EUROPEAN COMMISSION

Brussels, 25.11.2011
COM(2011) 790 final

COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT AND THE COUNCIL

First Annual Report on the implementation of the EU Internal Security Strategy

COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT AND THE COUNCIL

First Annual Report on the implementation of the EU Internal Security Strategy

I. Introduction

In July this year, a right-wing extremist in Norway carries out a devastating terrorist attack. In August, public authorities in the UK seize 1.2 tonnes of cocaine in a record haul. Across the EU, cyber attacks increasingly wreak havoc on public and private computer systems. These are stark reminders of the importance of action to counter threats to internal security.

'The EU Internal Security Strategy in Action',[1] adopted in November 2010, outlined priorities for the EU to focus on for the coming four years, which are: (1) the disruption of international criminal networks, (2) the prevention of terrorism and addressing radicalisation and recruitment, (3) raising the levels of security for citizens and businesses in cyberspace, (4) strengthening security through border management and (5) increasing Europe's resilience to crises and disasters.

As security threats emerge and evolve, the EU must be ready to respond. Regular threat and risk assessments from EU organisations such as Europol, Eurojust, Frontex and the EU Joint Situation Centre (SitCen), are necessary.

The latest Europol report[2] identifies three emerging threats of particular concern:

First, issues related to the fast-paced nature of **internet technology**. The internet is now an integral and indispensible part of the everday lives of EU citizens, but it is also becoming a major facilitator for a wide range of criminal activities and a vehicle for terrorist propaganda. Increasing reliance on internet technology makes our society more vulnerable to high profile hacking attacks, which can target administrations, industrial control systems or banks.

Second, the potential implications of the **ongoing economic crisis.** Increasing financial constraint may reduce the resources available to public authorities to combat internal security threats. There is no obvious and immediate solution to this – but we all need to be aware of the constraints and its consequences.

Third, the impact on the EU of the **external dimension of security**. The internal security of the EU is closely linked to the security situation in its neighbourhood, as demonstrated by recent events in the Arab world. These encouraging events which bring democracy and prosperity to the region, have also created considerable movements of people, putting increased pressure on neighbouring countries' border management capabilities including the EU's external border. Equally, continued displacement of people, and gaps in governance, may create conditions for increased criminal and terrorist activity across the Sahel area. To the south east of the EU, the Western Balkan countries continue to be a source of concern due

[1] Commission Communication: The EU Internal Security Strategy in Action: Five steps towards a more secure Europe — COM(2010) 673/3, (hereinafter 'the ISS in Action').

[2] See Europol: Organised Crime Threat Assessment (OCTA) 2011.

to the persistent activities of transnational organised crime, such as illicit trafficking in drugs, human beings and counterfeit goods.

The need for EU cooperation to face these challenges has never been greater. Implementation of the identified actions will be necessary within the coming years. But this will not be enough. These strategic objectives need to be translated into concrete plans and actions. In this respect, the Commission welcomes the methodology of the EU Harmony Policy Cycle, which will translate political priorities and threat assessments into operational action plans specifically in the areas of serious international and organised crime, cybercrime and border management, through the delivery of the eight priorities as agreed by the Council.[3]

In taking forward implementation of the Internal Security Strategy in Action, the Commission will continue to ensure full respect for the rule of law and the European Charter of Fundamental Rights, including the privacy rights of individuals.

The following report provides an assessment of the implementation of the ISS in Action in 2011. It outlines the state of EU internal security in the area of each of the ISS's five objectives[4] and provides a forward look for actions in 2012. A detailed evaluation of the key measures implemented in 2011 can be found in the Annex.

II. The state of EU internal security

1. Organised crime/international crime networks

A new criminal landscape is emerging, which is increasingly characterised by highly mobile and flexible groups operating in multiple jurisdictions and criminal sectors, and aided, in particular, by widespread illicit use of the internet. The groups with the best resources have gathered diverse portfolios of criminal business interests, improving their resilience at a time of economic austerity, and strengthening their capability to identify and exploit new illicit markets. Activities involving low levels of perceived risk, such as carbon credit fraud, payment card fraud and counterfeiting of various goods, are increasingly attracting the interest of established criminal groups.

Although the goals of terrorist and organised crime groups differ, the connections between their activities appear to be growing. Crime is being extensively used to finance terrorist activities.[5] Terrorist groups may be involved directly in organised crime or affiliated to individual criminals and criminal groups, in areas such as trafficking in weapons and drugs, in human beings, or financial fraud, money laundering and extortion.

Cross-border cooperation between authorities is an essential element in meeting the challenges to EU internal security. However, the instruments available for information exchange, in particular the Swedish Initiative[6] and the Prüm Decisions,[7] are still not fully

---

3 See Council conclusions on setting the EU's priorities for the fight against organised crime between 2011 and 2013; doc. 11050/11, JAI 396 COSI 46 ENFOPOL 184 CRIMORG 81 ENFOCUSTOM 52 PESC 718 RELEX 603. See also Annex.

4 This was prepared by Europol with contributions from Eurojust, Frontex, Commission/DG ECHO, inter alia based on the strategic documents — Europol's Organised Crime Threat Assessment (OCTA) 2011, Terrorism Situation and Trend Report (TE-SAT) 2011, Frontex' Annual Risk Analysis (ARA) 2011 and Western Balkans Annual Risk Analysis (WB ARA) 2011 — and on the casework of Eurojust, as reflected in its Annual Report 2010.

5 See Europol: EU Terrorism Situation and Trend Report (TE-SAT) 2011.

6 Council Framework Decision 2006/960/JHA of 18 December 2006.

implemented in the Member States. More coherence and consolidation of cross-border law enforcement information exchange is still needed.

Europe's citizens must have the assurance that effective disruption of criminal networks is complemented by the coordination of efficient and fair prosecutions. However, various instruments for judicial and law enforcement cooperation have yet to be ratified and implemented by all Member States.[8] Furthermore, the differing requirements of the Member States in relation to cross-border search and seizure can impede the coordination of urgent actions in different jurisdictions. A European Investigation Order would reinforce the principle of mutual recognition and address current difficulties in obtaining information and evidence in cross-border cases.

The overall value of the assets frozen and confiscated in the EU remains low compared to the estimated wealth of criminal organisations. More needs to be done in order to trace and seize criminal assets more effectively. Organised criminals are seeking to re-invest in lawful activities, which means that there is a need for stronger rules to combat money-laundering, and greater operational focus on the means by which criminals infiltrate the licit economy.

In 2011, to bolster the EU's toolbox in the fight against organised crime, the Commission inter alia adopted a package on anti-corruption and proposed EU legislation on the collection of Passenger Name Records on flights entering or leaving the territory of the EU.

Way forward in 2012

The Commission will:

- **adopt a package on confiscation and recovery of criminal assets;**
- **present a proposal on the reform of Europol and CEPOL together with the European Training Scheme;**
- **present a proposal on the reform of Eurojust;**
- **aim to conclude two new PNR Agreements with the U.S. and Canada;**
- **work towards the adoption of its proposal for a Directive on the collection of Passenger Name Records;**
- **present a Communication on the European Information Exchange Model;**
- **elaborate a financial investigation strategy;**
- **present a proposal for a revised Directive on Anti-Money Laundering/Countering the Financing of Terrorism; and**
- **issue a five year strategy on trafficking in human beings.**

[7] Council Decisions 2008/615/JHA and 2008/616/JHA (Prüm Decisions).

[8] Such as the European Convention on the Transfer of Proceedings in Criminal Matters of 1972 and the Convention on Mutual Assistance in Criminal Matters between the Member States of the EU of 2000.

Member States are encouraged to:

- **implement the actions foreseen in the EU Policy Cycle;**
- **step up efforts to develop the administrative approach, involving all public sector bodies, not just law enforcement bodies, to protect the economy against crime and corruption;**
- **make progress in establishing effective asset recovery offices and in facilitating exchange of information and best practice;**
- **ratify and implement existing instruments for judicial and law enforcement cooperation and information exchange, including the Swedish Initiative, the Data Retention Directive and the Prüm Decisions, as well as the Conventions on transfer of proceedings and on mutual assistance in criminal matters; and**
- **transpose the Directive on trafficking in human beings without delay.**

2. Terrorism and radicalisation

A decade after the events of 9/11, statistics on terrorist suspects indicate that Islamist terrorism remains the prevailing threat to the EU. Nevertheless, the tragic events in Norway in this July remind us that the threat posed by terrorism is not confined to a single set of political or religious ideologies or motivations. The First Response Network, established in the wake of the 2005 terrorist attacks in London, was activated for the first time following the attack in Norway and proved to be useful.

Home-grown terrorism and radicalisation of EU citizens is increasingly becoming a source of concern. The EU needs to stay ahead of developments both in terms of the process of radicalisation and the technology used. The EU Radicalisation Awareness Network, launched in September 2011, is designed to facilitate knowledge-sharing, raise awareness and identify new and creative solutions to counter violent extremism. The Commission will ensure that a coherent approach with the EEAS and the Counter-Terrorism Coordinator is taken to counter violent extremism both within the EU and externally.

The risk of radicalisation of individuals cannot be entirely eliminated. Therefore, initiatives which prevent terrorist access to funding and materials and which improve transport security will be critical in the fight against terrorism. In 2010, the Commission proposed an EU action plan to strengthen air cargo security, with new rules and a definition of criteria for identifying high risk cargo, and has now progressed to the final stage of the development of an EU aviation security risk assessment. Furthermore, improved information exchange with Europol and Eurojust would facilitate both prevention and subsequent prosecution of terrorist activity.

Way forward in 2012

The Commission will:

- **organise a high level conference on countering violent extremism, with the support of the EU Radicalisation Awareness Network;**
- **prepare a set of proposals addressing the use of internet by terrorists, exploring means to counteract radicalisation online;**
- **propose a legislative instrument on freezing of assets to combat terrorism and related activities;**
- **review the Directive on the designation of European Critical Infrastructure Protection;**
- **present a mid-term report on the implementation of the EU CBRN Action Plan and a review of the EU Explosives Action Plan; and**
- **propose options for the establishment of an EU terrorist Finance Tracking System based on discussions with the Council and the European Parliament; and**
- **propose options for further strengthening transport security, focusing in particular on land transport issues.**

Member States are encouraged to:

- **implement the Action Plan on air cargo security; and**
- **enhance efforts to counter violent extremism.**

3. Cybercrime and cyber security

The EU is a key target for cybercrime notably because of its advanced internet infrastructure, widespread usage and increasingly internet-mediated economies and payment systems. As a consequence of the pace and sophistication of technological development, cybercrime is constantly evolving. New technology trends, such as the growth of cloud computing and increased use of mobile devices, give rise to additional threats to users and compound the challenges faced by law enforcement.[9] The widespread usage of internet technology in the EU has also prompted an unprecedented expansion in the markets for child abuse material and intellectual property theft.

The internet knows no boundaries, but jurisdiction for prosecuting cybercrime still stops at national borders. Member States need to pool their efforts at EU level in order to put in place a common response. This would also entail more extensive use of existing capabilities of EU agencies. Cooperation with international partners will also reinforce the EU's ability to tackle cyber crime.

In 2011 achievements have been made to prepare the ground for the European Cyber Crime Centre as well as for supporting the Member States in setting up National/Governmental Computer Emergency Response Teams. The EU/US working group on cyber has been successful in delivering results, from cooperation on combating child pornography to joint exercises on how to prevent cyber attacks.

[9] See Europol: Threat Assessment on Internet Facilitated Organised Crime (iOCTA) 2011.

Way forward in 2012

The Commission will:

- **develop an overarching European strategy for internet security;**
- **make all arrangements for the configuration of the European Cybercrime Centre to be set up by 2013; and**
- **build on the work done by the EU/US working group on cyber-security and cybercrime, and initiate cooperation with other international partners.**

Member States are encouraged to:

- **implement the actions in the EU Policy Cycle;**
- **continue with efforts to develop national cybercrime awareness and training capabilities and set up centres of excellence;**
- **ratify the Council of Europe Convention on Cybercrime;**[10]
- **establish National/Governmental Computer Emergency Response Teams (CERTs) and create a well-functioning network;**
- **And improve reporting systems for cybercrime.**

4. Border management

Over the course of 2011, Member States and Frontex have had to step up their efforts to counter increasing pressure on the EU's external borders. Since the deployment of 'Operation Hera' from 2006, Frontex has succeeded in closing the irregular migration route from West Africa to the Canary Islands. There continues to be large-scale smuggling along the EU's Eastern border. However, the Commission this year presented a range of actions to be taken to tackle this.[11] The Mediterranean sea border and the land border with Turkey are currently, and are likely to continue to be, key points for irregular border crossings into the EU.

Following recent events in North Africa, over 50,000 migrants entered the EU across the Mediterranean sea border, often facilitated by criminal networks. The deployment of Frontex's 'Joint Operation Hermes' in February 2011 was instrumental in patrolling this route. Equally, Frontex's Rapid Border Intervention Team (RABIT), which for the first time ever provided border management support at the Greece-Turkey land border contributed to a reduction of 75% in the number of irregular crossings during its deployment.

In January 2011, the Commission presented the framework of the European Border Surveillance System (EUROSUR). A pilot project has been launched at the external land/sea border by FRONTEX in cooperation with six Member States. This has informed the Commission's legislative proposal on EUROSUR to be presented in December 2011, with a view to it becoming operational in 2013.

---

[10] Austria, Belgium, Czech Republic, Greece, Ireland, Luxembourg, Malta, Poland and Sweden have not yet ratified the convention.

[11] http://ec.europa.eu/anti_fraud/documents/Working-paper.pdf

Management of external borders must both enhance security and facilitate travel. With these objectives in mind, in 2011 the Commission has presented proposals for an improved Schengen evaluation and monitoring system, and an analysis of the potential establishment of Entry/Exit and Registered Traveller systems as called for by the European Council.

Way forward in 2012

The Commission will:

- **present proposals based on the outcome of the discussions on the Smart Borders Communication (Entry/Exit System and Registered Traveller Programme); and**
- **make suggestions for improvements to coordination of border checks carried out by different national authorities (police, border guards, and customs).**

Member States are encouraged to:

- **implement the actions foreseen within the EU Policy Cycle;**
- **continue their efforts with regard to the establishment of EUROSUR; and**
- **actively participate in migration, mobility and security dialogues with the new governments of North Africa and the Middle East.**

5. Crisis and disaster management

In recent years, European citizens have experienced various disasters, whether natural or manmade. The threat of malicious acts, like terrorist and cyber attacks, and hostile or accidental releases of disease agents and pathogens, remains. The earthquake in Aquila/Italy, the ash cloud crisis deriving from a volcano eruption in Iceland and the July terrorist attack in Norway reinforce the need for the EU to enhance its crisis and disaster management capacity. Moreover, the Fukushima incident highlighted not only the potential of a causal chain of events - from earthquake to tsunami to nuclear crisis – but also the global impact of these events, for example, on international transport, customs and food safety, which require complex risk management solutions.

The complexity and scope of these challenges require a comprehensive approach to the assessment of risks, preparation of forecasts, and prevention, preparedness and mitigation. This requires the joining up of the different policies, instruments and services available to the EU and Member States.

Through Europol, Frontex, the EU Joint Situation Centre (SitCen), and the European Commission's Monitoring and Information Centre, the EU is able to draw on certain capacity and expertise in information gathering, analysis, threat assessment and emergency response in the different areas of internal security. However, one of the main challenges for the coming years will be to move gradually towards a coherent risk management policy, linking threat and risk assessment to policy formulation and implementation. Over 2011 initial steps have been made in this direction.

Way forward in 2012

The Commission will:

- **contribute to the further development of an EU threat and risk assessment policy, and prepare an overview of the major natural and man-made risks the EU may face in the future;**
- **further develop its strategic assessment capacity, notably by bringing together the existing expertise of the different actors (Europol, Frontex, and SitCen) in the area of internal security; and**
- **present a joint proposal on the implementation of the solidarity clause with the High Representative for Foreign Affairs and Security Policy.**

Member States are encouraged to:

- **develop regular threat and risk assessments; and**
- **support efforts to increase the European response capacity to disasters.**

III. Conclusion

This report on the Internal Security of the EU highlights some of the issues that need to be considered further by the European Parliament, Member States, the Commission and society in general.

The threats highlighted in the ISS in Action of November 2010 are of no less significance in 2011 and should continue to be the focus of the EU's actions on internal security.

Considerable progress has been achieved in the **fight against organised crime**, in particular with the proposal for EU legislation on the collection of Passenger Name Records on flights entering or leaving the territory of the EU, and the package on anti-corruption. Further progress needs to be made on judicial and law enforcement cooperation, and on the development of the administrative approach in combating serious crime.

As regards **terrorism and radicalisation**, achievements include, in particular, the establishment of the European Radicalisation Awareness Network. The adoption of a Communication on an EU Terrorist Financing Tracking System is also an important step forward. However, increased efforts are needed in relation to a framework for administrative measures on the freezing of terrorist assets and the improvement of land transport security.

Actions to combat **cybercrime** are developing well. Progress has been made towards establishing the European Cybercrime Centre and the establishment of Computer Emergency Response Teams. Several Member States need to take urgent action to ratify the Budapest Convention.

In the area of **border management**, the establishment of EUROSUR is on track, but further discussion on the Smart Borders proposals and further work to improve interagency cooperation at national level is needed.

Actions related to **crisis and disaster management** have also been taken forward. Work was undertaken in 2011, for example, in the field of risk assessment. However, in the area of crisis management, additional effort is needed if we are to reach our objective. Full commitment and cooperation between Member States, the Commission and the EEAS is essential.

Advanced work has been done to bridge the gap between internal and external security. Several initiatives to foster cooperation and coordination have been developed: this includes practical cooperation on terrorism, trans-national crime and irregular migration in the Western Balkans, the Horn of Africa and the Sahel. Furthermore, the EEAS and the Commission developed a Joint Paper on enhancing ties between the Common Security and Defence Policy (CSDP) and Freedom, Security and Justice (JHA) actors; including possibilities for cooperation between the CSDP police missions and Europol.

Finally, the success of any strategy depends on its ability to deliver concrete results. For the ISS in Action, 2011 has been a promising start. But three years remain and there is still much work to be done to ensure the security of the European citizen. For the next Annual Report, progress in all priorities is needed, but in particular in the fight against serious and organised crime, as well as countering the growing cyber threat.

Annex

Implementation of the five ISS objectives in 2011

This annex gives an update on the implementation of the five priorities of the Internal Security Strategy in Action, with information on the key deliverables from 2011 and a table illustrating the state of play for the measures foreseen under each objective.

Since the adoption of the ISS in Action in 2010, the EU 'Harmony' Policy Cycle on Organised Crime 2011-2013 has also been adopted by the Council. This consists of eight priorities which focus on tackling serious and organised crime, cybercrime and strengthening border management.[12] This methodology is an important step in translating the political priorities and strategy of the ISS into operations that deliver collective concrete results for internal security.

Objective 1 — Disrupt international crime networks

EU Passenger Name Records (PNR)

In February 2011 the Commission proposed EU legislation on the collection of Passenger Name Records on flights entering or leaving the territory of the EU. Its aim is to enable the competent authorities in Member States to analyse the data in order to prevent, detect and prosecute terrorist offences and serious crimes. This proposal is currently being discussed by the European Parliament and the Council. The proposal is part of a wider PNR policy that includes the conclusion of PNR agreements with third countries. Such agreements allow the use of PNR data originating from the EU by law enforcement authorities of these countries for the same purpose. The agreements in place with Canada and the US are currently under renegotiation, while a new agreement with Australia was signed in September 2011.

[12] The EU Harmony Policy Cycle, covers the following eight priorities:
1. Weaken the capacity of organised crime groups active or based in West Africa to traffic cocaine and heroin to and within the EU;
2. Mitigate the role of the Western Balkans, as a key transit and storage zone for illicit commodities destined for the EU and logistical centre for organised crime groups, including Albanian-speaking organised crime groups;
3. Weaken the capacity of organised crime groups to facilitate illegal immigration to the EU, particularly via southern, south-eastern and eastern Europe and notably at the Greek-Turkish border and in crisis areas of the Mediterranean close to North Africa;
4. Reduce the production and distribution in the EU of synthetic drugs, including new psychoactive substances;
5. Disrupt the trafficking to the EU, particularly in container form, of illicit commodities, including cocaine, heroin, cannabis, counterfeit goods and cigarettes;
6. Combat against all forms of trafficking in human beings and human smuggling by targeting the organised crime groups conducting such criminal activities in particular at the southern, south-western and south-eastern criminal hubs in the EU;
7. Reduce the general capabilities of mobile (itinerant) organised crime groups to engage in criminal activities;
8. Step up the fight against cybercrime and the criminal misuse of the internet by organised crime groups.

In the 2012 Annual Work Programme[13] of the Prevention of and Fight against Crime Programme (ISEC) the Commission has included EUR 25 million in funding opportunities for the setting up of PNR units in Member States.

Joint Investigation Teams

In order to support the setting up of Joint Investigation Teams (JITs) - in particular at short notice - and to have a positive practical impact on the fight against cross-border crime, the Commission has provided a second round of funding, worth EUR 2.1 million, to the Eurojust JIT project 'Supporting Greater Usage of Joint Investigation Teams'. The project supports the creation of new and existing JITs by improving their access to financial assistance in the coming years. In the first year, Eurojust's current project has supported 33 JITs, investigating crimes such as drug trafficking, human trafficking, irregular immigration, vehicle crime, cybercrime and financial crime. Europol has also contributed to the setting up and work of JITs with its fast and secure communication and information exchange network, logistical and forensic support and analysis capabilities.

Example 1:
Eurojust, among others, supported a successful joint investigation team established between Germany and Romania, investigating activities of an organised criminal group involved in human trafficking. As a result of this investigation, 50 perpetrators have been accused of trafficking in human beings and related crimes, 6 offenders have been so far sentenced, 148 witnesses have been interviewed and EUR 860.000 has been seized (cash and property). Under the JIT funding project, Eurojust assisted with travel and accommodation costs of JIT members which enabled direct communication and realisation of the aforementioned joint investigative actions. Financial support was also provided for translation of investigative materials.

Example 2:
A multilateral JIT coordinated at Eurojust was vital to the successful investigation and prosecution of large-scale cocaine trafficking from South America to Europe. The JIT agreement was signed for an initial period of six months, but extended several times to allow uninterrupted work for more than two years. Investigating and judicial authorities in the JIT met regularly to decide on common strategies, and exchanged information and evidence without the delay associated with traditional mutual legal assistance requests. Prosecutors and law enforcement authorities from country X were present during the hearings of suspects in country Y. Appointment of JIT leaders with the power to head the entire JIT when operating in their own countries facilitated rapid execution of law enforcement and judicial cooperation measures in different jurisdictions. Eurojust co-ordinated the JIT's work at meetings in The Hague, with Europol's active involvement and analytical contribution. JIT funding from Eurojust was used to assist with costs such as interpretation, translation of documents, travel and accommodation. Eurojust also provided devices to permit secure communication between JIT members. The JIT contributed to the arrest of some 30 leading suspects around the world, the seizure of more than 1000 kg of cocaine and of assets valued in millions of euros.

[13] C (2011) 6306 final; adopted on 19 September 2011.

Since February 2011, the Secretariat of the Network for Joint Investigation Teams has been operational within Eurojust,[14] with a view to raising awareness, solving problems and exchanging best practices among practitioners. Provisions in the revised Eurojust Decision which make Community funding of JITs conditional on inviting Eurojust to participate (Article 9f) and which ensure that Member States notify Eurojust when setting up a JIT (Article 13.5) will help provide a more accurate overview of all the existing JITs in the EU.

Combating corruption

Corruption has long been seen as a primarily national problem. Over time, however, it has become clear that it also has cross-border effects and cannot be combated successfully in isolation. Cross border organised crime is frequently reverting to bribery in order to facilitate the infiltration of the legal system. The necessary laws and institutions to address corruption are largely in place, but the implementation of anti-corruption policies remains uneven across the EU. The Stockholm Programme calls on the Commission to develop indicators to measure the Member States' efforts to combat corruption.

In June 2011 the Commission adopted an anti-corruption package which set up an EU reporting mechanism ('EU Anti-Corruption Report') for the periodic assessment of the Member States' efforts against corruption. The EU Anti-Corruption Report will assess Member States' achievements, failures and vulnerabilities, with a view to generating additional political will to implement genuine zero-tolerance approaches to corruption, encourage peer learning and facilitate the exchange of best practices. The Commission will publish the report every two years, starting in 2013. It will focus on cross-cutting issues, identify EU trends and provide country specific analyses and recommendations.

As part of the anti-corruption package, a Commission report on European Union participation in the Council of Europe Group of States against Corruption (GRECO) analyses various ways to strengthen cooperation between the EU and GRECO, concluding that EU membership in GRECO is the appropriate way forward to meet the objectives of the Stockholm Programme. Based on these findings, the Commission will request authorisation from the Council to open negotiations for participation in GRECO. This would create synergies between the GRECO evaluation system and the EU Anti-Corruption Report, and would ensure a coherent approach against corruption at European level.

With the financial support of the Programme 'Prevention and Fight against Crime (ISEC)', Transparency International has carried out comparative research across the European Union to assess the relevance of statutes of limitations in the fight against corruption (project ended in March 2011). To identify both weaknesses and best practices in statutes of limitations, the research examines the situation in 27 EU countries (in-depth analyses for 11 Member States and general overview of the state of play for the other 16). Based on the results of the research, Transparency International will call for the adoption, where necessary, of the best practices identified[15].

[14] Council Decision 2002/187/JHA of 28 February 2002 setting up Eurojust with a view to reinforcing the fight against serious crime as amended by Council Decision 2003/659/JHA and by Council Decision 2009/426/ JHA of 16 December 2008 on the strengthening of Eurojust.

[15] Countdown to Impunity: Corruption-related Statutes of Limitation in the European Union (EU) — JLS/2008/ISEC/100.

Confiscation and recovery of criminal assets

In order to recover criminal assets, the Commission will propose legislation[16] to strengthen the EU legal framework[17] on the confiscation and recovery of criminal assets in the European Union and on strengthening the mutual recognition of freezing and confiscation in the area of serious crime.

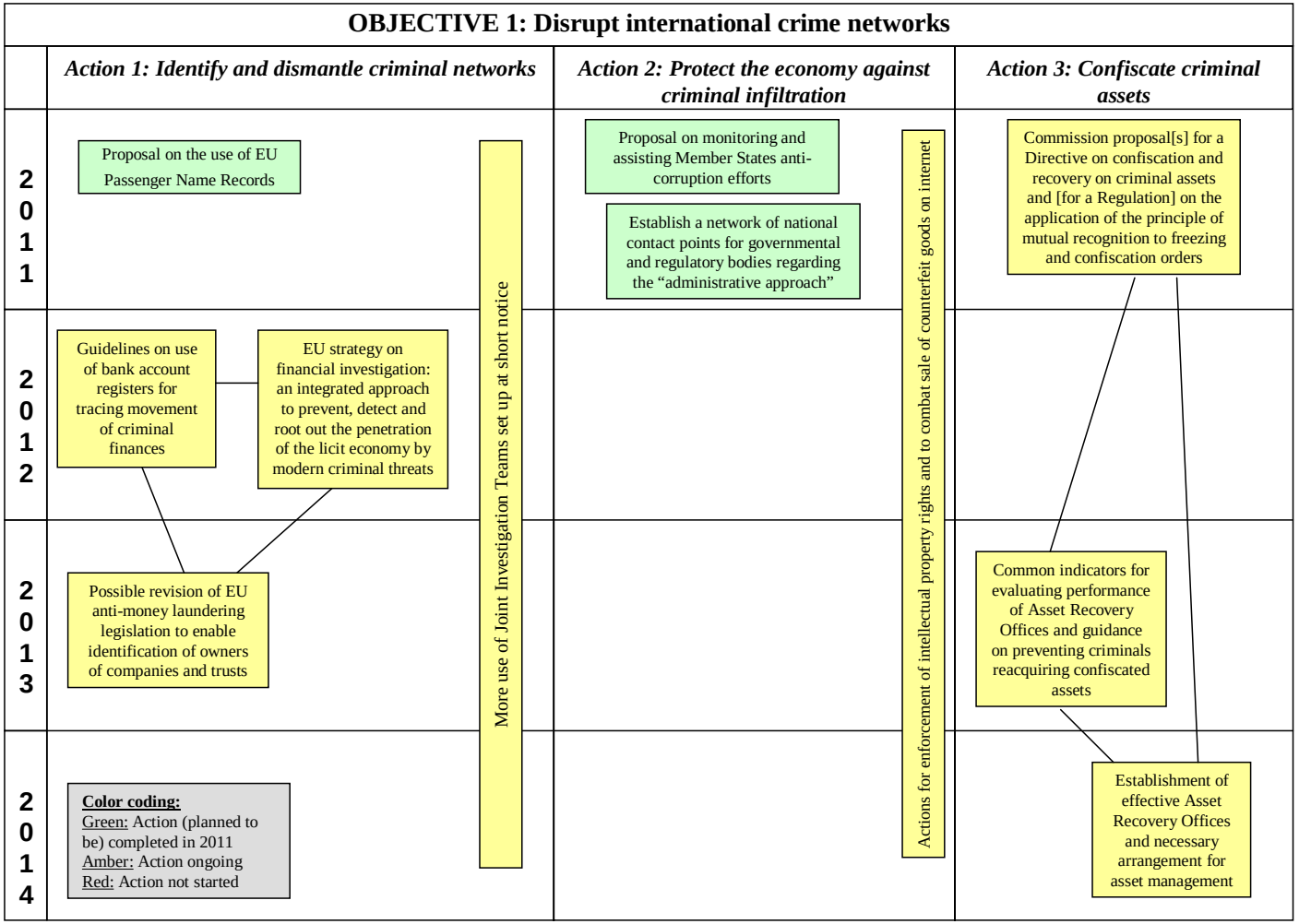
With the help of ISEC, the EU has assisted Member States in setting up and strengthening asset recovery offices. For example, an ISEC project resulted in 2010 in the setting up of the Hungarian Asset Recovery Office, including the development of new working methods on the basis of best practice in other Member States[18]. This and other ongoing projects aimed at fostering the exchange of best practices between asset recovery offices (e.g. CEART, FENIX) are regularly presented to practitioners at the meetings of the EU ARO Platform.

16 Adoption foreseen in 2012.

17 Framework Decisions 2001/500/JHA on money laundering and confiscation, 2005/212/JHA on extended confiscation, 2003/577/JHA and 2006/783/JHA, respectively on the mutual recognition of freezing and confiscation orders. .

18 Development of investigation methods and techniques in the field of asset recovery — JLS/2008/ISEC/FPA/C1/018.

Progress report overview table of all ISS objectives and actions



Objective 2 — Prevent terrorism and address radicalisation and recruitment

EU radicalisation-awareness network

The Commission has established the European Radicalisation Awareness Network (RAN), in partnership with the Committee of the Regions. The RAN was inaugurated on 9 September 2011 by Commissioner Cecilia Malmström. The RAN is an EU-wide umbrella network of practitioners involved in countering violent extremism and includes policy makers, law enforcement and security officials, local authorities, academics, field experts and civil society organisations, including victim groups. The main objectives of the network are to pool experience, knowledge and good practices and, in particular, to:

- Enable communication and networking among the RAN members in order to enhance awareness of radicalisation and improve communication techniques for challenging terrorist narratives;
- Identify, test, assess and compare approaches and lessons learnt in countering violent extremism; and
- Inform policy makers both at the EU and Member States' level and act as a communication channel between the Commission and the front-line practitioners.

Through ISEC the Commission supported the work of civil society and public organisations which expose, translate and challenge terrorist propaganda including its manifestations on the internet.

To strengthen operational cooperation to counter terrorist activities on the internet, the Commission funded a number of projects, such as the German-led multilateral project entitled 'Exploring the Islamist extremist Web of Europe' which focuses on terrorist content aimed at young Europeans.

Moreover ISEC funding was also used to fund a public private dialogue to develop a voluntary European Code of Conduct on good practices for cooperation between Law Enforcement Authorities and the private sector including internet service providers, as well as network operators and complaint hotlines.

The Commission also used ISEC funding to support policy-makers and enhance the capabilities of EU law enforcement authorities by a number of studies, including one on methodologies and technological tools to effectively detect violent content on the internet and to trace its authors, which is expected to be delivered by end of 2011 and will help in investigating and prosecuting those responsible for illegal material.

Extraction and analysis of financial messaging data (EU TFTS)

The EU signed the Terrorist Financing Tracking Programme agreement with the United States (US TFTP), which provides the legal framework for the transfer of EU financial messaging data from the EU to the US for counter-terrorism purposes. A review in March 2011

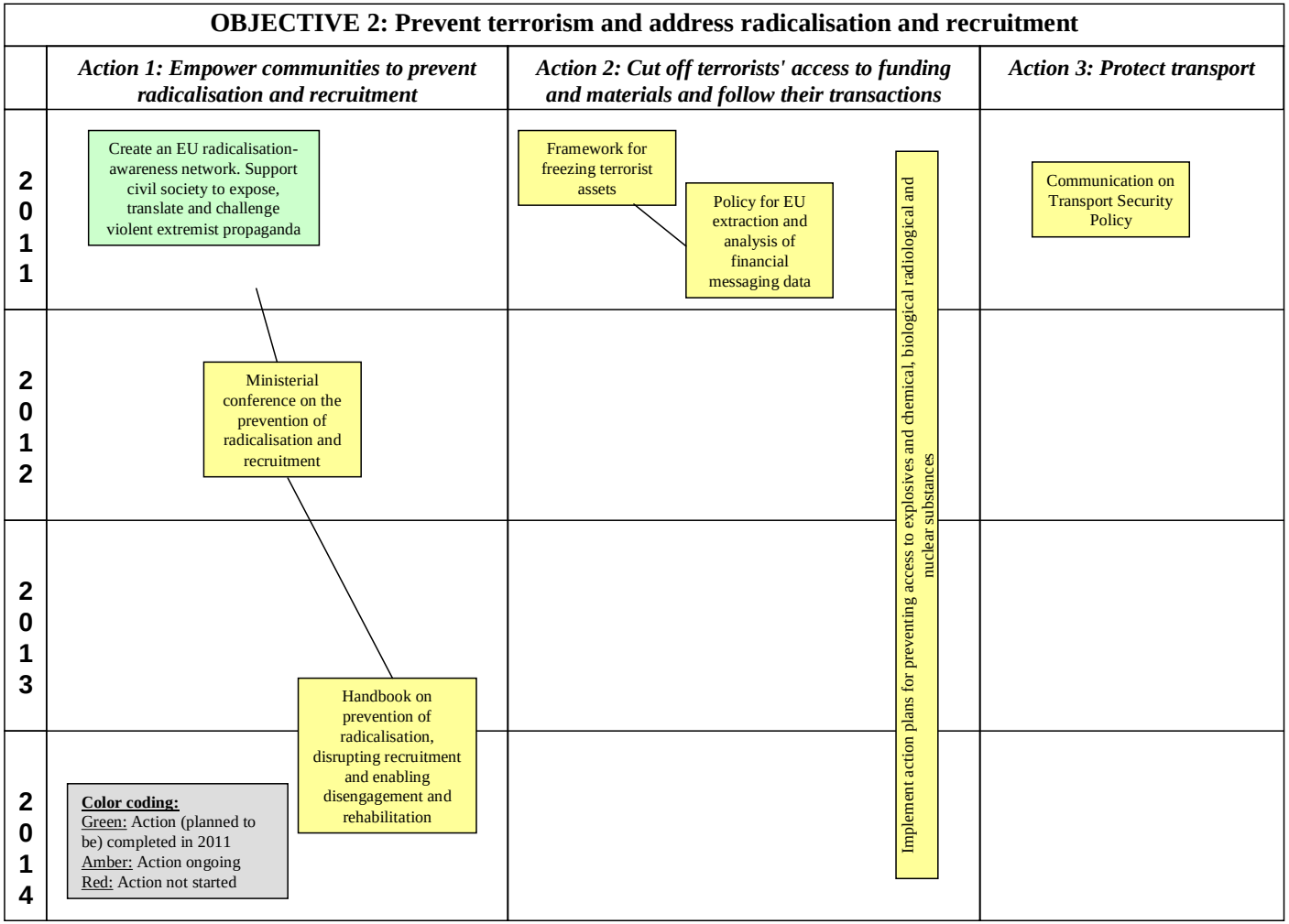
demonstrated its effectiveness in the fight against terrorism. A Communication on an EU Terrorist Financing Tracking System (TFTS) was also adopted in July 2011, which outlined the main options available for establishing such a system, and pointed to the major issues which still need to be resolved before a system could be formally proposed. The Communication is intended to stimulate debate with the European Parliament and the Council, and the Commission will await the outcome of these discussions before presenting a legislative proposal.

Transport Security

The maritime and aviation sectors have already demonstrated the added value that appropriate communication and coordination mechanisms, as well as common rules on security can bring at EU level, given the cross-border nature of the transport industry. The Commission's forthcoming Communication on transport security will focus largely on developing an equivalent EU approach to land transport security. It will also focus on the need for transport to have appropriate systems in place – preventative measures, contingency planning to deal with security incidents, recovery plans, training, etc. Its emphasis will be on setting security outcomes, rather than prescriptive security requirements for transport.

To facilitate policy development in this area an Advisory Group on Land Transport Security will be established in 2012. Priority issues for their consideration will include the need for EU-wide security standards to be set for the high-speed rail network.

Progress report - overview table of all ISS objectives and actions



Objective 3 — Raise levels of security for citizens and businesses in cyberspace

European Cybercrime Center

The Commission ordered a feasibility study on the questions of where and how to set up the European Cybercrime Centre (ECC), planned as the future focal point in the fight against cybercrime at a European level. This study, launched in May 2011, will produce its initial results by the end of this year. Final results with recommendations will be available at the beginning of 2012. Pending the recommendations that the study will produce, Europol decided in June 2011 to regroup its cybercrime competence and has redeployed resources to deal with this rapidly expanding crime phenomenon.

ISEC funds various training projects for law enforcement bodies to investigate cybercrime. For example, an ISEC project which finished in early 2011, developed and delivered training courses relating to internet and forensic investigations. The training was intended for the staff of various law enforcement services and of European and international bodies. A particular focus was put on developing closer cooperation with the private sector. Partners from all EU Member States and Europol participated in the project.[19].

At national level, the Commission supported financially the development of national cybercrime awareness and training capabilities, including centres of excellence. The year 2011 saw the start of four such centres: 2CENTRE (France and Ireland), B-CCENTRE (Belgium) and 2CENTRE EST (Estonia).

Computer Emergency Response Teams (CERTs)

In March 2011, the Commission adopted a Communication on Critical Information Infrastructure Protection (CIIP)[20] which took stock of the implementation of the 2009 CIIP Action Plan[21] and described the next steps for action at both European and international level. In May 2011, the Telecom Council adopted related conclusions. A number of areas where greater efforts were needed to strengthen national cyber-security capabilities were identified, in particular regarding: the establishment of national/governmental CERTs and the creation of a well-functioning network of national/governmental CERTs in Europe by 2012; the development of national cyber incident contingency plans and of a European cyber incident contingency plan; and the organisation of regular national and pan-European cyber incident exercises. The EU institutions made progress towards establishing their own CERT by setting up a CERT Pre-configuration team on 1 June 2011. It will be assessed within 12 months, leading to decision on the conditions for establishing a CERT for the EU institutions.

---

19 Title and Reference: Cybercrime Investigation — Developing and disseminating an accredited international training programme for the future — JLS/2008/ISEC/FP/C4-077.

20 COM(2011) 163, Commission Communication on Critical Information Infrastructure Protection 'Achievements and next steps: towards global cyber-security'.

21 COM(2009) 149, Commission Communication on Critical Information Infrastructure Protection 'Protecting Europe from large scale cyber-attacks and disruptions: enhancing preparedness, security and resilience'.

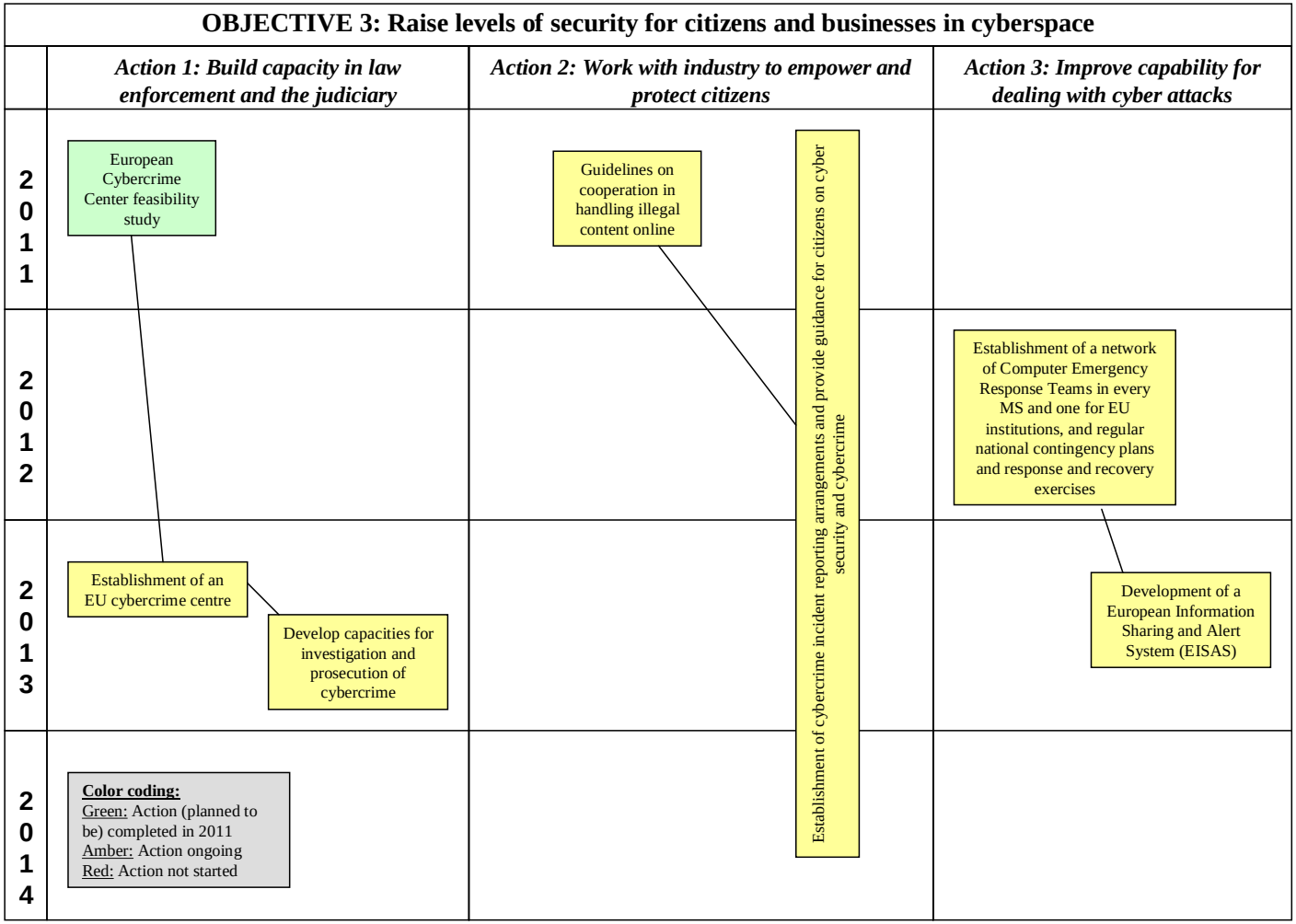
EU/US Working Group on cyber security and cybercrime

In addition to the specific steps outlined above, the Commission continued its close collaboration within the strategic partnership in the EU/US Working Group on cyber-security and cybercrime, working on protecting crucial internet resources from abuse and preventing and prosecuting online child sexual abuse.

Internet behaviour

Together with the European External Action Service the Commission is working on shaping a European position in relation to recent initiatives on recommended internet behaviour and on enabling third countries to develop cybercrime legislation, set up investigation capacities and improve network resilience based on the provisions of the Budapest Convention against cybercrime.

Progress report - overview table of all ISS objectives and actions



Objective 4 — Strengthen security through border management

Establishment of EUROSUR

During 2011 significant progress has been made in further developing and implementing EUROSUR. In January 2011 the Commission presented the technical and operational framework of EUROSUR and identified the actions to be taken in order to make EUROSUR operational by 2013[22]. Accordingly, 16 out of the 18 Member States located at the southern maritime and eastern land borders of the EU have established their national coordination centres in the course of 2011. In parallel, Frontex is setting up the EUROSUR network, which will enable the national coordination centres and Frontex to exchange information with each other in a secure manner. After successful testing between Frontex and the Polish national coordination centre during the summer, Frontex will have extended the EUROSUR network to another five Member States by November 2011. The Commission is currently finalising its work on the legislative proposal for EUROSUR, which will be presented to the Council in mid-December 2011.

In the context of EUROSUR and in close cooperation with COSI, several southern Member States started preparing the establishment of the regional network 'SEAHORSE Mediterraneo' with selected neighbouring African countries. In parallel, Frontex, the European Maritime Safety Agency (EMSA) and the EU Satellite Centre (EUSC) jointly elaborated a concept of operations for the common application of satellites, ship reporting systems and other surveillance tools. Selected applications of this envisaged interagency cooperation have been tested during 2011 between Frontex, EMSA, EUROPOL and CeCLAD-M[23] in the Western Mediterranean as part of the Frontex Joint Operation Indalo. Finally, progress has been made in further developing the common information sharing environment (CISE) for the EU maritime domain.

Establishment of the Visa Information System (VIS)

Significant progress was achieved in the finalisation of the VIS development in 2011. The last two testing phases of the Central VIS were performed with the participation of Member States. The so-called Operational System Tests and Provisional System Acceptance Tests were successfully completed in the second and third quarter of 2011 respectively. Following the completion of these comprehensive tests, and after receiving notifications of readiness by all Member States participating in VIS, VIS began on 11 October 2011 in the first rollout region (North Africa). Subsequent regions for the gradual deployment of the system will follow in the course of the coming months and years. The operational management of the VIS will be entrusted to C-SIS, the authority responsible for the operational management of SIS 1.

---

22 Commission staff working paper determining the technical and operational framework of EUROSUR and the actions to be taken for its establishment, SEC(2011) 145final of 28.1.2011. See also COM(2008) 68final of 13.2.2008 and SEC(2009) 1265final of 24.9.2009.

23 Centre de Coordination pour la lutte antidrogue en Méditerranée.

Common risk management for movement of goods across borders

The EU wide implementation of the Security Amendment of the Customs Code and the Common Customs Risk Management Framework (CRMF) was completed on 1 January 2011, including systematic electronic submission of pre-arrival and pre-departure declarations by trade, electronic risk analysis by EU customs, exchange of messages through the Common Customs Risk Management System (CRMS) and the Authorised Economic Operator (AEO) programme. This full implementation lays the foundation for initiatives to improve capabilities for risk analysis and targeting.

Progress report - overview table of all ISS objectives and actions

OBJECTIVE 4: Strengthen security through border management

	Action 1: Exploit the full potential of EUROSUR	*Action 2: Enhancing the contribution of Frontex at the external borders*	*Action 3: Common risk management for movement of goods across external borders*	*Action 4: Improve interagency cooperation at national level*
2011	Proposal for the establishment of EUROSUR Pilot operational project at the southern or south-western border of the EU	Joint reports on human trafficking, human smuggling and smuggling of illicit goods as basis for joint operations	Initiatives to improve capabilities for risk analysis and targeting	Development of national common risk analyses involving police, border guards and customs authorities to identify hot spots at the external borders
2012				Suggestions for improving the coordination of checks at the border carried out by different authorities
2013				
2014	**Color coding:** Green: Action (planned to be) completed in 2011 Amber: Action ongoing Red: Action not started			Development of minimum standards and best practices for interagency cooperation

Objective 5 — Increase Europe's resilience to crises and disasters

Implementation of the solidarity clause

By implementing the solidarity clause, the EU is seeking to give tangible expression to the principle of solidarity laid down in the Lisbon Treaty (Art. 222). Work has begun on the solidarity clause.

Risk assessment and mapping guidelines for disaster management and national approaches to risk management

In view of the planned establishment of a coherent risk management policy, linking threat and risk assessments to decision making, the Commission, together with Member States, has developed EU risk assessment and mapping guidelines for disaster management[24], based on a multi-hazard and multi-risk approach, covering in principle all natural and man-made disasters, including the consequences of terrorist acts. By the end of 2011, Member States should have developed national approaches to risk management, including risk analyses.

Health threats

The European Commission is developing an initiative on health security in the European Union in order to better protect citizens' health against serious cross-border threats. The prevention and control of threats from communicable diseases at EU level are already being addressed under the legislation adopted in 1998, which provides a basis for epidemiological surveillance and coordination of the response. This system has proved effective for more than a decade. However, there is no such legislation in place on health threats from chemical and biological agents other than communicable diseases or environmental events. The aim of this initiative is, therefore, to consider the possibility and need to ensure that all types of public health threats are addressed in a similar manner to communicable diseases. As part of the impact assessment process, the Commission has launched a stakeholders' consultation aimed at the public health community in the Member States. The outcomes of the consultation will support the preparation of a legislative initiative to be submitted by the end of 2011[25].

Protection of classified information

The EU should develop an integrated approach based on common and shared appreciations of crisis situations. Certain EU agencies are key actors in this process and the possibility to share classified information at the appropriate level is a precondition for better information sharing and, where required, for preparing joint EU threat and risk assessment reports. Effective coordination between the EU institutions, bodies and EU agencies requires a coherent general framework to protect classified information. The Commission is working on developing a coherent general framework for the exchange of classified information with the EU agencies, ensuring that Classified Information is granted equivalent protection as in the other EU Institutions and Member States.

---

[24] Commission Staff Working Paper on Risk Assessment and Mapping Guidelines for Disaster Management, SEC(2010) 1626final of 21.12.2010.

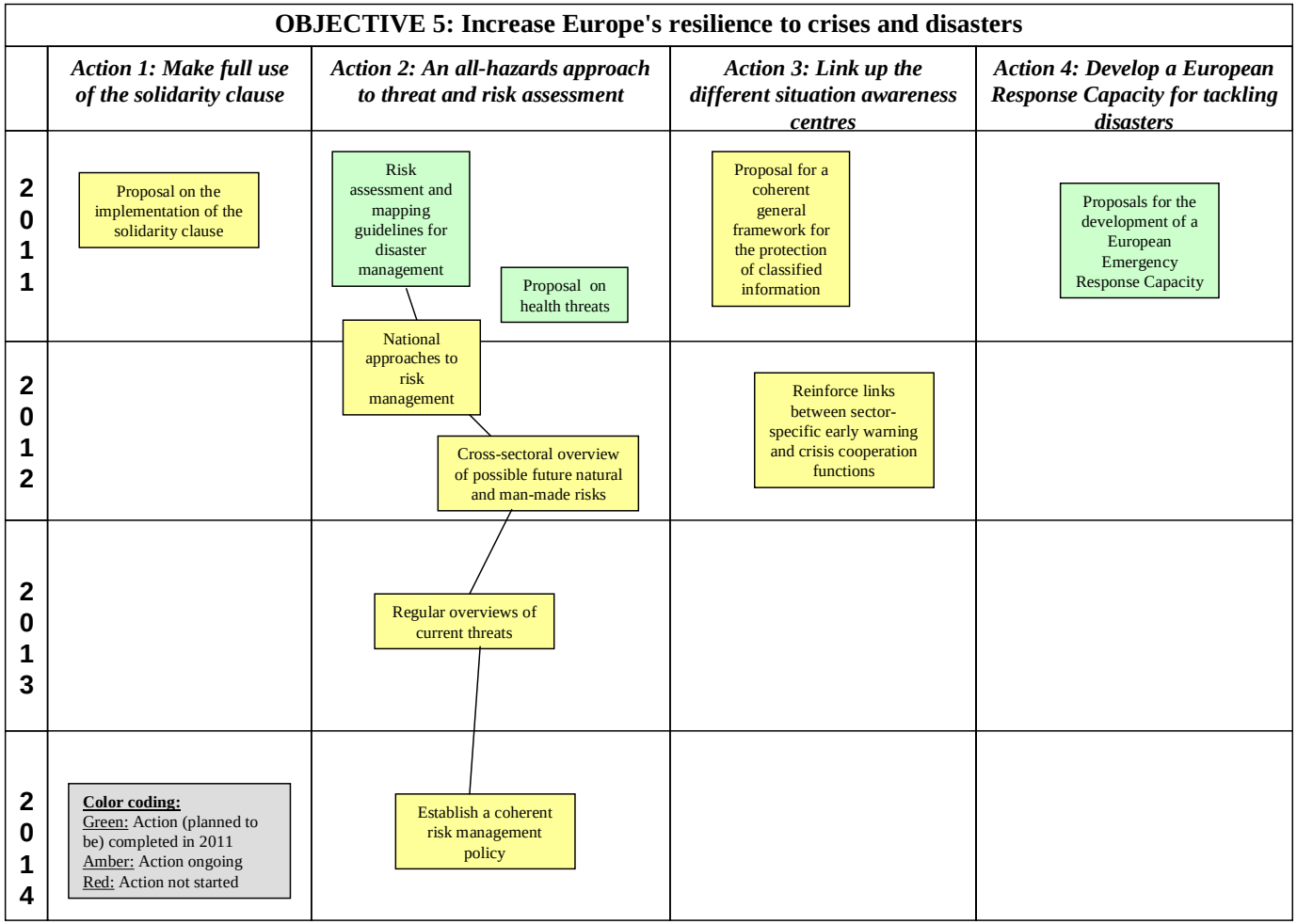
[25] Adoption foreseen on 07 December 2011.

European Emergency Response Capacity

The Commission has tabled a proposal establishing a European Emergency Response Capacity[26] based on pre-committed Member States' assets on-call for EU operations and pre-agreed contingency plans. The EU needs to move from ad hoc coordination towards a system that is pre-planned, pre-arranged and predictable. This would make the EU's disaster response more effective, efficient, coherent and visible. This will be achieved by means of a number of actions, including regular risk assessments, developing reference scenarios, mapping of assets and contingency planning, the establishment of a European Emergency Response Capacity in the form of a voluntary pool of Participating States' assets committed to the EU operations which would further contribute to both the planning and the availability of assets for a European emergency response. An impact assessment exercise (including a stakeholders consultation) has been launched in order to support the Commission's proposal to renew the EU civil protection legislation by end of 2011.

[26] Commission Communication 'Towards a stronger European disaster response: the role of civil protection and humanitarian assistance', 26.10.2010, COM(2010) 600final.

Progress report - overview table of all ISS objectives and actions



Cross-cutting issues

Coherence between the internal and external dimensions of security

A series of initiatives aimed at fostering cooperation between the internal and external aspects of security are currently being developed. To ensure closer cooperation and coordination in the field of EU security, regular inter-institutional information meetings will be convened to improve planning and information flow in the area of EU security. The first such meeting between COSI and the Political and Security Committee was held on 1 June 2011 in order to exchange views on how to improve the synergy between the internal and external aspects of EU security. In addition, the EEAS and the Commission drew up a Joint Paper on enhancing ties between the Common Security and Defence Policy (CSDP) and the Freedom, Security and Justice (JHA) actors, which supports the idea that closer cooperation between civilian CSDP missions and JHA actors could yield tangible improvements in terms of European security. The specific recommendations in the Joint Paper single out sharing of information as being important and needing improvement in order to find ways of anticipating rather than reacting to events. Secondly, coordination in planning EU external action needs to be fostered, as it is essential for cooperating upstream in the planning of the missions.

Another area where tangible results can be achieved is the cooperation between the CSDP police missions and Europol. The Council has acknowledged on many occasions that CSDP[27] and many JHA external actions have had shared or complementary objectives. CSDP missions have also made an important contribution to the EU's internal security in their efforts to support the fight against serious transnational crime in their host countries and to build respect for the rule of law. The European Council encouraged greater cooperation between JHA and CSDP in developing these shared objectives. Also the Stockholm Programme, as adopted by the European Council, states that Europol should work more closely with the CSDP police missions and help promote standards and good practice for European law enforcement cooperation in countries outside the EU.

It is of particular interest for the JHA area to make sure that it is closely associated from the very start of the process, especially in the identification and assessment of the need for EU action in a crisis situation. This will enable a proper and timely evaluation of the necessary expertise, taking the organised crime situation in the respective third country or region into account. This will also help improve political and operational decisions and the definition of tasks which will subsequently be implemented by the civilian police mission. Europol's analytical capacities, and its Secure Information Exchange Network Application (SIENA) for information exchange which connects all 27 EU Member States' law enforcement authorities, can help CSDP missions to adjust their methods and refine their objectives in the light of the pan-European picture of organised crime provided by Europol through threat assessments and analyses.

A second factor, namely the exchange of information between CSDP police missions and Europol, is an important aspect in the mutual cooperation. The mechanism of cooperation involving the exchange of non personal data is broadly speaking well established via an administrative arrangement between Europol and the Secretariat General of the Council. Therefore, the main issue at stake is how to make possible the direct exchange with Europol

[27] The reference to 'ESDP' (European Security and Defence Policy) now should be read 'CSDP' (Common Security and Defence Policy), following the entry into force of the Lisbon Treaty. .

of personal data collected by or in relation to CSDP police missions. In the case of EULEX Kosovo[28], where the mandate also includes executive tasks, specific arrangements have been put in place to allow the exchange of personal data with Europol. This mechanism could serve as an example of best practice and be applied in other CSDP missions on a case by case basis. The need to establish a data protection framework applicable also to CSDP has to be assessed.

The EU enlargement policy continues to be one of the key elements contributing to the EU internal security. The enlargement process provides for important incentives for relevant countries to deliver on reforms enhancing their law enforcement and judicial capacities. Additionally, the visa liberalisation dialogue and the post-visa liberalisation mechanism have substantially contributed to the implementation of reforms in Western Balkan countries.

The EU also aims to increase the ability of partner countries to play their role in addressing today's key threats to security, peace and stability around the world. For this purpose, the long-term priorities identified in the "Instrument for Stability (IfS)" foresee innovative capacity building that combines financial and technical assistance at national, regional and trans-regional levels. Priority 1 of this instrument is related to the support for international efforts to mitigate chemical, biological, radiological and nuclear (CBRN) risks. The measures financed through IfS target the mitigation of CBRN risks, including proliferation of weapons of mass destruction (WMD), in particular through policies for the effective control of CBRN materials and agents, export controls on dual-use goods, and redirecting former weapons scientists into peaceful research activities. For the 2007-13 period, EUR 300 million have been earmarked for this purpose, and an initiative named CBRN Centres of Excellence has been launched with an allocated budget of nearly EUR 100 million. This initiative aims at developing, at national and regional level, the necessary institutional capacity to fight CBRN risk regardless of its origin: criminal (proliferation, theft, sabotage and illicit trafficking), accidental (industrial catastrophes – such as Bhopal or Fukushima and transport) or natural (mainly pandemics).

Regarding organised crime, terrorism, illicit trafficking in drugs, human beings and arms and threats to critical infrastructure Priority 2 of the Instrument for Stability focuses on capacity building in close consultation with beneficiary countries. Typically, security capacities are strengthened at the national, regional and ultimately trans-regional level. For the 2007-13 period, EUR 118 million was earmarked for these measures.

Financial support

The Commission is eager to ensure that security-related activities, including security research, industrial policy and projects under EU internal security-related funding programmes, are consistent with the strategic objectives of the ISS. EU funding that might be needed for the period 2012-2013 will be made available within the current financial programmes ('Prevention and Fight against Crime (ISEC)' and 'Prevention, Preparedness and Consequence Management of Terrorism and other Security Related Risks (CIPS)'. In that respect, the ISEC Annual Work Programme 2011 reflects the priority areas of the ISS in

[28] Following the Adoption of draft conclusions of the Council of the European Union on possible cooperation mechanisms between civilian ESDP missions and EUROPOL as regards the mutual exchange of information on 17 November 2008, the exchange of personal data has been implemented between EUROPOL and EULEX Kosovo: The personal data is transferred between EULEX (by the EUOCI (European Union Office for Criminal Intelligence) and EUROPOL through EUROPOL National Units (ENUs) located in three MS capitals (FI, SE, UK).

Action. Furthermore, the Commission has conducted an evaluation[29] on the results obtained and the qualitative and quantitative aspects of the Framework Programme 'Security and Safeguarding Liberties (2007-2013)', which consists of the two Programmes ISEC and CIPS.

For the post-2013 period, internal security funding will be examined in the context of a Commission-wide debate on all proposals to be made for that period. As part of that debate, the Commission has proposed the setting up of an Internal Security Fund (ISF) in the next multi-annual financial framework, which reflects the strategic objectives and priorities of the Internal Security Strategy, facilitates the best possible implementation of priority actions by the relevant national authorities and agencies and remains sufficiently flexible to allow for adaptation to new security threats and challenges. The Commission considers that the current gap between research funding and operational funding should be closed by supporting specific testing and validation activities (e.g. of system prototypes) under the proposed ISF. This will enable bringing results from high quality security research more easily into serial application and large-scale operational use by law enforcement authorities.

Security research and cooperation with the private sector

Security research is funded under a specific theme in the Seventh Research Framework Programme (2007-13). The Commission ensures that the overall programming is closely aligned with EU security policies, which also many of the over 200 research projects funded until now in this programme show. The ISS objectives are well reflected in the Security Research Work Programmes for 2011-12. For the Work Programme 2013, which alone will provide around EUR 290 million, an analysis is currently being carried out which will help to identify the most important research gaps and needs, taking into account also the priorities set out in the ISS in Action.

Beyond 2013, security research will continue to be funded by the future multiannual research and innovation instrument ('Horizon 2020'). The Commission proposal for the total budget for research and innovation in the next multi-annual financial framework will increase by 46 %, which should be reflected in the respective share for security research.

In order to better align security-related funds with policies, the Commission has also been stepping up its dialogue with the private sector, in particular with industry. For this purpose it was proposed to establish a regular (annual) public-private high-level roundtable where EU institutions and bodies, Member States, and the private sector can exchange their ideas on how best to make progress with the implementation of the ISS priorities. The first High Level Public–Private Security Roundtable between the EU and Member States' Public Sector and representatives of the private sector was held in February 2011. Moreover, to exploit the untapped potential of a fully functioning security market, the Commission is currently preparing a Communication on an EU Security Industry Policy.

[29] Commission Communication on the mid-term evaluation of the Framework Programme 'Security and Safeguarding Liberties' (2007-2013), COM(2011) 318final.