure traffic,**	see section 3.7,
-	Acknowledging the **governmental responsibility** and recognising the company's responsibility,	see section 3.8,
-	Assuring **secure freight transport**,	see section 3.9,
-	Assuring a **fair distribution of costs and benefits** of security measures in transport,	see section 3.10,
-	Setting a **strategy for research and development programmes** on security in transport,	see section 3.11.

---

[1] http://europa.eu.int/comm/dgs/energy_transport/security/index_en.htm (Accessed September 2005)

XVIII.1. Introduction

XVIII.1.1. Policy need for a secure passenger and freight transport

Security in traffic and transport has become a critical worldwide issue. There are four motives for security in traffic and transport.

First, traffic networks process many movements of persons. Especially during rush hours, commuters and other passengers make metropolitan public transport systems highly crowded areas. The intense crowd and low level of physical (luggage) control make public transport systems susceptible for terrorist attacks. This was demonstrated by the attacks on the railway and subway transport in Madrid and London respectively. Security should thus protect travellers.

Second, terrorists can use transport units and loading units as means for attack. Airplanes, trains and underground trains, and (fully bombed) trucks are actual examples of terrorist weapons. Security should thus prevent terrorists taking over a transport unit. In addition, security should prevent terrorist taking access to loading units, especially hazardous materials (like on railway platforms).

Third, passenger and freight transport can be used for smuggling purposes. In general, smuggling is primarily used to illegally transport people, weapons, drugs, antique, restricted list goods and heavy tax goods. Terrorists may exploit smuggling not only for the movement of goods that have terrorist purposes, but also for making money. Security should thus prevent smuggling in both passenger and freight transport.

Fourth, freight transport is used to transport valuable goods. Theft, fraud and vandalism are both undesired acts in terms of social inequality and a significant business cost factor. Security should therefore also reduce crime in transport.

XVIII.1.2. White Paper on security

European Commission (the Commission hereafter) published the White Paper on European transport policy 'Time to Decide' on September 12th 2001. It did of course refer to safety as an important policy issue for traffic. Safety measures are aimed at the prevention and mitigation of unintentional acts and minimisation of the consequences.

In the White Paper 'security' is mentioned eleven times. However, the White Paper only relates security to either the 'security of energy supply' or in the context of common security checks in the 'rethinking of airport capacity use'. Security referring to 'attack' is only mentioned in the context of attacks on European passenger cruises.

> **The White Paper on security: Attacks on European passenger cruises**
> "Propose a regulatory framework for safety controls for passengers embarking on ships offering European cruises in order to combat the risk of attacks, along the lines of what is done in air transport." (p.107)

> **The White Paper on security: Security of energy supply**
> "The strategic objectives deal in particular with the reduction of greenhouse gases and pollutant emissions, the security of energy supply and the balanced use of the various transport modes, all of these being priority research themes with a contribution to make to the implementation of the transport policy recommended in the White Paper." (p.120)
>
> "As stated in the Commission's November 2000 Green Paper on security of supply, in 1998 energy consumption in the transport sector was to blame for 28% of emissions of CO2, the leading greenhouse gas." (p.10)
>
> "As the main objective of these international rules is to facilitate trade and commerce, they do not take sufficient account of environmental protection or security of supply concerns. Consequently, for some years now, certain countries such as the USA have been implementing regional transport accords, particularly in the maritime or aviation sector, to protect specific interests. The European Union has followed closely in their footsteps in order to guard against catastrophic accidents at sea or to abolish inappropriate rules on aircraft noise or on compensation for passengers in the event of accidents." (p.18 and 91)

> **The White Paper on security: Rethinking airport capacity and use**
> "Nevertheless, intensive use of such large carriers will pose a number of problems. First, airports must be adapted to cope with such aircraft – embarkation and disembarkation of 500 to 600 passengers instead of 150 to 200 poses a greater strain on organisation of baggage delivery, security checks, customs formalities and passenger reception at airports. And, of course, use of such large carriers will do nothing to reduce connecting traffic, since passengers taking these new aircraft will have to continue their journey, thus creating an even more acute need for efficient intermodality." (p.38)

However, the White Paper did not yet address security in relation to terrorism. The September 11th 2001 attacks produced a new political awareness. In response, security has become an highly important political issue all over the world.

Security measures relate to the prevention and mitigation of intentional acts to disturb social harmony and/or create casualties for mass dismay. The March 11th 2003 attacks in Madrid and the July 7th and 21th 2005 attacks in London proved that Europe is also subject to terrorist attack.

XVIII.1.3. Policy need for assessment and updating the White Paper on security

XVIII.1.3.1. Strengthening the European Union as an area of freedom, security and justice

One of the fundamental objectives of the European Union, as stated by the constitutional treaty which was signed in 2004 and is now undergoing a ratification process in the member states, is to offer its citizens an area of freedom, security and justice without internal borders.

The Treaty of Amsterdam on the European Union (EU) which came into force on 1 May 1999 states that the EU:
- must be maintained and developed as an area of freedom, security and justice;
- (an area) in which the free movement of persons is assured;
- in conjunction with appropriate measures with respect to external border controls, asylum, immigration and the prevention and combating of crime.

To this effect, the European Council adopted in October 1999 in Tampere a first work programme, which implementation was achieved in 2004.

On 4 November 2004, the European Council adopted the Hague programme which set the objectives to be implemented in the area of freedom, security and justice in the period 2005-2010 (COM(2005) 184). The programme's main focus is on setting up a common immigration and asylum policy for the 25 EU member states. This new programme takes into account the final evaluation made by the Commission on the Tampere programme, as well as the comments received during the citizens on-line consultation held in July/August 2004.

The Commission presented in May 2005 an action plan with a set of detailed measures and a calendar to implement the programme adopted in the Hague. On the 2nd of June 2005, the Council approved the Action Plan, which will be the frame of reference for Commission and Council work over the next five years[2].

Concerning future developments, the Constitutional Treaty signed in October 2004 by the Head of States and of Governments reinforces the objective to offer citizens an area of freedom, security and justice. It facilitates decision-making, increases the powers of the European Parliament and extends the competencies of the European Court of Justice with regard to certain domains.

During the second semester of 2006, the European Council will examine the progress made in the implementation of the Hague Programme.

XVIII.1.3.2. Community responsibility on securing transport

In accordance with articles 11 and 12 of the Treaty of Nice, the Community has the responsibility to maintain and develop the security of transport systems.

The Treaty of Nice, based upon the earlier Treaties, establishing the European Community as in force from 1 February 2003, states the Union shall set itself the following objectives (article 2):

- to assert its identity on the international scene, in particular through the implementation of a common foreign and security policy including the progressive framing of a common defence policy, which might lead to a common defence, in accordance with the provisions of Article 17,
- to maintain and develop the Union as an area of freedom, security and justice, in which the free movement of persons is assured in conjunction with appropriate measures with respect to external border controls, asylum, immigration and the prevention and combating of crime.

In addition, article 11.1 states that The Union shall define and implement a common foreign and security policy covering all areas of foreign and security policy, the objectives of which shall be:

- to safeguard the common values, fundamental interests, independence and integrity of the Union in conformity with the principles of the United Nations Charter,
- to strengthen the security of the Union in all ways.

Further, article 12 states that the Union shall pursue the objectives set out in Article 11 by:

- defining the principles of and general guidelines for the common foreign and security policy,
- deciding on common strategies,
- adopting joint actions,
- adopting common positions,
- strengthening systematic co-operation between Member States in the conduct of policy.

---

[2] http://europa.eu.int/comm/justice_home/fsj/intro/fsj_intro_en.htm

Although the Treaty in Title V 'Transport' does not relate transport directly to security, it is obvious that the contemporary transport policy needs to counteract intentional unauthorised and undesired acts designed to cause harm or damage to, or by, the supply chain.

In this context, Com (2004) 72 states for example that security is an evolving concept and presents many challenges to the EU-25 that impact on a wide range of existing and emerging EU policies, citizens' concerns, including the protection against terrorist threats, and the adaptation of governance structures to effectively deal with these matters. Policies include Competitiveness (COM(2003) 704), Transport, Environment, Energy, Health, Consumer Protection, Finances, Trade, Space and Telecommunications; as well as the Common Foreign and Security Policy (CFSP), the European Security and Defence Policy (ESDP), and policies in respect of Justice and Home Affairs.

In line with this, objective 4.2.1 of the updated EU Plan of Action on Combating Terrorism (November 2004) aims at "strengthening of the security of all forms of transport systems, including through the enhancement of the legal framework and the improvement of prevention mechanisms".

XVIII.1.4. Scope: security of passengers and goods transport

In line with the White Paper on a European transport policy, this assessment links security to the overall policy framework of both traffic and transport. Security in traffic can be defined as protection of passenger and freight transportation against intentional unauthorised and undesired acts designed to cause harm or damage to society in general and cause casualties in particular. Security in transport can be defined as the resistance to intentional, unauthorised and undesired act(s) designed to cause harm or damage to, or by, transportation activities, services and infrastructure in the supply chain.

XVIII.1.5. Research method

The security assessment has been based on expert opinion, the Community documents available at the websites of the Community[3], Cordis[4], Eurolex[5] and other internet searches. It should be noted that the analysis and conclusions are those of the authors and not the Community in any kind of way.

The security assessment follows the structure of the four scenario structure that is used by the other work packages of the 'Assessment of the contribution of the TEN and other transport policy measures to the mid-term implementation of the White Paper on the European Transport policy for 2010'.
However, the White Paper did not set any important transport security actions. Since a lot has changed after 9/11, the base scenario and the full implementation scenario are not relevant for transport security. Therefore, the following chapters will discuss consecutively:
- Most likely scenario,
- Recommended scenario.

The current status of actions and policies developed since 2001 is discussed in the 'most likely scenario' of chapter 2. The 'recommended scenario' suggests other relevant policy issues that also may be taken into consideration for Community policy (and an update of the White Paper) on transport security.

---

[3] http://europa.eu.int
[4] http://www.cordis.lu/en/home.html
[5] http://europa.eu.int/eur-lex/lex/en/index.htm

XVIII.2. Most likely scenario on transport security

XVIII.2.1. Generic developments on security in the European Union

Plan of Action against terrorism

The citizens of Europe rightly expect the European Union, while guaranteeing respect for fundamental freedoms and rights, to take a more effective, joint approach to cross-border problems such as illegal migration, trafficking in and smuggling of human beings, terrorism and organised crime, as well as the prevention thereof (The Hague Programme). Notably in the field of security, the co-ordination and coherence between the internal and the external dimension has been growing in importance and needs to continue to be vigorously pursued. The EU's basic objective in the fight against terrorism is to ensure that its citizens have the ability to live in freedom, peace and safety (SEC 2004 332).

As communicated by the 'Plan of action of the extraordinary European Council meeting on 21 September 2001', the European Council quickly responded to the threat of terrorist attacks via air transport. The Council called upon the Transport Council to take the necessary measures to strengthen air transport security at its next meeting on 15 October. Effective and uniform application of air security measures are ensured in particular by a peer review. These measures will cover in particular:
– classification of weapons;
– technical training for crew;
– checking and monitoring of hold luggage;
– protection of cockpit access;
– quality control of security measures applied by Member States.

The European Council adopted the 'Plan of Action against terrorism' on 28 September 2001. The Plan of Action contains a wide range of measures to be adopted in various crucial sectors in the fight against terrorism (judicial and police cooperation, transport safety, border controls and document security, blocking financing, political dialogue and external relations, defence against biological-chemical-radiological-nuclear etc. attack).

The most recent version to the 'EU Plan of Action on Combating Terrorism- Update' (PoAaT-U) was made on 29th November 2004 by the Dutch Presidency in Council. It consists of three parts: this Cover note, an updated matrix, containing all the actions of the Action Plan and an annex showing an overview of the implementation by Member States of EU-legislation in the fight against terrorism as well as ratification of the relevant UN-Conventions.

The European Council Declaration of 25 March 2004 set out the following seven strategic objectives for the EU's Action Plan against terrorism (PoAaT-U, 2004):

1. To deepen the international consensus and enhance international efforts to combat terrorism;
2. To reduce the access of terrorists to financial and economic resources;
3. To maximise the capacity within EU bodies and Member States to detect, investigate and prosecute terrorists and to prevent terrorist attacks;
4. To protect the security of international transport and ensure effective systems of border control;
5. To enhance the capability of the European Union and of member States to deal with the consequences of a terrorist attack;
6. To address the factors which contribute to support for, and recruitment into, terrorism;
7. To target actions under EU external relations towards priority Third Countries where counter-terrorist capacity or commitment to combating terrorism needs to be enhanced.

It was reviewed and approved by the European Council of June 2004, and integrated with subsequent measures (European Council of 16-17 December 2004). The European Council of 16-17 December 2004 approved a series of further measures in the area of the fight against terrorism, which include reinforced intelligence capability in the Council Secretariat General, outline of a global protection strategy for critical infrastructures, terrorism financing block, integration of counter-terrorism activities in the European Union's external relations with regard both to the development of political dialogue and to technical assistance to third countries. Particular importance was given to the radicalisation of the terrorist phenomenon and the recruitment of terrorists on the basis of the common principles as regards integration adopted at the Groningen Conference, including inter-religious dialogue. The conference was aimed at strengthening political support to ethnic minorities, which is important for the unity of European societies, and at exchanging experience, particularly when it comes to the integration of young immigrants.

Also on 25 March 2004, the "Declaration on solidarity against terrorism" was adopted, which, anticipating the provisions of Article 42 of the Treaty on the European Constitution, establishes the obligation to assist, "with all the instruments available, including military resources", any Member State struck by a terrorist attack.

In its meeting of 25 March 2004, the European Council ratified the appointment of a Counter-Terrorism Coordinator — Dutchman Gijs de Vries — whose task it is to ensure a more effective coordination of the European Union's activities in the various sectors and different pillars.

XVIII.2.2. Policy on security in energy and transport

DG TREN (2005) emphasises that Europe's citizens and economy depend on reliable transport and services. The internal market and the fundamental principle of free movement in the EU make these services vital. Strongly interconnected European networks are at the heart of both energy and transport services; incidents in one region may have knock-on effects across the Union. Therefore, the EU institutions and Member States must work together at EU level to protect people, goods and facilities.
Enhancing security in transport and energy must – according to DG TREN (2005) be at the forefront of operator's priorities. Security is as much an element in quality of service as safety or management methods.

Directorate-General for Energy and Transport undertakes security policy activities on the following seven areas.

Aviation
Common rules at al EU airports ensure the implementation of essential security measures to deter and prevent acts of unlawful interference against civil aviation. Regulations include 2320/2002, 1486/2003, 849/2004 and 1138/2004. Details can be found in appendix B.
Inspections of airports and of national authorities in charge of civil aviation by European Commission teams identify room for improvement and ensure that all Member States are applying EU Standards consistently. Regulation 1217/2003 lays down the common specifications for national civil aviation security quality control programme (see appendix B).
Mandatory rules mean the EU is a leading player in raising global security standards in aviation.
DG TREN (2005) states that the Commission is able to react quickly to address new threats, in consultation with Member States' experts.

Maritime transport
EU legislation enforces International Maritime Organisation (IMO) security standards for all ships flying the flag of a Member State, and all other vessels sailing in European waters. EU regulations 725/2005 and 724/2004 lay down this enforcement of the International Ship and Port Facility Security Code (ISPS). Details can be found in Appendix C. Member States are required to carry out checks on vessels, and their cargoes, in ports throughout the Union. A security officer in each ship's crew ensures sufficient awareness of security issues at all times. Inspections of port facilities, ships, companies, recognised security organisations and national authorities in charge of maritime security by Commission inspectors will complement Member States' own inspections and ensure correct application of EU rules throughout the EU.

Critical transport infrastructure
The European Commission adopted a Communication on the protection of the vital infrastructures against terrorism (COM(2004) 702). This Communication announces that a European programme for the protection of the critical infrastructures (programme EPCIP) will be proposed. In this context, DG TREN launched the invitation to tender (TREN/J1/11-2005) concerning the protection of transport critical infrastructures at European level. At the moment of writing the tender deadline (15/06/2005) has been passed and DG TREN is deliberating on the project assignment on behalf of the Commission.
The Commission will draw up an inventory of critical infrastructure in the EU which is of highest priority for protective action, such as bridges, tunnels and terminals, to which damage or disruption from unlawful acts would harm transport services at EU level (DG TREN, 2005). It could then propose protective measures for action by Member States.
With the rapid development of an increasingly networked world, protection of information infrastructures is crucial to the correct functioning of modern society (SEC 2004 332). The impact of possible terrorist attacks on these infrastructures will have devastating affects for all economic sectors e.g. energy, communications, transportation and water supplies. The EU is also developing a multifaceted approach, enhancing the legal framework (electronic communications legal instruments such as the 'telecom package'.); developing policies on cyber-crime (Framework Decision on attacks against information systems) and improving prevention mechanisms.

Land passenger transport
Whilst most public transport services are local or regional, rather than European, operators will be encouraged to share security concerns and knowledge with counterparts across the EU in user forums to increase protection for all citizens.
Exchanging good practice in this way will lead to the development of common security standards and requirements for all public transport services in the EU.
Action at EU level will be a catalyst for improved security across the EU ensuring that both authorities and operators are better aware of security risks and appropriate responses.

The supply chain
Intermodal transport security aims to protect all sectors of the supply chain from interruption caused by unlawful and undesired acts.

EU action aims to bring together public and private actors to ensure coordinated measures and a systematic approach to security throughout the supply chain.

The complexity of the supply chain means that those parties dispatching goods, operators of road, rail and inland waterway transport, freight forwarders, and terminal operators must all work together to raise security standards to satisfactory levels (DG TREN, 2005).

Transport of dangerous goods
International carriage of dangerous goods is addressed by UN standards, under the road (ADR), rail, and inland waterways (ADNR) conventions. These apply to all transport activities of dangerous goods within the EU. Details can be found in Appendix C.7.

While safety was their main purpose, these rules are also vital for security. Recent extensions focus on security. In particular, stricter rules are included on 'high-consequence dangerous goods', which have the potential for misuse by terrorists.

Specific rules have also been adopted covering the use of transportable pressure equipment, to provide effective containers for particular dangerous goods.

Energy facilities and infrastructure
The electricity and gas markets are increasingly being opened to competition in the same way as communication services are. Energy is considered to be a special product, of which the security of supply remains a political priority (SEC 2004 332). This importance was already discussed in the White Paper on European transport policy in 2001. Nuclear installations and other key industries are other examples of infrastructures requiring a high level of security.

DG TREN (2005) states that it is essential to prevent disruptions to energy suppliers across the Union, since unlawful acts which provoke power interruptions have a major impact on the lives of citizens, disrupt essential social and government services and harm industry. In the single market in energy, major supply disruption in one Member State also affects others.

In the Communication from the Commission on the development of energy policy for the enlarged EU, its neighbours and partner countries (COM(2003) 262), the Commission brought up the need of protecting the energy infrastructures from external attacks.

Today, the Commission is working with Member States to draw up a common strategy for the protection of critical energy infrastructure (like pipelines, transmission networks) and installations (power stations, refineries, storage facilities, etc) in the EU (DG TREN, 2005).

This security strategy will enable the Union to develop means to bypass or isolate situations where supply is disrupted and so avoid them cascading across EU networks.

The private and public operators of energy facilities and infrastructure together with public authorities in all Member States are working with the Commission, creating security platforms for the coordination of action across the whole energy sector

Since much of the EU's energy consumption comes from outside EU borders, cooperation with foreign governments and operators is essential to ensure supplies are not disrupted. In particular collaboration will be reinforced with neighbouring supplier and transit countries.

XVIII.2.3. Other developments

Financing terrorism

The European Union has made terrorism one of the cardinal elements of its political dialogue with regional groups and third countries. An anti-terrorism clause is foreseen in participation and cooperation agreements and in other similar instruments.

One of the EU's most innovative instruments are the community level lists aimed at freezing the assets of individuals and terrorist groups other than Al Qaeda (Position 931/2001 and Regulation 2580/2002). Through Regulations 881/2002 and 187/2005, the European Union automatically acknowledges the revisions of the UN Sanctions Committee's lists and enforces them in the regulations of Member States.

The Italian EU Presidency of the second semester of 2003 achieved results of political and operational significance under both the second and third institutional pillars. Within the context of the CFSP (Common Foreign and Security Policy) a dialogue has been set in motion with the Gulf Cooperation Council countries on the subject of financing terrorism (a specific meeting was held in Brussels on 7 November 2003, and was followed by a second meeting in Abu Dhabi on 5 and 6 March 2005).

External borders

"Ad hoc multinational teams" were set up in the third pillar, made up of investigators from EU countries operating in the "pre-judiciary" segment of police investigations; a related "operating manual" was also approved. The first time the multinational teams were employed was on the occasion of the Athens Olympic Games in 2004. The European Union has also defined a series of regulations concerning border control, exchange of information and judicial and police cooperation.

In this respect, the Hague Programme to reinforce the European space of freedom, security and justice, aims at developing an integrated management system for external borders, with responsibility and financial expenses divided equally between Member States. The European Agency for External Borders, which will coordinate operational collaboration to stem illegal immigration and its connections to organised crime and trafficking of human beings, is operational as of 1 May 2005 (see COM(2003) 687). Its headquarters is in Warsaw. In this framework attention will also have to be paid to the risk of these illegal flows becoming a vehicle for terrorist infiltration from Sub-Saharan African countries sympathetic to Muslim fundamentalism.

Identity checks

In order to strengthen the fight against illegal immigration, the Hague Programme foresees the implementation of security measures through the use of innovative techniques, such as biometrics, in identity checks at the borders and in European Union territory, and by achieving inter-operability between the Schengen Information System[6] (SIS II), the Visa Information System (VIS) and EURODAC, by the end of 2005. It is in this context that the adoption of Council Regulation no. 2252 (2004), regarding regulations on security aspects and the biometric elements of passports and travel documents issued by member states, has been adopted, as well as a proposal for a conclusion of the Council on biometric information in visas and in temporary residence permits of citizens from third countries. This proposal is aimed at accelerating the setting up of the VIS, and is currently being examined by the appropriate Council working groups. As far as common policy in terms of visas is concerned, the Hague Programme foresees the future creation of joint services for the issuing of visas between Schengen area countries, and in this connection the Council

---

[6] See also Com(2003) 771 and Regulation 871/2004.

has asked the Commission to present a proposal, before the end of 2005, for the establishment of joint centres for the introduction of visa requests.

Many legislative instruments have been adopted in the framework of judicial, penal and police cooperation. Some of these are already being applied in practice in response to delays associated with the ratification or acknowledgement procedures in the organisational arrangements of Member States. Some Framework Decisions could be mentioned at this point: on the European arrest warrant; on joint investigation teams; on the fight against terrorism; on the creation of Eurojust; on the recycling and confiscation of the instruments and proceeds of crime; on the specific measures for judicial and police cooperation in the fight against terrorism; on the proposal being examined by the Council for reciprocal acknowledgement of decisions to confiscate. In this context, the Convention on mutual criminal assistance between member states[7] should also be mentioned.

Advance passenger data for EU entering persons
Council Directive 2004/82/EC lays down the obligation of carriers to communicate passenger data. The Directive aims at improving border controls and combating illegal immigration by the transmission of advance passenger data by carriers to the competent authorities. The directive states that Member States shall take the necessary steps to establish an obligation for carriers to transmit at the request of the authorities responsible for carrying out checks on persons at external borders, by the end of check-in, information concerning the passengers they will carry to an authorised border crossing point which these persons will enter the territory of a Member State. After the passengers have entered, these authorities shall delete the data within 24 hours after transmission, unless the data are needed later for the purposes of exercising statutory functions in accordance with national law and subject to data protection provisions of Directive 96/46/EC.

XVIII.2.4. Principal areas of multilateral cooperation against terrorism

XVIII.2.4.1. United Nations

In the UN sphere, Security Council Resolution 1373 (2001) constitutes the basis for establishing numerous Member State obligations, which include: international judicial and police cooperation, the signing and ratification of the 12 UN Conventions against terrorism, the fight against the flow of capital that fuels terrorist groups, the development of technical aid programmes aimed at strengthening the operational capacities of member states in this sector, and so on.

The Security Council disposes of two subsidiary organisations with mandates to fight terrorism:
– the Counter-Terrorism Committee, CTC was set up after 11 September on the basis of Resolution 1373 with a monitoring role and the task of boosting the overall counter-terrorism activities;
– the Sanctions Committee against Al Qaeda and the Taliban, has the specific task of updating the list of individuals and entities associated with these organisations, and of monitoring the enforcement of sanctions.

---

[7] http://conventions.coe.int/treaty/en/Treaties/Html/030.htm

XVIII.2.4.2. G8

The G8 has systematically dealt with the main themes related to terrorism at the political level, above all in the course of the last three summits (Kananaskis 2002, Evian 2003, Sea Island 2004). At expert level, there are two specialised bodies, the Lyon/Rome Group and the CTAG:

The Lyon/Rome Group is the result of the merger, decided on at the 2002 Kananaskis Summit, of the Lyon Group (active in the fight against organised crime) and the Rome Group created after 9/11 with a specific mandate in the field of combating terrorism. It is a forum for information exchange, analysis and promotion of coordination and cooperation initiatives in the fight against terrorism and organised crime. It meets three times a year and develops proposals for approval at political level (Heads of Government, Foreign Affairs Ministries, Justice and Interior Ministries), as well as "best practices" and "guidelines" for the adoption of operative measures on the part of specialised multilateral bodies, like ICAO (International Civil Aviation Organisation) and the IMO (International Maritime Organisation).

The CTAG (Counter-Terrorism Action Group) coordinates technical assistance to third countries that are weaker institutionally and more exposed to the terrorist threat.

In addition, according to COM(2003) 229, G8 members agreed to develop, within the United Nations and other relevant international organisations, an effective and proportionate security regime for the overland transportation and distribution of hazardous cargoes which potentially significant security risks.

Another crucial sector is **transport safety**. At the G8 Summit on Sea Island (8-10 June 2004) the Heads of State and Government approved an Action Plan (SAFTI – Secure and Facilitated International Travel Initiative), which extends and develops measures already approved at the Kananaskis Summit of 2002. The Plan principally concerns air traffic and consists of a short Declaration and a more detailed Action Plan covering a wide series of measures intended to heighten aircraft safety standards, improve airport control procedures and facilitate exchanges of information. One section of the Plan concerns the safety of maritime transport and infrastructures.

XVIII.2.4.3. NATO

NATO approved a Declaration on terrorism at the ministerial level informal Atlantic Council on 2nd April 2004. The Declaration reaffirms the principles of cooperation and solidarity between member states and refers to the guidelines established by the UN for collaboration in opposing international terrorism. NATO's activities in Afghanistan and in training Iraqi military forces constitute a commitment in the struggle against terrorism in a broad sense.

Furthermore NATO is collaborating with the European Union in the development of cooperation for civil protection and defence in the case of CBRN (Chemical, Biological, Radiological and Nuclear) attacks. An analogous form of collaboration is taking place in the framework of the NATO-Russia and Euro-Atlantic Partnership Councils.

International cooperation in the fight against terrorism

Trends in counter-terrorism approaches vary and must be adapted to the development of terrorism strategies, above all in terms of public policies and operational methods.
In the first place the trend toward reinforcing intelligence capabilities must be underlined, both at national level and at that of international organisations.

One measure in this sense is the previously mentioned one adopted by the European Council of 16-17 December 2004. The NATO Declaration on Terrorism of 2nd April 2004 contains a series of operational measures referring to the improvement of intelligence information exchanges, and the organisation is completing the implementation of a "Terrorist Threat Intelligence Unit".

With regard to the United Nations, the need to reinforce the organisation's capacities in this field is being pointed out from several quarters.

Finally, strong emphasis is placed on regional cooperation, both in the political sense and in the sense of solidarity, also at the operational level. The United Nations encourages this type of agreement, as is demonstrated by the periodic meetings organised by the Counter-Terrorism Committee with various regional bodies (the most recent took place in March 2004 in Vienna, in collaboration with the OSCE and the United Nations Office on Drugs and Crime). On the operational level, various regional centres for training and sharing of experiences have recently been set up with the clear intent of reinforcing bonds of solidarity and achieving scale economies. Some examples are the SEARCCT (South East Asia Regional Centre on Counter Terrorism) based in Kuala Lumpur, the JCLEC (Joint Centre on Law Enforcement Cooperation) based in Jakarta, and the Anti-terrorism Centre of the African Union inaugurated in October 2004. Italy fully supports such initiatives, also within the framework of the European Union, and has arranged for collaboration with some of these centres. A forum for political dialogue and counter-terrorist collaboration of particular importance is the ASEM (Asia-Europe Meeting), in which EU countries and a significant number of Asian countries take part.

XVIII.2.4.4. ISO and CEN

Technical Committee 8 (TC8) of the International Standardisation Organisation is currently developing the ISO/PAS 28000 standard for a security quality management system. The standard is as a quality management system (comparable with ISO 14000) that identifies the security procedures (answering the question "which procedures") required by manufacturers/shippers and logistics service providers. If approved, the Public Available Specification 28000 will be available winter 2005/2006. ISO/PAS 28001 will provide one solution as specification of the procedures required (answering the questions "how and to what level of detail").

CEN, the European Committee for Standardization, is currently contributing to the objectives of the European Union and European Economic Area with voluntary technical standards which promote 'Protection and Security of the Citizen' CEN BT/WG 161[8]. Subject-matter related expert groups have now been established to look at needs for standards and identify areas where additional effort is required, and report to BT/WG 161. Their titles are as follows:

- Identification and reduction of crime risk in products and services
- CBRN incidents (Chemical, Biological, Radiological and Nuclear)
- Critical infrastructure - Energy supply
- Critical infrastructure - Building and Civil Engineering works
- Security of the supply chain

- Integrated Border Management
- Emergency services
- Defence against terrorism
- Security of water supply

XVIII.2.4.5. Other institutes

Document security and the application of new technologies is another prominent trend. In order to guarantee adequate protection against the possible forging of passports and other travel documents, also for the

---

[8] http://www.cenorm.be/cenorm/businessdomains/businessdomains/security+and+defence/security/btwg161.asp

purposes of terrorism, several States have decided to insert biometric data into such documents.. Agreements on joint approaches and standards in this area of considerable operational importance are being discussed within the ICAO (International Civil Aviation Organisation). Significant activity in terms of analysis and proposals in this field is also taking place within OSCE. The EU is also preparing to apply new technologies to travel documents so as to establish a reliable link between the citizen and the document

On the subject of international cooperation against the financing of terrorism, 9 Special Recommendations against the *financing of terrorism* have been drafted (which have been added to the already existing 40 Recommendations against money laundering) by the GAFI (Gruppo di Azione Finanziaria Internazionale, FATF – Financial Action Task Force). To date more than 90 States not belonging to the GAFI have presented self-assessment reports on their conformity with this body's recommendations.

XVIII.2.5. New security programmes on transport

XVIII.2.5.1. Background

Europe has entered a new phase in its history, marked by major political, demographic, social and economic evolutions. The challenge facing the EU-25 is to adapt and prosper within this changing environment, whilst being guided by the fundamental values and objectives of the Union[9].

Security is one particular global challenge that has recently come to the fore due to world events and societal changes. Europe needs to invest in a "security culture" that harnesses the combined and relatively untapped strengths of the "security" industry and the research community in order to effectively and innovatively address existing and future security challenges.

The need to address the new security situation, and the role of a strong industrial and technology base has been) stressed by Heads of state and governments on various occasions, such as[10]:
– The Cologne European Council, which emphasised the need for a competitive and dynamic industrial and defence base
– The Lisbon Council drive to a competitive knowledge-based society
– The Barcelona Council, calling for a boost to overall research, development and innovation effort in the Union
– The decision of the Thessalonica Council to take concrete steps in the field of defence
– The adoption by Council of the EU Security Strategy 'A secure Europe in a better world' (Solana, 2003)
– The discussion at the Brussels Council of 25/26th March 2004 which resulted in a Declaration on Combating Terrorism.
– The approval by the European Council of 16-17 December 2004 of the updated EU's Action Plan against terrorism (see section XVIII.2.1).

The need for Community Security Research[9]
Europe needs to tackle threats that are more diverse, less visible, and less predictable. This calls for behavioural changes as well as more innovative means to deal with complex situations to address security in a comprehensive manner ("comprehensive security").

---

9   http://www.cordis.lu/security/policy.htm
10   Discussed in e.g. COM(2004) 590

Europe must use its technological strengths to build the capability for deploying significant resources for peacekeeping, humanitarian aid and state-building activities, either on its own or in international alliances. It requires an optimal use of the resources and the development of European industrial capabilities.

In its Communications setting out its strategic orientations for the definition of the Financial Perspectives 2007-2013[11], the Commission has already highlighted the objective of supporting the development of the area of Freedom, Security and Justice with adequate financial resources, to be included in a new Heading relating to "Citizenship, Freedom, Security and Justice". In accordance with the objectives set out by the European Council, the proposed framework programme 'Security and Safeguarding Liberties' for this period (as discussed in COM(2005) 124) would respond to the challenges that the EU is facing.

XVIII.2.5.2. Pursued developments in passenger and freight transport

COUNTERACT
Given the current vulnerability of transport systems, emphasised by recent public transport bomb attacks in London and last year in Madrid, volatile energy prices and widespread public and political concern, such solutions and proposals need to be determined rapidly.

In response, DG TREN prepared task 3.3 of a call for proposals published in the framework of the sixth Research Framework Programme on 30 October 2004. The COUNTERACT project (Cluster Of User Networks in Transport and Energy Relating to anti-terrorist ACTivities) was evaluated the best of three proposals. This project aims to assess and recommend feasible and cost-effective solutions for the improvement of security in transport and energy.

COUNTERACT is a coordination action involving 18 partners active in the transport, energy and security domains. The consortium is led by UITP – the International Union of Public Transport. The partners include three international organisations, one Commission service (JRC) and private companies and a university from 10 different countries. The total budget of the project is 3.48 M€, fully paid by the Commission. The COUNTERACT project would commence in September 2005 and produce its first outputs before the end of 2005.

The project is intended to begin in September 2005 and is programmed to last for 34 months.
The activities will be developed in parallel in three "clusters" on:
- passenger transport,
- freight transport (including road haulage, air freight, maritime, intermodal)
- energy (gas, electricity, oil).

Stakeholders (energy companies and public transport operators, and umbrella groups acting as their representatives) will contribute to the definition and the validation of the activities of the clusters. They are organised into four thematic user groups (TUG) with either one or two TUGs per cluster. Clusters will gather information, define terms of reference of studies.
Outputs of the projects will be:
- monthly report (two pages including a financial sheet)
- meeting reports (including terms of reference for studies and/or task sheets for experts)
- specific study reports and recommendations to the Commission
- participation in international meetings
- databases.

---

[11]   COM(2004) 101

PASR projects in call 1

Subscribing to the recommendation to establish a European Security Research Programme (ESRP) to commence in 2007, the Commission will initiate an inter-institutional debate for consensus on such a programme, building on the work of the Preparatory Action on Security Research (PASR), which it will continue until the end of 2006 (COM(2004) 101). In March 2004, the Commission[12] launched this three-year Preparatory Action with a budget of €15 million for 2004 and €25 million for 2005 and 2006. The first call for proposals closed on 23 June 2004 and surpassed expectations. It attracted over 170 eligible proposals, and 12 projects have been launched by the end of 2004[13].

The PASR initiative finances projects in five priority research categories identified by the Commission as key to safeguarding the security of Europe's citizenry:
  – Improving situation awareness;
  – Optimising security and protection of networked systems;
  – Protecting against terrorism;
  – Enhancing crisis management;
  – Achieving interoperability and integrated systems for information and communication.

Each of these objectives has direct implications for Europe's transport sector, particularly the notion of interoperability since the logistics and communications interface between sub-transport sectors grow evermore intertwined: road-rail, road-port and rail-port. Situation awareness along an extensive railway line, for example, can only be implemented via the most advanced and tamper-proof surveillance and communications technologies.

PASR projects have the following characteristics:
  – Duration 1 to 2 years;
  – Mission-oriented or related to system interoperability & integration;
  – Tangible results, providing a basis for future ESRP;
  – Collaborative, multidisciplinary, multi stakeholder;
  – Minimum 2 partners from EU25, involving final users/

PASR projects in call 2

In February 2005, the Second Call[14] was made for Proposals for the Preparatory Action on "The enhancement of the European industrial potential in the field of Security Research" (PASR 2005). The following priority missions are identified in the basic documents of the PASR and remain applicable for PASR-2005:
  – Optimising security and protection of networked systems;
  – Protecting against terrorism (including bio-terrorism and incidents with biological, chemical and other substances);
  – Enhancing crisis management (including evacuation, search and rescue operations, control and remediation);
  – Achieving interoperability and integration of systems for information and communication.
  – Improving situation awareness (e.g. in crisis management, anti-terrorism activities, or border control).

A European panel of independent experts evaluated the 2nd call for proposals of the PASR action. With 156 proposals submitted the response to this call was again overwhelming. Like in 2004, with an available

___

[12]   Introduced in COM(2003) 704
[13]   http://europa.eu.int/comm/enterprise/security/articles/article_1495_en.htm
[14]   http://www.cordis.lu/security/calls.htm

budget of €15 Million, thirteen proposals - 8 technology projects and 5 supporting activities - were selected.

Type of PASR projects
The next table illustrates the relations of the PASR projects of call 1 to the objectives of the White Paper on European transport policy. In the appendix, the PASR projects of call 1 are summarised in appendix 1.

Table 1: PASR research (call 1) along the White Paper's action topics

White Paper objectives	PASR research of call 1	PASR research of call 2
1. Improving quality in the road transport sector		
2. Revitalising the railways		TRIPS
3. Balancing air transport and environment	TERASEC	PATIN MANPADS
4. Promoting transport by sea and inland water-way		SOBCAH (SECCOND)
5. Turning intermodality into reality		
6. Building the Trans-European transport network		SECCOND
7. Improving road safety	VITA	
8. Effective charging for transport		
9. Recognising the rights and obligations of users		PRISE
10. Developing high-quality urban transport	CRIMSON ISCAPS	(TRIPS)
11. Enabling clean, efficient transport		
12. Managing the effects of globalisation	ASTRO+ IMPACT SUPHICE ESSTRT GEOCREW	ROBIN MARIUS HiTS/ISAC PROBANT BSUAV USE IT

XVIII.2.5.3. 7th Framework Programme for Research & Development

Security has been included in the list of priority research themes in the proposal for the 7th Framework Programme for Research & Development (FP7) issued to the European Parliament and Council by the Commission. As well as responding to widespread demand in the face of new security challenges this move will enhance the competitiveness of the European security industry[15].

Security research forms part of the Security and Space thematic priority for collaborative research within FP7, which aims to find synergies between security and space research and is endowed with a budget allocation of half a billion Euro per year for the 2 sectors. Security Research is needed to increase levels of security for European citizens. In addition, it will help in creating a favourable social and business environment for prosperity and development. Business will gain, not only within the security industry, but also in many other economic sectors, leading to higher growth and employment in Europe.

As well as being an important building block in supporting the Common Foreign and Security Policy, security research will promote the establishment of an EU-wide area of justice, freedom and security as endorsed by the Hague programme and contribute to developing technologies and capabilities in support of other EU policies in areas such as transport, civil protection, energy and environment.

---

[15] Source: http://europa.eu.int/comm/enterprise/security/articles/article_2005-04-06_en.htm

To prepare for the new financial period starting in 2007, in April 2005, a European Security Research Advisory Board (ESRAB), composed of private and public security stakeholders, was created and is in the process of advising the Commission on the content and the implementation of security research within the 7th RTD Framework Programme.

The European Security Research Priority enshrined in FP7 constitutes a basis for consolidation of all security research at EC level and has the ambition of providing a coherent and comprehensive set of responses to the high expectations of all stakeholders. It will benefit from the experience gained from the ongoing Preparatory Action for Security Research and from the longer term vision and inputs to be provided by the newly appointed ESRAB.

Being part of the 7th Framework Programme, security research will be pre-competitive in nature but will seek to provide tangible results and responses to urgent needs. It will therefore encompass research, development, integration and demonstration activities.

The credibility of security research at Community level stems from the high level of interest from the security constituency demonstrated through the Preparatory Action, its significant level of allocated financial resources, its comprehensiveness, its pragmatic approach based on mission- and capability-related activities and the clear recognition of the specific requirements of the sensitive security sector in terms of rules of participation, intellectual property rights, classified information handling and funding schemes.

Security research at Community level, managed by the Directorate-General for Enterprise and Industry under Vice-President Verheugen, focuses on civil security applications. However the Commissioner also sits on the European Defence Agency steering board, which will facilitate cooperation between the Commission and EDA on dual use aspects of security research.

XVIII.2.6. Conclusion

Today, Community policy on transport security relates to civil aviation, maritime transport, critical infrastructure, land passenger transport, the supply chain, transport of dangerous goods and energy facilities and infrastructures. DG TREN is the leading Directorate-General of the Commission for these topics. In addition, DG Enterprise is responsible for the main research and development projects. Coordination between both DG's synchronises the R&D on transport security.

The table below provides an overview of the security issues along the White Paper's action topics.

Table 2: Issues of the most likely scenario on transport security along the White Paper's action topics

		Implementation relevant to security	transport sector development
1.	Improving quality in the road transport sector	Directive 2004/82/EC on passenger data; ADR chapter 10, directive 94/44/EC, 96/35/EC, 2000/18/EC, 98/91, 1999/36 on dangerous goods;	Critical infrastructure protection; Multimodal supply chain security regulation;
2.	Revitalising the railways	RID part 5, directive 95/50/EC, 96/35/EC, 2000/18/EC, 1999/36 on dangerous goods;	Critical infrastructure protection; Multimodal supply chain security regulation;
3.	Balancing air transport and environment	Directive 2004/82/EC on passenger data; Regulation 3922.91 as framework on regulation on aviation and airport security; Regulation 2320/200 on civil aviation security; Regulations 1486/2003, 849/2004, 1138/2004, 622/2003, 68/2004, 1217/2003;	Multimodal supply chain security regulation;
4.	Promoting transport by sea and inland waterway	Directive 2004/82/EC on passenger data; Regulation 725/2004 on maritime security (ISPS code); ADNR chapter 10, directive 94/44/EC, 96/35/EC, 2000/18/EC, 1999/36 on dangerous goods;	Critical infrastructure protection; Multimodal supply chain security regulation;
5.	Turning intermodality into reality		Multimodal supply chain security regulation;
6.	Building the Trans-European transport network		Multimodal supply chain security regulation;
7.	Improving road safety		Critical infrastructure protection;
8.	Effective charging for transport		
9.	Recognising the rights and obligations of users	Regulation 2252/2004 on travel doc's; Memory of victims of terrorism;	The Hague Programme (Identity checks);
10.	Developing high-quality urban transport		
11.	Enabling clean, efficient transport		WCO Framework of standards to secure and facilitate global trade (a.o. Advanced Manifest Rule)
12.	Managing the effects of globalisation	Plan of Action against Terrorism; Framework of judicial, penal and police cooperation;	WCO Framework of standards to secure and facilitate global trade (a.o. Authorised Economic Operator);

Security is a strategy that should exist for passenger and freight transport from any door to any door. In this policy making process, DG TREN is on the right way to secure traffic and transport. The establishment of an integral European transport security policy should fully secure transport and energy markets

XVIII.3. Recommended scenario on transport security

XVIII.3.1. Achievement of White Paper objectives on transport security

Because of the fact that terrorism has become a supranational policy issue after 9/11/2001, the White Paper on European transport policy could hardly set the security policy actions in this field. This assessment however demonstrates in the previous chapters that the European Union has always put a secure society for its residents as one important fundament of the Union. A joint counteraction to terrorism is not only necessary because of the existing geographical relations, but unquestionably because of the corresponding democratic ideologies, the intense internal trade relationships and the joint interest for a competitive position worldwide.

Security is currently one of the hottest topics in policy making. The sense-of-urgency is stressed by terrorist attacks again and again. A common security policy on traffic and transport is highly needed to align and integrate the existing parallel initiatives, and fill the missing policy gaps. Such a policy should ensure an adequate counteraction by the Community to terrorist activity.

XVIII.3.2. Transport security objective

The aim of policy on 'security in transport and energy' is to conceive and implement measures to improve security, mainly to protect citizens against terrorism[16].

This assessment suggests the following relevant policy issues that also may be taken into consideration for Community policy (and an update of the White Paper) on transport security.

XVIII.3.3. European (transport) security policy

To mitigate terrorist threat, security policy should cover *(1)* an adequate structural prevention, *(2)* prevention of terrorist events and *(3)* reaction to these events. Structural prevention is the mitigation of terrorist threat at the highest level. This consists of the elimination of terrorists, the invalidation of radical anti-democratic (e.g. anti-Western) beliefs and conviction, and the plead for life principles like democracy, equivalence, human rights, compliance to the rule of law and fair justice. Prevention of terrorist events includes making terrorist preparations (e.g. terrorist procurement, smuggling of weapons, reconnaissance) highly difficult and resistance to terrorist actions (like the counteraction to observed actions of a terrorist attack). Reaction to a terrorist events comprises 'damage control' in terms of aid to victims and the capturing and arrest of the terrorist(s) involved.

Security measures should be proportional to the threat it is deployed to. Security policy should include *(1)* assessment of threats and vulnerabilities, *(2)* setting vulnerability priorities in terms of risk, impact and exposure time, and *(3)* taking suitable action(s) to mitigate the threats and/or minimise impact in accordance with the set priorities.

Security is a strategy that exists for passenger and freight transport from any door to any door. Therefore, a transport security policy should assess the threats, vulnerabilities and security opportunities in any perspective. Through prioritising, security research may be further dedicated to European's security needs.

---

[16] http://europa.eu.int/comm/dgs/energy_transport/security/index_en.htm (Accessed September 2005)

Putting security objectives into the existing White Paper's objectives underlines the importance of relating security to the other policy areas. Although the urge for security is a given fact, security still needs to be deliberated upon the other policy issues. The fundament of a European transport policy is the political balance that takes all interests of all policy issues into account. Security in traffic and transport may have become a very important additional objective to the White Paper's objectives, but an overall European transport policy should consider all objectives and all interests. Consequently, security may be added to the White Paper's objectives, but it needs to be in line with the other twelve.

It can be argued that a consistent European policy on transport security is needed to set long term Community objectives. The policy directions of the three most relevant directorates general (DG TREN, DG Taxhood, DG Enterprise and DG Freedom, Security and Justice) should be aligned and integrated to completely cover all security aspects. From a Community security perspective, a debate is needed on the range, extent and context in which the policy needs to be developed. In any case however, a security policy is needed in traffic and transport, because of the necessity for safe and secure travelling (e.g. commuting) residents and freight transport. In this field, DG TREN is on its right way.

XVIII.3.4. International Cooperation and Coordination

To ensure a sufficient level of protection of passengers, transport and energy infrastructures, and the prevention of trafficking of (wo)men, drugs, and weapons, security must be addressed as a political issue at international level.

In 2001, the White Paper already proposed to raise the European Union's profile within international organisations such as the International Maritime Organisation (IMO) and the International Civil Aviation Organisation (ICAO) to make Europe more assertive and place the EU at the forefront of the efforts to improve safety and protect the environment.

Today, European Union and DG TREN are actively involved in work and initiatives of international organisations like IMO, ICAO, IAEA, G8, OSCE, UITP, UITC.

In addition, bilateral Transport Security Working Groups are well established with US, Korea and Japan. Talks with Russia and Caspian Sea countries just got initiated. Transport Security Working Groups are aiming at:
  – enable common understanding of security matters;
  – exchange experiences and best practice;
  – make further progress towards standardisation of security practices;
  – establish mutual agreements of security practices allowing reciprocal reviews and leading to savings in the security treatment of cargo and passengers coming from countries with mutually recognised Security measures.

International cooperation and coordination may become more extensive in the field of security, because of the international character of terrorism. Resistance and mitigation of terrorist threats consequently requires joint measures and a joint policy approach.

At level of Member States, many governments may feel the sense-of-urgency of a tighter security regime, but hold in their actions on to their own traditional policy interests, objectives and priorities. An effective European (transport) security regime requires the full support of Member States to cooperate. This may require that they release important national priorities for the Community's good.

XVIII.3.5. EU must set a security awareness culture

Taking concrete security measures, the European Union should also create a social security awareness culture. Since terrorism endangers individual human wellbeing, all European citizen need to be aware of the threats they are encountering. It needs to be stressed here that terrorism does not only come from outside the EU. Terrorists can also come (and even be trained) from within the Community.

For travellers, citizen need to be properly instructed by the Community on what circumstances are too unusual and how an individual should react to it. Security instructions may save lives, just like the safety instructions can in civil aviation. In addition, citizen can assist security surveillance in this manner by reporting suspicious behaviour.

XVIII.3.6. Liberty paradox

The European Union has always striven for satisfactory citizens' liberties and rights. Due to counteracting terrorism, some privacy issues may come into discussion.

COM(2005) 124 states that "Freedom can only be enjoyed within a framework of personal security provided by law. In particular, citizens' liberties and rights can only be guaranteed if they are sufficiently protected from criminal acts, which do not only threaten the freedom and rights of individuals but also the democratic society and the rule of law." Hence, trough security measures, (supranational) governments are preserving a free wellbeing.

Effective security measures may also need information of individuals. However, privacy on personnel information is considered as one of the established liberties and rights in the Western society. Personal information does not only include information on living address and financial status, but also judicial files and biometrics (finger prints, face recognition). Providing more personnel information to the government and approving the government to use personnel information (also) for security reasons may pressurise the contemporary feelings on privacy in society.
The European Union should perform a profound debate on the privacy issues of security issues. Further, in addition to the security awareness culture mentioned in section XVIII.3.5, the European Union should create and prove the security culture in which the common sense is that 'Big brother is not watching you, but he is looking after you'.

XVIII.3.7. Towards common goals on security in traffic

Securing traffic consists of the resistance to misuse and sabotage to harm traffic networks in general and create casualties and (economic) damage in particular. Transport security policy should at least pay attention to the following issues.
1. Resistance to misuse and sabotage of transport infrastructure to prevent attacks on transport vehicles, intentional caused collision(s) of (public) transport vehicles, obstruction and blocking economic valuable network nodes and links;
2. Adequate technically equipped transport vehicles to defend against any kind of attacks (e.g. air missiles launched from ground) on public transport vehicles and minimise impact (in terms of casualties);
3. Resistance to misuse and sabotage of transport vehicles to prevent any kind of attacks on public transport vehicles and crowded areas;

4. Resistance to misuse and sabotage of traffic management systems (including air control) to prevent fraud, misuse of (vulnerability) information and any harm to these systems (including secure information exchange);

5. Resistance to misuse and sabotage of storage of dangerous materials (like fuel) near crowded areas (like air ports);

6. Deployment of the European satellite radionavigation programme Galileo for security requirements. The White Paper on European transport policy already suggested this issue[17]. COM(2004)636 also states that the GALILEO can be deployed as public regulated service[18].

7. Upgrading to traffic management systems (e.g. with cameras, real-time threat analysis and detection tools) to detect reconnaissance, preparations and execution of (terrorist) attacks;

8. Training personnel that uses traffic management systems in security awareness, detection skills, and intervention possibilities;

9. Training logistics personnel and regulating traffic planning where necessary to prevent dangerous goods being transported near very crowded areas in general and during rush hours in particular (e.g. chlorine transport through the very crowded Rotterdam central station Fridays at 7 pm);

10. Assurance that essential links in the transport network remain accessible in case of any kind of network failure;

11. Resistance to access to public transport services and crowded areas by possible terrorists carrying suspicious items that are potential means for attack;

12. Assurance that situation information is quickly accessible by the appropriate authorities to react to any (terrorist) event. This includes for public transport, free emergency exits available, number of persons present and vulnerable to terrorist attack, their physical status, and air quality. For freight transport this includes shipment information on goods present on spot, particularly of dangerous goods.

13. With specific respect to the EU border, security measures must be taken to secure:

    a. European sea ports in general;

    b. European sea border (especially the Mediterranean sea in relation to the Middle East and Africa);

    c. European air ports and airspace in general;

    d. European border by land (especially to Russia, Belarus, Ukraine, Rumania, Yugoslavia, Bosnia and Croatia);

14. The government needs to have adequate security surveillance and inspections teams. In respect of inspection, it can be questioned whether the customs (traditionally focussed on fiscal matters) is the appropriate party to conduct security checks. The military police or a dedicated institute could be an alternative.

---

[17] "By 2008 this project will provide the European Union with a system with global cover over which it will have full control and which will meet its accuracy, reliability and security requirements. It will thus have at its disposal a tool essential to its transport development policy. For instance, it will be possible using Galileo instantly to trace goods carried on the railway network, facilitating the development of a just-in-time policy. Galileo will permit highly accurate positioning of ships carrying dangerous cargoes and give the maritime authorities the means to ensure safe navigation, particularly in areas of high traffic density such as the Ushant TSS. The emergency, search and rescue and civil protection services are other applications for which Galileo will offer reliable, guaranteed solutions to the strictest standards." (COM(2001) 370, p.101)

[18] "It should be stressed that the public regulated service (PRS) is one of the key aspects of the programme. It will enable the public authorities to have a secure high-performance service. Many ministries have taken part in the technical definition of this service and confirm the need to establish it. This applies in particular to the services responsible for border surveillance and inland security, which are fighting crime, smuggling, illegal immigration and terrorism, etc, and civil protection teams. However, use of the public regulated service will remain optional. Member States and their administrations will be free to use it or not." (COM(2004)636, p. 7)

XVIII.3.8. Company responsibility versus governmental responsibility

The (supranational) government can not take all necessary security measures by itself. Many measures must be taken by companies involved. Because of regulation 725/2004, a terminal must for example comply specific security rules in a sea port.

European Union can either regulate security measures to be taken by companies or can initiate voluntary programmes. The choice between these two options depends on the both the responsibilities involved and the Community objective to be reached[19].

Company responsibility

Organisations are responsible for the activities they fulfil. Hence, organisations (including companies, institutes, foundations and so on) can be hold judicial responsible for their actions. Each (supply chain) company needs to have procedures and security management integrated in the overall company's strategy in general and supply chain management in particular, where necessary. Nonetheless, the liability of others misusing the organisation's activity should be limited to the deployment of security measures (incl. technique and procedures) to prevent unauthorised intended acts by others.

Policy makers need to enter a debate on whether such security measures need to be promoted through voluntary programmes or via regulation. Through regulation, the (supranational) government can set security measures for predetermined groups of supply chain parties without any unfair effect to market competition.

Governmental responsibility

The (supranational) government is responsible for a secure society in general and secure traffic and transport networks in particular. This includes the protection of crowded areas.

Consequently, the government can assure that companies take the necessary security measures and procedures, but the government is responsible if an attack takes place in any manner. Through surveillance and inspections the government can assure a secure traffic and transport.

XVIII.3.9. Towards common goals on security in freight transport

Trustworthiness should ensure that organisations responsible for traffic and/or transport are reliable in their actions. This includes both prevention of fraud and misbehaviour of the organisation's own employees and resistance to misuse and sabotage of the organisation's activities and information by others. Exemplary measures to ensure trustworthiness in transport (and traffic where appropriate) are:

1. Screening of employees and tracking of employees' behaviour where necessary in terms of security interest;
2. Ensuring the incorruptibility of dedicated security personnel by proper conditions of employment and salaries.
3. Security management procedures (e.g. like the coming ISO/PAS 28000);
4. Enhanced security management for shippers (e.g. security officer responsible for secure loading and unloading of containers and trucks);
5. Security certification to prove that a company can be trusted;
6. Security procedures and certification to prove that an authority issuing documents of title is a trustworthy party and that the documents can be trusted;

---

[19]   Note: this also stresses the need for a European transport security policy.

7. Secure (logistics) information exchange to prevent unauthorised copy and distribution of sensitive information, theft, and misuse of transport processes. This includes authorised issuing of logistics documents and verification of information where necessary (e.g. prohibition of forwarders distributing waybills to truck drivers via restaurants and other third party pickup points);

8. Verification of logistics documentation through parallel information exchange (e.g. sending a document both physically with a shipment and digitally to the consignee);

9. Supply chain security measures along the supply chain to protect the integrity of the door-to-door transport process. This includes road haulage but also intermodal transport chains, such as inland waterways transport, rail transport, short sea shipping, pipeline, inland terminals, and access and egress transport by road.

10. Threat analysis of procured goods and resources (incl. transport vehicles) and only collaboration (i.e. trade) with trusted parties where necessary;

11. Threat analysis of self-manufactured goods or self-provided services in terms of different purposes of usage by customers and third parties, and only collaboration (i.e. trade) with trusted parties where necessary;

12. Full container scanning in sea ports and air ports integrated in the logistics system of a terminal. This should affect logistics performance to a minimum. Full container scanning includes empty containers for sea and air transport and all types of loading unit used in air transport.

XVIII.3.10. Fair distribution of costs and benefits

A fair distribution of costs and benefits and – as a consequence – a fair competition is one of the fundaments of Community policy. Security measures may affect multiple organisations in the supply chain. Policy on transport security should realise that an organisation that needs to implement security measures, may not be the same as the supply chain party that benefits from the security measures.

For instance, manufacturers do not want the transport lead time of exported goods to be influenced by security checks in the country of destination. Looking at import of goods into the EU, such a manufacturer may apply for Authorised (secured) Economic Operator. But if the manufacturer deploys one or more logistics service provider(s) for the physical transport activities, both the manufacturer and the logistics service provider have to arrange their security procedures and other measures. The logistics service provider is forced to comply to the security requirements because of the risk of loosing market.

For a fair competition, transport security policy should consider whether Community security measures need to be taken voluntary by supply chain parties or that these measures are regulated. Voluntary programmes may have the disadvantage that costs and benefits of security measures are not distributed to supply chain parties in a fair manner.

XVIII.3.11. Transport security research

A profound and consistent transport security policy is missing as basis for security research in the Community. Current security research (i.e. PASR) is related to Community policy, but securing the Community requires policy to cover all security issues. The PASR projects can be allocated to the five predetermined priority research categories, but each individual project remains being proposed by researchers, consultants and business partners. A European transport security policy might be a more solid fundament for the necessary research on this important topic.

Transport security research may focus on the following exemplary topics:

1. Research and development (R&D) on threats of terrorism and criminality. This includes risk analysis (e.g. character travellers, child trafficking[20]), setting vulnerability priorities, and assessing the effects of possible counteractions;
2. R&D of real-time surveillance and intervention techniques to protect crowded areas;
3. R&D on decision making in surveillance and intervention to protect crowded areas (including strategies, procedures and training programmes);
4. R&D on tracking and tracing of traffic for end to end control of vehicle movement (incl. license plate recognition, identification and verification with black list, car tracking and car interception);
5. R&D on travel and logistics information scanning and processing techniques;
6. Programme to study secure methods to integrate security efficiently into the logistics transport process;
7. Training and knowledge exchange programmes of security guards.

---

[20] Child trafficking: e.g. a mother with five children registered on her passport becomes suspicious if she travels with four children. She can easily take a random child with her on a return journey. This child can be used for various undesired purposes, like sex abuse, suicide attack.

References

European Commission, Directorate-General for Energy and Transport, *Protecting Europe: ensuring the security of energy and transport services across the European Union*, leaflet, July 2005.

European Council, *Conclusions and plan of action of the extraordinary European Council meeting on 21 September 2001*, Brussels.

European Council and Commission, *Action Plan implementing the Hague Programme on strengthening freedom, security and justice in the European Union*, 9778/2/05 rev 2, Brussels, 10 June 2005

Heads of State and Government and the President of the European Commission, *Plan of Action against terrorism*, Brussels, 28 September 2001.

Heads of State and Government and the President of the European Commission, *EU Plan of Action on Combating Terrorism - Update*, Brussels, November 2004, 16090.

Solana, J., 2003. '*A Secure Europe in a Better World*', presented to the European Council meeting in Thessaloniki on 19-20 June 2003 by High Representative Javier Solana, and endorsed by the European Council on 12th December 2003.

The Hague Programme: *strengthening freedom, security and justice in the European Union, from General Secretariat to Delegations*, Brussels, 13 December 2004.

World Customs Organisation, *Framework of standards to secure and facilitate global trade*, version 3, June 2005.

Communications of the European Commission

COM(2001) 370	-	*WHITE PAPER* *European transport policy for 2010: time to decide* Brussels, 12.9.2001
COM(2003) 229	-	*Proposal for a regulation of the European Parliament and of the Council on enhancing ship and port facility security* Communication from the Commission to the Council and the European Parliament, the European Economic and Social Committee and the Committee of the Regions Brussels, 2.5.2003
COM(2003) 262	-	*The development of energy policy for the enlarged European Union, its neighbours and partner countries.* Communication from the Commission to the Council and the European Parliament Brussels, 13.05.2003
COM(2003) 687	-	*Proposal for a Council Regulation establishing a European Agency for the Management of Operational Co-operation at the External Borders* Proposal for a COUNCIL REGULATION Brussels, 20.11.2003
COM(2003) 704	-	*Some Key Issues in Europe's Competitiveness – Towards an Integrated Approach* Communication from the Commission to the Council and the European Parliament Brussels, 21.11.2003
COM(2003) 771	-	*Development of the Schengen Information System II and possible synergies with a future Visa Information System (VIS)* Communication from the Commission to the Council and the European Parliament Brussels, 11.12.2003

COM(2004) 72	-	*Communication on the implementation of the Preparatory Action on the enhancement of the European industrial potential in the field of Security research: Towards a programme to advance European security through Research and Technology* Commission communication Brussels, 3.2.2004
COM(2004) 101	-	*Building our Common Future – Policy challenges and budgetary means in the enlarged Union 2007-2013* Communication from the Commission to the Council and the European Parliament Brussels, 10.02.2004
COM(2004) 221	-	*Proposal for a Council decision on the exchange of information and cooperation concerning terrorist offences* Communication from the Commission to the Council and the European Parliament Brussels, 29.03.2004
COM(2004) 590	-	*Security Research: the next steps* Communication from the commission to the council, the European Parliament, the European Economic and Social Committee and the Committee of the Regions Brussels, 7.9.2004
COM(2004) 636	-	*Moving to the deployment and operational phases of the European satellite radionavigation programme.* Communication from the Commission to the Council and the European Parliament Brussels, 06.10.2004
COM(2004) 698	-	*Prevention, preparedness and response to terrorist attacks* Communication from the Commission to the Council and the European Parliament Brussels, 20.10.2004
COM(2004) 700	-	*Terrorist Financing – taking the fight forward* Communication from the Commission to the Council and the European Parliament Brussels, 20.10.2004
COM(2004) 701	-	*Prevention and consequence management in the fight against terrorism* Communication from the Commission to the Council and the European Parliament Brussels, 20.10.2004
COM(2004) 702	-	*Critical Infrastructure Protection in the fight against Terrorism* Communication from the Commission to the Council and the European Parliament Brussels, 20.10.2004
COM(2005) 124	-	*Proposal for a Council decision. Establishing the specific Programme "Prevention, Preparedness and Consequence Management of Terrorism", for the Period 2007-2013 General Programme "Security and Safeguarding Liberties"* Communication from the Commission to the Council and the European Parliament Brussels, 6.4.2005

COM(2005) 184	-	*The Hague Programme: Ten priorities for the next five years The Partnership for European renewal in the field of Freedom, Security and Justice* Communication from the Commission to the Council and the European Parliament Brussels, 10.5.2005
COM(2005) 195	-	*Communication on the mutual recognition of judicial decisions in criminal matters and the strengthening of mutual trust between Member States* Communication from the Commission to the Council and the European Parliament Brussels, 19.5.2005
Regulations and directives		
3922/91	-	Council Regulation (EEC) No 3922/91 of 16 December 1991 lays down the harmonisation of technical requirements and administrative procedures in the field of civil aviation.
94/44/EC	-	Council Directive 94/55/EC of 21 November 1994 lays down the transport of dangerous goods by road ("ADR framework directive")
95/50/EC	-	Council Directive 95/50/EC of 6 October 1995 lays down uniform procedures for checks on the transport of dangerous goods by road.
96/35/EC	-	Council Directive 96/35/EC of 3 June 1996 lays down the appointment and vocational qualification of safety advisers for the transport of dangerous goods by road, rail and inland waterway.
96/46/EC	-	COMMISSION DIRECTIVE 94/46/EC of 13 October 1994 amending Directive 88/301/EEC and Directive 90/388/EEC in particular with regard to satellite communications
98/91	-	Directive 98/91 of the European Parliament and of the Council, relates to motor vehicles and their trailers intended for the transport of dangerous goods by road, and amending Directive 70/156/EEC relating to the type-approval of motor vehicles and their trailers.
1999/36/EC	-	Directive 1999/36/EC to enhance safety with regard to transportable pressure equipment approved for the inland transport of dangerous goods by road and by rail.
2000/18/EC	-	Directive 2000/18/EC of the European Parliament and of the Council of 17 April 2000 lays down minimum examination requirements for safety advisers for the transport of dangerous goods by road, rail or inland waterway.
2320/2002	-	Regulation (EC) No 2320/2002 of the European Parliament and of the Council of 16 December 2002 establishes common rules in the field of civil aviation security.
622/2003	-	Commission Regulation (EC) No 622/2003 of 4 April 2003 lays down measures for the implementation of the common basic standards on aviation security.
1217/2003	-	Commission Regulation (EC) No 1217/2003 of 4 July 2003 lays down common specifications for national civil aviation security quality control programme.
1486/2003	-	Commission Regulation (EC) No 1486/2003 of 22 August 2003 lays down procedures for conducting Commission inspections in the field of civil aviation security.

68/2004	-	Commission Regulation (EC) No 68/2004 of 15 January 2004 amending Commission Regulation (EC) No 622/2003 lays down measures for the implementation of the common basic standards on aviation security.
725/2004	-	Regulation 725/2004 established a Maritime Security Regulatory Committee (MARSEC Committee) needed to ensure technical adoption of the Annex to Regulation 725/2004 and development of the necessary implementation tools
849/2004	-	Regulation (EC) No 849/2004 of the European Parliament and of the Council of 29 April 2004 amending Regulation (EC) No 2320/2002 establishes common rules in the field of civil aviation security.
871/2004	-	COUNCIL REGULATION (EC)No 871/2004 of 29 April 2004 concerning the introduction of some new functions for the Schengen Information System, including in the fight against terrorism.
984/2004	-	COMMISSION REGULATION (EC) No 984/2004 of 14 May 2004 amending for the 34th time Council Regulation (EC) No 881/2002 imposing certain specific restrictive measures directed against certain persons and entities associated with Usama bin Laden, the Al-Qaida network and the Taliban, and repealing Council Regulation (EC) No 467/2001.
1138/2004	-	Commission Regulation (EC) No 1138/2004 of 21 June 2004 establishes a common definition of critical parts of security restricted areas at airports.
2252/2004	-	COUNCIL REGULATION (EC) No 2252/2004 of 13 December 2004 on standards for security features and biometrics in passports and travel documents issued by Member States.
2004/82/EC		COUNCIL DIRECTIVE 2004/82/EC of 29 April 2004 on the obligation of carriers to communicate passenger data.
187/2005	-	COMMISSION REGULATION (EC) No 187/2005 of 2 February 2005 amending for the 43rd time Council Regulation (EC) No 881/2002 imposing certain specific restrictive measures directed against certain persons and entities associated with Usama bin Laden, the Al-Qaida network and the Taliban, and repealing Council Regulation (EC) No 467/2001
Commission Staff Working paper		
SEC (2004) 332	-	*European Security Strategy: Fight against terrorism* Commission staff working paper Brussels, 24.3.2004
SEC (2004) 669	-	*Compendium Counter-Terrorist Actions: Contribution of the Commission Services* Commission staff working paper Brussels, 25.05.2004
SEC (2005) 272	-	*Fighting terrorism: A memorial report dedicated to the victims of terrorism* Commission staff working paper Brussels, 28.2.2005
Invitations to tender		
TREN/J1/11-2005	-	*Protection of transport critical infrastructures at European Level* Invitation to tender European Commission, DG TREN Brussels, 2 May 2005

TREN/J3/13-2005	-	*Definition of critical infrastructures at EU level in the Energy sector* Invitation to tender European Commission, DG TREN Brussels, 2 May 2005
Notes		
16054/04 JAI 559		The Hague Programme: strengthening freedom, security and justice in the European Union, Note from General Secretariat to Delegations, Brussels, 13 December 2004
	-	

Definition of critical infrastructures at EU level in the Energy sector
Invitation to tender
European Commission, DG TREN
Brussels, 2 May 2005

APPENDIX A. THE HAGUE PROGRAMME

Also see "Note of the Commission of the European Union 16054/04, JAI 559"

The citizens of Europe rightly expect the European Union, while guaranteeing respect for fundamental freedoms and rights, to take a more effective, joint approach to cross-border problems such as illegal migration, trafficking in and smuggling of human beings, terrorism and organised crime, as well as the prevention thereof. Notably in the field of security, the coordination and coherence between the internal and the external dimension has been growing in importance and needs to continue to be vigorously pursued.

A key element in the near future will be the prevention and suppression of terrorism. A common approach in this area should be based on the principle that when preserving national security, the Member States should take full account of the security of the Union as a whole. In addition, the European Council will be asked to endorse in December 2004 the new European Strategy on Drugs 2005-2012 that will be added to this programme. The European Council considers that the common project of strengthening the area of freedom, security and justice is vital to securing safe communities, mutual trust and the rule of law throughout the Union. Freedom, justice, control at the external borders, internal security and the prevention of terrorism should henceforth be considered indivisible within the Union as a whole. An optimal level of protection of the area of freedom, security and justice requires multidisciplinary and concerted action both at EU level and at national level between the competent law enforcement authorities, especially police, customs and border guards.

In the light of this Programme, the European Council invites the Commission to present to the Council an Action Plan in 2005 in which the aims and priorities of this programme will be translated into concrete actions. The plan shall contain a timetable for the adoption and implementation of all the actions. The European Council calls on the Council to ensure that the timetable for each of the various measures is observed. The Commission is invited to present to the Council a yearly report on the implementation of the Hague programme ("scoreboard").

APPENDIX B. EUROPEAN FRAMEWORK FOR AVIATION AND AIRPORT SECURITY

The following regulation constitute the European framework of regulation on aviation and airport security[21].

Regulation 3922/91

Council Regulation (EEC) No 3922/91 of 16 December 1991 lays down the harmonisation of technical requirements and administrative procedures in the field of civil aviation.

Common rules in the field of civil aviation security

Regulation 2320/2002

Regulation (EC) No 2320/2002 of the European Parliament and of the Council of 16 December 2002 establishes common rules in the field of civil aviation security. It is a mandatory Regulation that is in effect since January 19, 2003 setting standards in aviation security at all EU airports. Regulation 2320/2002 was based on standards contained in ICAO Annex 17, recommendations of European Civil Aviation Conference and Commissions proposals, thus providing a comprehensive and advanced base for EU aviation security standards. EU Regulation 2320/2002 and its implementing regulations are applicable immediately after entry into force.

Regulation 2320/2002 also established an Aviation Security Regulatory Committee (AVSEC Committee) needed to ensure technical adoption of the Annex to Regulation 2320/2002 and development of the necessary implementation tools. The Regulatory Committee is chaired by the Commission and consists of experts representing all Member States.

Regulation 1486/2003

Commission Regulation (EC) No 1486/2003 of 22 August 2003 lays down procedures for conducting Commission inspections in the field of civil aviation security. EU Regulation 2320/2002 requires that Commission shall undertake monitoring of application of Regulations 2320/2002 and all its implementing regulations as of July 19, 2003. Regulation 1486/2003 sets forth the standards under which the Commission shall undertake its inspections of Member States application of Community standards

Regulation 849/2004

Regulation (EC) No 849/2004 of the European Parliament and of the Council of 29 April 2004 amending Regulation (EC) No 2320/2002 establishes common rules in the field of civil aviation security. Regulation 849/2004 amended the Regulation 2320/2002 in areas where clarification and necessary corrections where needed.

---

[21] http://europa.eu.int/comm/dgs/energy_transport/security/aviation/background_en.htm

Regulation 1138/2004

Commission Regulation (EC) No 1138/2004 of 21 June 2004 establishes a common definition of critical parts of security restricted areas at airports. Regulation 1138/2004 details and conformed with requirements set in Regulation 2320/2002. The work of the Aviation Security Regulatory Committee will continue to ensure that EU regulations meet the objectives and provide the necessary protection to civil aviation in the Community as well as incorporate international developments in the field.

Measures for the implementation of the common basic standards on aviation security

Regulation 622/2003

Commission Regulation (EC) No 622/2003 of 4 April 2003 lays down measures for the implementation of the common basic standards on aviation security. EU Regulation 622/2003 was developed in the Regulatory Committee and contains the operations standards needed to ensure harmonised implementation of standards set forth in Regulation 2320/2002. The implementing Regulation 622/2003 as well as all subsequent implementing Regulations are developed in the Regulatory Committee.

Regulation 68/2004

Commission Regulation (EC) No 68/2004 of 15 January 2004 amending Commission Regulation (EC) No 622/2003 lays down measures for the implementation of the common basic standards on aviation security. Regulation 68/2004 and 1138/2004 provided additional implementing.

Common specifications for national civil aviation security quality control programme

Regulation 1217/2003
Commission Regulation (EC) No 1217/2003 of 4 July 2003 lays down common specifications for national civil aviation security quality control programme. Regulation 2320/2002 requires establishment of National Aviation Security Programmes and National Quality Control Programmes needed to ensure proper implementation of Community and National standards. Implementing Regulation 1217/2003 was adopted and contains therefore detailed requirements on how a Member State shall effectively monitor proper implementation of Community and National aviation security standards.

APPENDIX C. EXISTING SECURITY INITIATIVES ON FREIGHT TRANSPORT

C.1.   *International Ship and Port Facility Security Code*

The ISPS Code has been set up by the International Maritime Organisation as a globally effective regulation to monitor the security situation on board ships, at port facilities and at the so-called ship/port interface - places where ships and port infrastructure such as quays come together or when a ship is mooring at a port. Examples of security measures are:
– Protect that persons enter port locations or sea-vessels while they are not allowed to enter these areas
– Protect that weapons and explosive material will be transported on board.
– The making of realistic security plans
– Training to make different parties comfortable to work with the new security plans.

Port Security operates at three security levels, established by the national Minister of the Interior Affairs.
– Security level 1: basic level, always applicable, maintenance of a minimum suitable, protective security measures.
– Security level 2: maintaining additional protective measures for a fixed period of time due to the higher risk of a security incident for example.
– Security level 3: maintaining further special protective security measures for a fixed period of time due to a security incident being probable or approaching (although the exact target may not be known).

EU Regulation 725/2004

Regulation 725/2004 of the European Parliament and of the Council of 31 March 2004 has the objective to introduce and implement Community measures aimed at enhancing the security of ships used in international trade and domestic shipping and associated port facilities in the face of threats of intentional unlawful acts.

The Regulation is also intended to provide a basis for the harmonised interpretation and implementation and Community monitoring of the special measures to enhance maritime security adopted by the Diplomatic Conference of the IMO on 12 December 2002, which amended the 1974 International Convention for the Safety of Life at Sea (SOLAS Convention) and established the International Ship and Port Facility Security Code (ISPS Code).

EU Regulation 724/2004

Regulation 725/2004 established a Maritime Security Regulatory Committee (MARSEC Committee) needed to ensure technical adoption of the Annex to Regulation 725/2004 and development of the necessary implementation tools. The Regulatory Committee is chaired by the Commission and consists of experts representing all Member States.

PAS 20858:2004

Public Available Specification (PAS) 20858:2004 places the ISPS code into the ISO framework[22]. A PAS can be seen as a pilot phase of an ISO certification. A PAS holds for three years and can only once be ex-

---

[22] www.iso.org

tended. Within these six years, businesses need to take up a PAS as an ISO standard, else the PAS is terminated.

ISO/PAS 20858:2004 is designed to ensure that the security measures of a port facility meets the requirements of the ISPS Code and appropriate maritime security practices and that the measures can be verified by an external auditor. It provides a framework to assist marine port facilities in:
– specifying the competence of personnel to conduct a marine port facility assessment;
– developing a security plan as required by the ISPS Code;
– conducting the marine port facility security assessment; and,
– drafting a port facility security plan to protect the people, ships and cargo within a port facility from the risks of a security incident.

C.2. Container Security Initiative

US Customs has developed the Container Security Initiative (CSI) in order to ensure that international terrorists do not misuse container transports for destructive and illegal activities. CSI should secure the ocean going sea container. The Container Security Initiative consists of four core elements (Eye for Transport, 2002):
– Establishing security criteria to identify high-risk containers
– Pre-screening those containers identified as high-risk before they arrive at U.S. ports
– Using technology to quickly pre-screen high-risk containers
– Developing and using smart and secure containers

Voluntary countries are Singapore, Netherlands, Belgium, France and Germany (Bremerhaven and Hamburg). Hong Kong and Malaysia have public concern that new security requirements will affect port efficiency (GIT, 2002).

CSI also comprises Customs representatives of one country to be located in a the country of one of the participants. Generally, US Customs has sent its representatives to the voluntary participants. However, Canada and Japan also have located their customs in the USA.

Part of CSI is the "**24 hours notice"-rule**. Cargo destined for the US and Canada must be submitted 24 hours before being loaded at their port of origin. US customs officers are being deployed in foreign ports to help identify and inspect high risk containers before they reach the US. The information about the container transport consist of port of origin, description of loading, owner, destination, route and transport and shipping companies. The electronic data interchange goes via the Automated Manifest System (AMS).

C.3. Customs-Trade Partnership Against Terrorism

The Customs-Trade Partnership Against Terrorism is an initiative of US Customs with private businesses to build co-operative relationships that strengthen overall supply chain and border security.
Businesses must apply to participate in C-TPAT. Participants will sign an agreement that commits them to the following actions:
- Conduct a comprehensive self-assessment of supply chain security using the C-TPAT security guidelines jointly developed by Customs and the trade community. These guidelines encompass the following areas: Procedural Security, Physical Security, Personnel Security, Education and Training, Access Controls, Manifest Procedures, and Conveyance Security.
- Submit a supply chain security profile questionnaire to Customs.

- Develop and implement a program to enhance security throughout the supply chain in accordance with C-TPAT guidelines.
- Communicate C-TPAT guidelines to other companies in the supply chain and work toward building the guidelines into relationships with these companies.

C-TPAT is currently open to all large and small sized importers and carriers in the US. However, since C-TPAT requests suppliers of these parties also to be compliant, also EU shippers and logistics service providers are involved.

Audits will be used to assess overall trade compliance. Customs Regulatory Audit will apply the new "Focused Assessment" methodology, a risk-based audit program, in conducting these audits. Companies will not be required to undergo a Focused Assessment in order to participate in C-TPAT. However, to take advantage of Customs Regulatory Audit Importer Self-Assessment (ISA) program, importers must be C-TPAT participants.

C.4.   Smart and Secure Trade lanes

Smart and Secure Trade lanes (SST) has been launched by the Strategic Council on Security Technology. SST is an industry-driven, supply chain security initiative. The SST initiative focuses on deploying an end-to-end, technical supply chain security solution – from point of origin to point of delivery -- across multiple global trade lanes.

C.5.   Operation Safe Commerce

Operation Safe Commerce is an program of the US Department of transport to fund US business initiatives designed to enhance security for container cargo moving throughout the international transportation system. The following methods are applied in this programme:
1. maintaining secure loading docks that restrict access to authorised individuals and that use cameras to monitor the loading process,
2. using technology to secure and monitor containers and their movement through the intermodal supply chain,
3. outfitting container with theft-resistant mechanical and electronic seals,
4. installing light, temperature, or other sensors in the interior of the container, which could be programmed to set off an alarm if the container is opened illegally at some point of transit,
5. conducting background checks of truck drivers who deliver goods to the port and outfitting them with biometrically based identity cards,
6. attaching electronic transponder and Global Positioning System to the truck cab and chassis or rail car carrying container and using intelligent transportation system technologies to monitor in-transit movements to and within the port terminal,
7. maintaining means to communicate with operators from their pick up to their off-load destinations.

C.6.   WCO Framework of standards to secure and facilitate global trade

In June 2005, the World Customs Organisation (WCO) democratically determined the WCO Framework of standards to secure and facilitate global trade. The framework consists of four core elements.
1. Harmonisation of advance electronic information on inbound, outbound and transit shipments.
2. Consistent risk management approach.
3. Sending nation's customs administration will perform an outbound inspection of high risk containers.

4. benefits to Businesses that meet minimal supply chain security standards

WCO framework rests on two pillars of Customs-to-Customs network arrangements en Customs-to-Business partnerships.

Customs-to-Customs Pillar

For Risk management, Screening and Inspection:
- There must be an ability to inspect and screen containers or cargo before it arrives.
- Customs administrations should use modern technology to inspect high-risk shipments. This technology includes large-scale X-ray en gamma-ray machines and radiation detection devices.
- The Customs administration should conduct outbound security inspection of high-risk containers and cargo at the reasonable request of the importing country.
- Maritime containers: screening and scanning prior to loading onto the ship.
- The customs office of departure must perform screening and risk assessment of containerised cargo prior to loading onto the ship.
- Customs should agree on consistent control and risk management standards.

Management of information
- The use of advance electronic information to identify high-risk containers or cargo.
- Customs administrations should agree to use an electronic messaging system to exchange Customs data.
- The exporter has to submit an advance electronic export Goods declaration to the Customs at export prior to the goods being loaded into the container (a list of 17 ID's).
- The carrier has to submit an advance electronic cargo declaration to the Customs at export and/or at import. For Maritime containerised shipments, the advance electronic cargo declaration should be lodged prior to the goods/container being loaded onto the vessel (a list of 13 ID's).
- The importer has to submit an advance electronic import Goods declaration to the Customs at import prior to arrival of the means of transport at the first customs office.
- National legislation must contain provisions to allow Customs to transmit information they collect to other Customs administrations.
- Advance Manifest Rule on declarations to be submitted:

Containers:	24 hours before loading at port of departure
Bulk:	24 hours before arrival at first port in country of destination
Rail:	2 hours prior to arrival at the first port in country of destination
Road:	1 hour prior to arrival at the first port in country of destination

- Customs should use WCO Customs data model (interoperable and open standard).
- The Ocean carrier provides advance electronic cargo manifest information to the terminal operator.

Seals and Technology
- Customs should facilitate the voluntary use of technologies to assist in ensuring the integrity of the container, e.g. the use of e-seals
- Customs should apply a seal integrity programme based on the use of a high security mechanical seal as prescribed is ISO/PAS 17712 at the point of stuffing.
- Customs should facilitate the voluntary use of technologies
- Seal integrity: the transhipment terminal operator shall inspect the security seal between the off-loading and re-loading of the container. This requirement may be waived for transhipment terminals which comply to the ISPS Code.

Certification and co-operation
-   The Authorised Supply Chain is a concept under which all participants in an international trade trans-action are approved by Customs. Consignments would benefit from an integrated cross-border sim-plified procedure.
-   In the context of the Authorised Supply Chain, the possibility for Customs to have online access to the commercial systems of the parties involved, once any confidentiality or legal issues haven been re-solved, would provide enhanced access information and offer the possibility for far-reaching simpli-fied procedures.
-   Governments should develop co-operative arrangements between Customs and other agencies in-volved in international trade to facilitate seamless transfer of international trade data (Single Window concept)
-   Authorised Economic Operators (AEO's) should be entitled to participate in simplified and rapid release procedures.

Customs-to-Business Pillar

Certification and validation
-   Creation of an international system for identifying private businesses that offer a high degree of secu-rity guarantees.
-   AEO's involved in the international trade supply chain will engage in a self-assessment process meas-ured against pre-determined security standards.

Benefits
-   Companies that demonstrate a verifiable willingness to enhance supply chain security will benefit.
-   Benefits include quicker movement of low-risk cargo through Customs and optimised supply chain cost through security efficiencies.
-   The Customs administration will offer incentives to AEO's including reduced risk-targeting, reduced inspections and expedited processing of goods.
-   The Customs administration should document the tangible benefits that the administration expects to provide

Security measures
-   The Customs administration and AEO should jointly determine and document the appropriate part-nership security measures that will be implemented and maintained by the AEO.
-   Security measures of the AEO include: security of buildings, control of exterior and interior perime-ters, access control, identification badges, terminated employee procedures, protection of trade-sensitive data, screening of employees, periodic background checks on employees working in secu-rity-sensitive positions

C.7. EU legislation

Carriage of dangerous goods

The international carriage of dangerous goods[23] has long been governed by established international agreements known, in the case of land transport, by the abbreviations ADR, RID or ADNR. These rules were drawn up by international organisations which have a wealth of experience and knowledge in the field. They are updated at intervals to keep pace with technical progress and improve safety.

---

[23] http://europa.eu.int/comm/dgs/energy_transport/security/goods/index_en.htm (Accessed June 2005)

The European Union's approach is to transpose these rules via specific directives which are then applicable to national transport too, not just transport between Member States

In the context of its global goal of improving safety in transport, the European Union has issued in 1999 the Directive 1999/36/EC to enhance safety with regard to transportable pressure equipment approved for the inland transport of dangerous goods by road and by rail. The Directive aims simultaneously to ensure the free movement of such equipment within the Community, including the placing on the market and repeated putting into service and repeated use aspects.

Directive 1999/36/EC is commonly referred to as TPED (Transportable Pressure Equipment Directive). In order to facilitate the use of the Directive, the Commission together with Member States' experts has elaborated TPED Guidelines, which may be found here. These will be completed as new Guidelines are adopted.

The carriage of dangerous goods is controlled by following legislation[24]:

Directive 94/44/EC

Council Directive 94/55/EC of 21 November 1994 lays down the transport of dangerous goods by road ("ADR framework directive"). The first general directive covering land transport was Directive 94/55, commonly known as the "ADR framework directive". This directive makes the provisions of the ADR agreement uniformly applicable to road transport nationally and between Member States, adopting in particular the technical annexes to the ADR agreement. These annexes set standards for the classification, packaging and labelling of dangerous substances and the construction of vehicles used to transport them.

Directive 95/50/EC

Council Directive 95/50/EC of 6 October 1995 lays down uniform procedures for checks on the transport of dangerous goods by road. This provides for a common list of points to be checked and the issuing of a copy of the report on the road check carried out. This is for the information of any authorities carrying out a second road check, either in the same Member State or another one.

Directive 96/35/EC

Council Directive 96/35/EC of 3 June 1996 lays down the appointment and vocational qualification of safety advisers for the transport of dangerous goods by road, rail and inland waterway. Under this directive "the activities of which include the transport or the related loading or unloading of dangerous goods by road, rail or inland waterway, (must) each appoint one or more safety advisers". Since this definition includes loading and unloading activities, it is also applicable to port undertakings which carry out these operations for the different modes of land transport.

The role of safety advisers is to help prevent the risks which these activities entail to individuals carrying out the work, other persons of the environment.

The directive also stipulates that the job of safety adviser may be done by an individual from outside the undertaking or by an employee already engaged on other duties.

---

[24] http://europa.eu.int/comm/dgs/energy_transport/security/goods/legislation_en.htm (Accessed June 2005)

The Commission sets great store by this directive, given the importance of the human factor in the risk of accidents and the part to be played by the safety adviser.

Directive 2000/18/EC

Directive 2000/18/EC of the European Parliament and of the Council of 17 April 2000 lays down minimum examination requirements for safety advisers for the transport of dangerous goods by road, rail or inland waterway. With this directive Member States shall take all necessary measures to ensure that safety advisers for the transport of dangerous goods are examined in such a way that they satisfy these minimum requirements.

Directive 98/91

Directive 98/91 of the European Parliament and of the Council, relates to motor vehicles and their trailers intended for the transport of dangerous goods by road, and amending Directive 70/156/EEC relating to the type-approval of motor vehicles and their trailers (OJ L11 of 16 January 1999). This directive is concerned with the type-approval of motor vehicles used to carry dangerous goods. It incorporates the technical requirements laid down by the ADR agreement and provides for the issuing of an EU certificate to facilitate vehicle registration in the various Member States.

Directive 1999/36/EC

Council Directive 1999/36/EC comprises legislation on transportable pressure equipment.   This is concerned with receptacles and tanks used to transport Class 2 gases. The proposal seeks to introduce a system of EU conformity markings for new equipment and EU markings for periodic inspections, with a view to free transport and use, including refilling, in all Member States of the European Union.

ADR 2005

The European Agreement concerning the International Carriage of Dangerous Goods by Road (ADR) was done at Geneva on 30 September 1957 under the auspices of the United Nations Economic Commission for Europe, and it entered into force on 29 January 1968[25]. The Agreement itself was amended by the Protocol amending article 14 (3) done at New York on 21 August 1975, which entered into force on 19 April 1985[26].

The Agreement itself is short and simple. The key article is the second, which say that apart from some excessively dangerous goods, other dangerous goods may be carried internationally in road vehicles subject to compliance with:
 the conditions laid down in Annex A for the goods in question, in particular as regards their packaging and labelling; and
-    the conditions laid down in Annex B, in particular as regards the construction, equipment and operation of the vehicle carrying the goods in question.

---

[25]   http://www.unece.org/trans/danger/publi/adr/adr_e.html (Accessed June 2005)
[26]   See for participants: http://www.unece.org/trans/danger/publi/adr/treaty.html

Chapter 1.10

A set of new Amendments entered into force on 1 January 2005, and consequently, a third consolidated "restructured" version was published as document ECE/TRANS/175, Vol.I and II ("ADR 2005").
In ADR 2005, a new chapter 1.10 has been included. Chapter 1.10 regulates 'security provisions' for the transport of dangerous goods. In this context, "security" means measures or precautions to be taken to minimise theft or misuse of dangerous goods that may endanger persons, property or the environment.

The new structure is consistent with that of the United Nations Recommendations on the Transport of Dangerous Goods, Model Regulations, the International Maritime Dangerous Goods Code (of the International Maritime Organization), the Technical Instructions for the Safe Transport of Dangerous Goods by Air (of the International Civil Aviation Organization) and the Regulations concerning the International Carriage of Dangerous Goods by Rail (of the Intergovernmental Organisation for International Carriage by Rail).

Notwithstanding the transitional measures provided for in ADR 2005, which allow compliance with certain requirements contained in previous editions, the editions of ADR published by the United Nations which may be used for compliance are as follows:
Until 30 June 2005:   2003 edition (ECE/TRANS/160, Vol. I and II and Corrig. 1-3);
As from 1 January 2005:   2005 edition (ECE/TRANS/175, Vol. I and II and Corrig 1);

APPENDIX D. PASR PROJECTS

D.1. *PASR project of Call 1*

According to Christiane Bernard of the Commission's Information Society Directorate-General (DG IN-FSO), from a total of 173 eligible proposals received under the first PASR call for proposals (PASR 2004), the Commission has selected seven projects and five supporting actions for funding[27].

1. TERASEC: detection of hidden weapons and explosives

The goal is to improve homeland security by delivering a new technology which will allow to detect threats, explosives, pathogens and chemicals hidden by a person or inside an object such as letters or luggage. The new technology is based on active and passive imaging concepts implementing terahertz (THz) radiation. In combination with advanced sensors this will lead to an increased level of security at public places for example airports. This new class of imaging systems will support governments, agencies and public authorities in their effort to protect the public against terrorism.

2. IMPACT: Innovative Measures for Protection Against CBRN Terrorism

Current European capabilities to detect and respond to the types of CBRN threats are very modest. Responsibility in Europe for initially responding to terrorist incidents is spread among many organisations. The lack of co-ordination is obvious. There is an urgent need to unify much of the current response capability while at the same time, setting standards and establishing guidelines for European nations to address coordination of their response to terrorism. To address the particular issues surrounding CBRN weapons, Europe must adopt a broad strategy to address the best ways to prevent a terrorist event.

The objectives of IMPACT are to lay the foundations for an integrated European CBRN counter terrorism research and acquisition programme and to validate, assess and demonstrate innovative technological capabilities, operational concepts and procedures to assist in developing preventive and suppressive crisis management.

The foundation of IMPACT will be to generate a limited set of planning scenarios and the design of a database of likely agents, actors, means of delivery and potential targets. This information will be applied to review, design and evaluate aspects involving CBRN counter terrorism, such as first responder operational concepts, C, B and R/N detection systems, physical protection and decontamination. The output of this process will be presented in 20 reports, 2 workshops, a demonstration and a database.

3. CRIMSON: crisis management system (CS)

The CRIMSON project aims to research, develop and validate an innovative system using the latest Virtual Reality technologies for the inter-organisational preparation, rehearsal and management of security missions in response to urban crisis (terror attacks, seizure of hostages, NBCR crisis, etc.).
The CRIMSON system will allow the 3D simulation and evaluation of complex urban crisis and contingency scenarios that would be difficult to simulate and validate in real conditions. This system will offer a unique tool for creating, communicating and sharing complex knowledge between users with very different educational or cultural background. It will dramatically enhance the planning and management of cri-

---

[27] http://europa.eu.int/comm/enterprise/security/articles/article_1681_en.htm

sis, the preparation of crisis management tasks, and, at the same time, it will provide a captivating tool for the collaborative training of the security actors and the information of citizens.

4. SUPHICE: Secure Unplanned Provisioning of High Integrity Communications
        Across Europe

In the EU, national classifications including the design of crypto take precedence over other member states and the Union itself and EU obligations to protect the rights of the citizen are enacted differently in each member state. SUPHICE will prove that;
- A common EU crypto with an unclassified design that is not owned by a member state is suitable for all grades in multiple nations;
- The EU's requirements for 'dual certification' can be achieved;
- A certified EU algorithm can be made available for requirements up to TOP SECRET;

SUPHICE will develop and demonstrate the use of on-demand, secure communications service-provision to deliver unplanned, policy based, reconfiguration of soft-loaded cryptos. This will enable communications consistent with national and international policies for the range of European and National agencies involved (MoD, Coalition, Civil, Intelligence). Using the above SUPHICE will create a working group of EU national IA authorities and propose ways forward.

5. ASTRO+: Integration of earth and space observation to support security operations

The objectives of ASTRO+ are to study and illustrate how space capabilities - Earth Observation and Reconnaissance, Navigation, Telecommunication and their integration and implementation into services and infrastructures *1)* can contribute in the short and long-term to the equipment of Europe in security facilities supporting i.e. the improvement of foreign operations, and *2)* Can support the definition and elaboration of the European Research Security Programme by proposing an R&T innovation roadmap for space.

6. ISCAPS: Surveillance of crowed areas exposed to terrorist attacks

Through a two year approach, the general objective of ISCAPS is to reduce the risks of malicious events by providing efficient, real-time, user-friendly, highly automated surveillance of crowded areas. This goal will be achieved through industrial research in complementary technologies, bringing some existing technologies to maturity and demonstrating them in a real world environment.

The general scenario for ISCAPS is a public area in which people are moving around, and where there is an opportunity for expected threats. The project will examine different types of public area and their surveillance requirements. These types will include:
- different crowd densities – ranging from isolated individuals to fairly crowded areas (using standard definitions of groups and crowds)
- different control levels for managing the public area – gated (restricted) areas, channelled areas and open areas.

7. VITA: protection of critical infrastructures – demonstration on energy

This project will deliver results on the threats to and assurance and protection of highly networked infrastructures, most of which are operating trans-nationally, and disruption of which is critical to Europe's security, the well being of its citizens and to the functioning of its economy. The project aims to provide:

---

1. Methods to raise awareness and the sense of urgency on the need for international critical infrastructure protection at both the European and national levels by developing, executing and analysing a scenario at the level of European Directorates with national stakeholder participation;
2. A vision on methods, tools and technologies required for the protection (pro-action, prevention, preparation, incident response, and recovery) of critical infrastructures as preparation for the forthcoming European Security Research Program (ESRP) agenda.
3. A demonstrator experiment of tools and technologies in a selected set of end-user applications for proving the feasibility and efficiency of the approach.

Support activities

In addition to the seven PASR projects, five support activities have also been started. Support activities are mostly desk research and do not have a demonstration requirement, like the PASR projects. The support activities are the following projects:

1. GEOCREW: Study on crisis management early warning system using geospatial data

The GEOCREW study is dedicated to the early detection of (man-made) crises with a potential international dimension and relevance to the security of European citizens. If detected early, a crisis can be handled and solved at lower engagement levels before it evolves to critical or military dimensions. There are two parts of the study which concentrate on different focuses and complement one another. Whereas the CREW part will comprise an overall architecture for integrating different information sources identified through user requirements of security related services, the GEODATA study part concentrates on the specific utilisation of geospatial data for improving situation awareness, using a more detailed technical approach. An essential part of the study is the collection of operational and functional requirements on geospatial and non-geospatial information from / together with the relevant users.

2. ESSTRT: European Security: High Level Study on Threats Responses and Relevant Technologies

The object of the Study will be to tie together multiple threads of work across the security spectrum with special emphasis on research and technological development (RTD). The results of this Study will be delivered at the mid-term of the Preparatory Action thereby allowing their exploitation in the building of the future security programme.
It will provide the Commission with a comprehensive overview of necessary responses to terrorism, by:
- Analysing threats and political context;
- Recommending new security approaches;
- Reviewing current and potential technologies, and shortfalls;
- Prioritising future security research efforts.

Two areas of technology will be studied:
- Systems providing situational awareness to protect against terrorism (that is, physical security);
- Security of communications and protection of information and networked systems.

The study will take account of European views to the widest possible extent. It will include consultation with end-users, NGOs, research institutes, community leaders, and governmental organisations. The information gained in the study will be used by the Commission to guide future security research effort.

3. TIARA: Treatment Initiatives After Radiological Accidents

The purpose is to constitute a European network which may participate in enhancing the management of a crisis after the malevolent dispersal of radionuclides in a public place.
A preview of the state of the treatment of contamination by radionuclides in Europe highlights the following points: a decrease in the number of physicians with experience of treatment, operational issues not anticipated, a need for the rationalisation of treatment and research into new treatments.

We propose to:
-    provide guidance on dose assessment and efficacy of treatment,
-    foresee the operational needs for treating persons in the case of mass casualties,
-    monitor scientific and technological development on research into new treatments.

This project includes physicians involved in decorporation treatment or in other emergencies, experts involved in dose assessment and research studies. The participants, exercising informed discussion with other physicians and scientists, intend to develop a European network which may disseminate information, contribute to the rationalisation of decorporation treatment and advise on European research programs where deficiencies are apparent.

4. SENTRE: Security Network for Technological Research in Europe

The SeNTRE support activity has the objective to prepare a strategic research plan for European security by establishing and consulting a network of users and technology experts at national and European levels in support of and to link with future EC Advisory Board on Security.

Performed by a number of European organisations with relevant expertise in these domains, the study provides the EU with a comprehensive input for planning the programmes for security research. It brings together a network of users from Member States and European organisations and through this approach makes a major contribution to the security of the citizen in Europe. Politically, it develops support for the action and builds visibility. Technically, it helps achieve wider commonality of the best possible security systems in Europe. Organisationally, it paves the way for an improved exchange between national and European levels through a network of security and technical experts**.**

D.2.   PASR projects in call 2

Source: http://europa.eu.int/rapid/pressReleasesAction.do?reference=MEMO/05/277

1. TRIPS: Improvement of the protection of rail passengers

The events in London show the vulnerabilities of the rail systems. Terrorists select targets based on the perceived weaknesses, on national sensitivities, on the extent of consequences and the impact on the public. The research project TRIPS (Transport Infrastructures Protection System) will design and demonstrate an anti-terrorist security system architecture that will allow the detection of terrorist threats (explosives chemical, biological, radiological and nuclear substances) on mainline or metro railway systems. The project will combine information from sensors, remote control or autonomous cameras, ground penetrating radars and line scanners.

The consortium is composed of significant industries, research organisations, SME's and organisations representing end-users spread over 11 Member States. In addition, an advisory group gathering governmental representatives and railways/public transportation operators will validate the different stages of the development of the project and contribute to the dissemination and the use of the results.

2. SOBCAH: Safer European borders

The new European border is formed of 6.000 km of land borders and 85.000 km of coastlines! It thus provides easy access for illegal migrants, drug smugglers and terrorists.
Surveillance across Europe is the focus of the SOBCAH project, driven by a well balanced consortium finalised after consulting a broad panel of industries. By establishing an Advisory Board encompassing the dispersed community of green and blue borders security stakeholders, this project investigates every possibility to increase the effectiveness, connectivity and reactivity of borders and harbours.
It will allow the advisory board to formulate needs that have not yet been expressed (gap analysis, enabling technologies, net-centric architectures, standardisations issues…) and to determine FP7's technological priorities. The diversity of rules and laws of EU countries will be taken into account. In parallel, practical solutions to increase the connectivity and reactivity of current information and sensors networks will be elaborated and materialised to demonstrate more effective and further automated surveillance functions in European harbours. This demonstration will confirm the gap analysis and rally the advisory board to a common analysis mixing both bottom-up and top-down views of the security issues, with a roadmap toward technical and operational solutions.
The project brings together 16 partners from 9 Member States out of which one new Member State. The involvement of a user group adds value to the project which is built-up upon and develops further existing activities.

3. ROBIN: Securing computers linked to networks

The vulnerability of ICT infrastructure is one of the key threats to modern society. Experience shows that this vulnerability is largely rooted in commonly used operating systems that have become incredibly complex and are thus very hard to harden against attacks. However, in practice the use of these legacy systems cannot be avoided. Even worse, stripped down versions increasingly find their way into embedded systems thus increasing the vulnerability of our infrastructure.
This project's (ROBIN) main benefit will be to robustly secure computers linked to networks. A robust platform will be developed by a small team of industries and universities (supported by a user group).
This platform hosts legacy operating systems and their applications which will be split into security sensitive and other areas. This platform will be open and originate from Europe which will establish an alternative to proprietary US solutions that are expected to appear soon.

4. PATIN: Security information network, airport, terrorism, protection exercises

This proposed project aims to ensure a comprehensive integrated system to improve the security of EU citizens by protecting the complete air transportation system, including aircraft, ground infrastructure and information networks against terrorist – including CBRN (Chemical, Biological, Radiological or Nuclear) - attacks.
The project (PATIN) will assess aspects of crisis management, interoperability and optimisation of security networks. The project's primary aim is to deliver tangible results in a field of immediate security challenge. PATIN analyses all potentially relevant threats and technologies. It derives from these a set of viable future operational concepts. On this basis a conference and joint exercises will be organized where

the entire stakeholder community, users and security organizations can assess the operational concepts and the improved security provided.

The project is built on a layered protection mechanism which forms a system-of-system interconnected through networks. A top level information network will provide situation awareness for the whole European air transportation. Local networks will detect anomalies at airports followed by reactive and proactive measures against co-ordinated terrorist attacks. Major deliverables are the basis for developing the roadmaps required to establish a platform for the future European Security Research Programme.

A pan European consortium from nine countries including end users, SMEs and research establishments has been formed.

5. MARIUS: More rapid and efficient crisis management

The main benefit of the proposed MARIUS project lays in the development of a pre-operational autonomous command post, equipped with its own sensors, information and communication systems, which can be deployed quickly to monitor crisis management operation. Its importance lies in the implementation of a demonstrator which could easily be deployed for inter-agency cooperation, situation assessment and decision making. The Demonstrator will be deployable by helicopter and will incorporate open scalable IT infrastructure, generic gateways, decision support and crisis communication support.

MARIUS focuses on improving Crisis Management efficiency: deployment rapidity, inter-agency co-operation, situation assessment and decision-making. It addresses other priority missions through the operational scenarios and (pre-)normative aspects.

Participants:
- the User Group, comprising national end-users and European Stakeholders, will warrant the operational pertinence of the project, from the present situation (NATO/Framework Nations dependency) to the 2010 Headline Goals,
- the Consortium, composed of 13 selected industrial and academic partners, will provide a pre-operational version of an easily deployable Command and Control Centre integrating technological components to evaluate innovative functions.

6. Protection of airliners against MANPADS attacks (man portable air defence systems)

Airplanes are vulnerable and attractive targets for terrorists. Recent events showed that man portable air defence systems (MANPADS) have become a new weapon in the hands of terrorists. Aircraft protection against missiles is already mastered in the military field but a mere adaptation of existing products will not match the much more demanding requirements of the civilian environment.

The proposed project (PALMA) addresses the protection of commercial aircraft against MANPADS with an appropriate and recognised industrial and technological expertise. The project aims to define both the required technological solutions and supporting operational concepts. In addition the project will offer the possibility to gather experience in handling classified information within research projects which will be an important aspect for the future security programme.

7.HiTS/ISAC: Highway to security: Secure interoperability of intelligence services

The vision of the proposed project HiTS/ISAC is a more secure Europe through prevention of terrorism and organized crime. It addresses the interoperability of intelligence services to exchange information on suspicious activities in order to enable information analysis and fusion from different sources.

Superior situation awareness and cross-border interoperability are key enablers, leading to new technical and operational methods to work, train and co-operate across Europe. Today, information on suspicious

activities in databases at law-enforcement authorities is distributed across Europe. The information is not easily available to other authorities in Europe, especially not "on-line".

The objective of HiTS/ISAC is to enable information analysis and fusion from many different sources, through secure cross-border on-line group co-operation between authorities, in order to detect and provide early warnings for suspicious activities, be it communication between suspected criminals, or anomalous movement of persons, goods or money, etc. HiTS/ISAC will develop a problem solving environment and demonstrate it in a virtual operations room which can be established anywhere, at any time. Tools and processes will be developed and implemented, and demonstrated using realistic scenarios.

8. PROBANT: *Crisis management: People real-time observation inside buildings*

Visualization and tracking of people inside buildings is a powerful tool to guide security forces in surveillance and crisis management. The objective of the PROBANT project will be reached by integrating technological novelties like arrays of sensors, modulated scattering, pulsed signal techniques, advanced data processing, biometric measurements. The technologies will be validated by the tests in realistic environment of three demonstrators. Conclusions will be drawn about the performance of the assessed techniques and future opportunities for further research and industrialization.

The team guarantees an optimum match between user requirements and technological excellence, being composed of an innovative French industrial company, a European Research Centre, a Dutch University and two national police agencies for specialist criminal investigations.

This project gathers a comprehensive consortium merging latest innovative techniques aimed at the realization of a breakthrough in security technology. It is lead by an industrial SME and brings together academic / industrial researchers with users (police forces) from 3 Member States.

9. PETRA.NET: *Network for the promotion, enhancement and take-up of security research*

This proposed supporting activity (PETRA.NET) will establish a network linking the security research community with public authority users such as the police, fire brigade, ambulance service and civil defence. It will develop secured systems for information exchange between researchers and end users. This network will promote the transfer of research results into the operational environment using trusted and secure dissemination mechanisms. It will also support the cross-fertilisation of emerging research results between PASR activities and the public authority user community.

PETRA.NET will meet these objectives through three thematic sub-actions:

- Establishing an interface between the PASR research community and the public authority user community in the form of an observatory
- Brokering information exchange relationships between members of the research and the user community
- Analysing, disseminating and exchanging information on how PASR research can have an impact in the operational environment.

PETRA.NET is led by members of the public authority user community with a wealth of experience in EU-funded research. They are therefore ideally placed to establish this network and to broker the necessary cross-fertilisation relationships.

10. SECCOND: *Standardisation of the technical interface between a secure container and a data reader at a port or border crossing*

This proposed project (SECCOND) is a network intended to initiate the international standardisation of the technical interface between a secure container or vehicle and a data reader at a port or border crossing.

The primary purpose of the interface is to enable law enforcement officials to determine where the container or vehicle has been, whether items (e.g. weapons of mass destructions) or people may have been inserted en route, and whether there may be hazardous items within it. Secondary purposes are to interface to a cargo tracking system and to provide data for automated cargo handling systems. The interface will be specified in such a way that it:

- employs radio frequencies which can be used worldwide
- can be read rapidly and at a range consistent with port operations
- has authentication and data protection features
- has optional data fields to support new sensors
- can be implemented in a device with low cost, small size and low power consumption.

11. BSUAV: Unmanned aerial vehicles to peacetime security

The purpose of this supporting activity (BSUAV) is to present a structured analysis of the potential contribution of unmanned aerial vehicles (UAV) to peacetime security on European borders. The study intends to understand the problems posed by various types of borders and to define realistic UAV based systems that would answer to those problems. The study results will be presented to end users, coupled with a live demo of a small UAV conducting a typical surveillance mission.

The expected outcome of the study will be:

- a global synthesis of border control problems. Similarities and differences between regions, national specificities and local analysis of threats,
- development of original and innovative concepts of use for UAV based surveillance systems,
- assessment of required technologies
- all available in less than ten years
- to support the proposed systems,
- conclusion including End-Users feedback on proposed solutions, and on UAV use itself.

The study will be conducted in five steps:

- the understanding of problems posed to people in charge of security on the continent's various types of borders,
- the synthesis of these expressions of need under the form of generic situations,
- the requirements on UAV systems able to handle these situations,
- as a conclusion the definition of realistic UAV based systems that would fulfil most of those requirements.
- presentation of those results to end-users.

The consortium is a well balanced partnership between industry, laboratories and universities covering the whole spectrum of technical requirements on one side and end users on the other side.

12. PRISE: Innovative security technologies and policies in line with privacy protection and human rights in general

Addressing the critical area of public acceptance of security technology, the results of this supporting activity (PRISE) could have a significant impact on European security research. PRISE will promote a secure future for European citizens based on innovative security technologies and policies in line with privacy protection and human rights in general by:

- developing and testing a set of criteria and guidelines for privacy enhancing security research and technology development
- elaborating these criteria and guidelines with direct involvement of providers of security technologies, private and public users and implementers, institutions and bodies shaping policies as well as organisations representing potentially conflicting interests

- transforming the results into privacy enhancing development and implementation scenarios of security technologies and measures
- testing these scenarios in a set of participatory technology assessment procedures in different European states allowing for a substantiated indication of public perception and citizens' preferences
- disseminating the results to actors relevant for the shaping of technologies and policies
- increasing competitiveness of European security industries by providing guidance for the provision of widely acceptable security technologies.

13. USE IT: Exchange of sensitive information: User/supplier network for information technology security

USE IT proposes to define a cooperation approach on the exchange of sensitive information between European organizations (private/public companies, universities/research labs, certification bodies…) to address user needs and user communities working in the security technologies. The main objective is to structure the European research and development community in the information technology security (ITS) domain by setting up an organized network with an adequate legal frame and dedicated communication means.

USE IT is built around experts coming from legal, technology and security fields. Based on consortium experience in security evaluation, IP management, legal aspects and sensitive data exchange the project corresponds to three priorities (building co-operation, classified information exchange, heavy analysis means joint use) of the PASR-2005 call.
A well balanced and knowledgeable consortium is established, creating a useful link between the technical and the legal communities in the security area.