EUROPEAN
COMMISSION

Brussels, 10.4.2013
COM(2013) 179 final

COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT AND THE COUNCIL

Second Report on the implementation of the EU Internal Security Strategy

COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT AND THE COUNCIL

Second Report on the implementation of the EU Internal Security Strategy

1. INTRODUCTION

1.1. Internal security in today's context

The EU's Internal Security Strategy is designed to enable Europe to respond to existing challenges and emerging threats, according to a shared approach that involves both EU actors and the national and local levels.

Underpinning the strategy are the common values of respect for fundamental rights and the rule of law, solidarity and mutual support. The Commission will continue to ensure full respect of these values, in particular of the European Charter of Fundamental Rights.

One of the major threats to our internal security is organised crime and its detrimental effects on the economy of the EU, including distortions in the internal market.

As an example, the United Nations Office on Drugs and Crime (UNODC) estimates that criminal proceeds are likely to have amounted to some 3.6% of global GDP or around US$2.1 trillion in 2009. Corruption, fraud and smuggling lead to huge losses for the governments of the EU Member States at a time when the need for a stable revenue and tax base is essential to tackle their public deficits.

To go after the money, and reclaim the proceeds of crime, continues to be a key aim of the EU's strategy for disrupting organised criminal networks.

The Commission has already introduced initiatives and instruments to achieve this goal, such as the Directive on the freezing and confiscation of the proceeds of crime in the European Union, the Fourth Anti Money Laundering Directive, and the Directive on the protection of the financial interests of the EU.

The administrative approach, providing opportunities for detecting and responding to criminal infiltration of the economy, also supports the aim of redressing imbalances caused among other things by organised crime and creating the conditions for the internal market to flourish. The recent establishment at Europol of the European Cybercrime Centre (EC3) is designed to strengthen Europe's capability to protect citizens, businesses and governments and their infrastructure from cyber-attacks that can cause staggering economic losses.

The ISS is based on five strategic objectives, namely disrupting international crime networks, preventing terrorism, enhancing cybersecurity, strengthening border security and increasing resilience to crises and disasters. In the 2011 ISS implementation report, the fight against organised crime and cybercrime were identified as two main challenges to be addressed in the coming year. A lot has since been done, together with actions under the other objectives of the strategy.

2. THE INTERNAL SECURITY STRATEGY IN THE PAST YEAR

2.1. Strategic objective 1: Disrupt international crime networks

The activities of organised crime networks are thought to be more complex, diverse and international in scope than ever before. For example, internet-facilitated organised crime will continue to increase in line with the rising use of broadband internet and mobile devices.

The **EU Policy Cycle on serious and organised crime** helps coordinate operational cooperation on crime phenomena relevant for the whole of the EU. Member States act jointly to fight prioritised cross-border crime, with the support of the EU agencies and institutions. The priority crime phenomena are identified through the threat assessments produced by Europol (notably, the SOCTA), based on contributions from the Member States. Currently a short policy cycle covering the period 2011-2013 is being implemented as a learning phase for a full policy cycle spanning 2013-2017.

In early 2013 the Commission adopted proposals for a **Fourth Anti Money Laundering Directive**[1] together with **a Fund Transfer Regulation**[2]. The latter will be supplemented, later in 2013, by a proposal for a **Directive on the criminalisation of money laundering**. This package will address new risks and threats, notably by enhancing the transparency of legal entities. Actions against money laundering are also developed outside the EU by the External Action Service in cooperation with regional platforms in Africa and Latin America.

A proposal for a **Directive on the counterfeiting of currencies**[3] was also adopted in early 2013. The proposal lays down in particular new criminal sanctions. Another important feature is the obligation of the Member States to make effective investigative tools available for detecting currency counterfeiting cases, equivalent to those used to combat organised or other serious crime.

The proposals for a **Directive on the fight against fraud to the Union's financial interests by means of criminal law**[4] and a **Directive on criminal sanctions for insider dealing and market manipulation**[5] are additional criminal law tools that address key vulnerabilities pertaining to trade in the internal market and financial markets, respectively.

The Commission has continued to promote a new **EU anti-corruption strategic initiative**. This follows a two-fold approach: an 'EU Anti-Corruption Report' to assess Member States' efforts against corruption on a regular basis, and a stronger focus on corruption across internal and external EU policy fields. A group of 17 experts on corruption and a network of local research correspondents in all Member States were set up to prepare the first EU Anti-Corruption Report to be presented in 2013.

The European National Integrity Systems (ENIS) project, co-financed by the Commission, was completed by Transparency International in 2012, covering 23 EU Member States, Norway and Switzerland. A total of 13 institutions and sectors in each country were analysed and scored for their capacity to cope with corruption. Transparency International published individual country assessments and a comparative analytical report. The recommendations and conclusions of the ENIS assessments are among the sources considered in the work on the EU Anti-Corruption Report.

Confiscation of criminal wealth can effectively combat crime as it attacks the financial incentive of criminals, protects the economy against criminal infiltration and corruption, and helps restore social justice. A proposal for a **Directive on the Freezing and Confiscation of Proceeds of Crime in the EU**[6] was adopted by the Commission to make it easier to freeze and confiscate the profits from serious and organised crime in the European Union through common minimum rules, and thus protect the licit economy.

1 COM(2013) 45/3.
2 COM(2013) 44/2.
3 COM(2013) 42 final.
4 COM(2012) 363 final.
5 COM(2011) 654 final.
6 COM(2012) 85 final.

Efforts at the EU level go hand-in-hand with Member State initiatives, such as the establishment of new asset recovery offices and teams in Austria, Romania and Estonia, and Europol's support to Member States through the Europol Criminal Assets Bureau. Some Member States have also put in place mechanisms to re-use confiscated assets for public and social purposes.

The Spanish Centre of Excellence on Asset Recovery and Training (CEART) project, co-financed by the European Commission, produced a White Book on Asset Recovery Offices which describes in detail the activities of each Office. The CEART project also included an international training course on asset recovery and financial investigations which was among the first pan-European courses available for asset recovery practitioners.

The European Union concluded new agreements with the United States and Australia on the use and transfer of **Passenger Name Records (PNR)**[7], and is close to concluding negotiations with Canada. These agreements enable data to be analysed by our partners to prevent, detect and investigate serious cross-border crimes, including terrorist offences. PNR data, not least by allowing the identification of persons previously 'unknown' to law enforcement authorities but posing a security risk, help disrupt criminal networks faster and more effectively.

The **EU Strategy towards the Eradication of Trafficking in Human Beings 2012-2016**, adopted in June 2012, concentrates on increased prosecution of traffickers, assistance to and protection of victims of trafficking and prevention of trafficking in human beings, expanding and complementing the Directive adopted in 2011[8]. The EU Anti-Trafficking Coordinator has a key responsibility in the implementation of the Strategy with a view to improving coordination and coherence among relevant actors. **The Operational Action Plan on Trafficking of Human Beings**, co-led by the United Kingdom and the Netherlands, is one of the eight priority areas in the EU Policy Cycle on serious and organised crime. To enhance focus and coherence in the external dimension of the EU's work on trafficking in human beings, a list of priority non-member countries was agreed by the Member States, in close cooperation with the Commission, the European External Action Service and the EU agencies.

Cross-border information exchange within the EU is essential to the fight against serious and cross-border crime. There is, however, scope for improvement. In its Communication on the **European Information Exchange Model** (**EIXM**), the Commission sets out a blueprint for better implementation of existing EU instruments, more systematic use of the Europol channel for information exchange, and national Single Points of Contact bringing together the main channels for information exchange[9].

The new EU drugs strategy 2013 – 2020 focuses among others on the dynamics in the illicit drug markets, including shifting drug trafficking routes, cross-border organised crime and the use of new communication technologies as a facilitator for the distribution of illicit drugs and new psychoactive substances. It has a number of objectives, among which to contribute to a measurable reduction of the demand for drugs, of drug dependence and of drug-related health and social risks and harms; to contribute to a disruption of the illicit drugs market and a measurable reduction of the availability of illicit drugs; to encourage coordination through active discourse and analysis of developments and challenges in the field of drugs at EU and international level

[7] OJ L 186, 14.7.2012, p. 4 (Australia) and OJ L 215, 11.8.2012, p. 5 (the United States).

[8] Directive 2011/36/EU on preventing and combating trafficking in human beings and protecting its victims.

[9] COM(2012) 735 final.

The **'EU Drug Markets'** report launched in January 2013 was a major step forward in coordination between agencies in the home affairs area to combat organised crime and illicit drug trafficking. Produced jointly by the European Monitoring Centre for Drugs and Drug Addiction (EMCDDA) and Europol, the report highlighted a number of new trends, including mobile amphetamine and ecstasy production and the explosive growth of new psychoactive substances that are aggressively marketed at young people via the internet. Pan-European cooperation and clear understanding of drug market developments are essential to effective law enforcement in this fast-changing area.

Europol plays an important role in facilitating cross-border information exchange in the EU through the provision of information exchange and storage systems and a range of operational support services and analytical products. By the end of the third quarter of 2012, Europol had facilitated the exchange of over 200 000 operational messages and almost 12 000 cases had been initiated. Europol supported an increasing number[10] of high-profile operations in the Member States through the provision of operational support services and over 600 operational analysis reports. Contributions of information by Member States to the Analysis Work Files increased by 40 per cent overall following the implementation of the priorities agreed in the EU Policy Cycle context, and increased by as much as 60 per cent in the area of trafficking in human beings.

Cross-border cooperation and information exchange is also supported by the EU-level training provided by **Cepol**. In 2012, Cepol provided training to almost 6 000 participants in more than 100 different training activities on various topics ranging from financial crime and drugs trafficking to JITs, trafficking in human beings and cybercrime.

Eurojust remains an important actor in judicial cooperation in criminal cases. The fight against serious and organised crime has been and continues to be a priority for Eurojust casework. Organised crime groups appear, not only as a stand-alone feature, but also as a cross-cutting characteristic that adds a more serious component to other crimes. In 2012, 231 cases related to organised crime were registered at Eurojust compared to 197 cases in 2011.

Another effective tool in tracing criminals is the use of **Joint Investigation Teams (JITs)**. The financing provided by Eurojust facilitates the establishment of JITs based on operational needs also at short notice. Until February 2013, Eurojust has supported, via the second JIT Funding Project, 87 different JITs based on 252 funding applications received. Most JITs focus on drugs and human trafficking, but they also targeted money laundering, fraud, corruption and organised robbery.

The JIT 'Tokyo case' was set up between Belgium, France and the United Kingdom, with the participation of Eurojust and Europol, to investigate a network of couriers recruited by an organised crime ring in Belgium and France for international drug trafficking from Brazil and some central African countries to Japan via London. A joint operation took place, with several arrests in Belgium and the UK. Two individuals were subsequently sentenced to eight years imprisonment and a fine of €3 780 and six years and six months imprisonment and a fine of €30 000, respectively.

The way forward in 2013

The Commission will:

- **publish the first EU Anti-Corruption Report, including recommendations for Member States;**

[10] An increase of 43 per cent compared to 2011.

- **propose a Directive on criminal penalties for money laundering;**
- **propose a reform of Eurojust;**
- **develop a political initiative to combat illicit trafficking in firearms to safeguard the internal security of the EU;**
- **propose two legislative acts amending Council Decision 2005/387/JHA of 10 May 2005 on the information exchange, risk-assessment and control of new psychoactive substances and Council Framework Decision 2004/757/JHA of 25 October 2004 laying down minimum provisions on the constituent elements of criminal acts and penalties in the field of illicit drug trafficking;**
- **present a Regulation on setting up a European Public Prosecutor's Office in order to improve the protection of the European Union's budget and enhance criminal prosecutions in this area;**
- **adopt a Communication on a comprehensive strategy to fight cigarette smuggling.**

Member States are encouraged to:

- **make swift progress in negotiating the proposal for the reform of Europol and Cepol, combined with a stronger emphasis on training of law enforcement officials, to strengthen cross-border cooperation;**
- **conclude the discussions with the European Parliament on the Directive on the freezing and confiscation of proceeds of crime in the EU and on the Directive on the use of PNR data for law enforcement purposes;**
- **continue further developing the resources and powers of their Asset Recovery Offices;**
- **follow up on the recommendations set out in the Communication on the European Information Exchange Model (EIXM);**
- **take action, as set out in the EU Strategies, to address trafficking in human beings and drugs;**
- **follow up on the recommendations set out in the upcoming first EU Anti-Corruption Report 2013;**
- **implement Operational Action Plans within the policy cycle on: trafficking in human beings, mobile organised crime groups, smuggling of commodities in container form, synthetic drugs, drugs routes originating from West Africa, and crime originating from the Western Balkans.**

2.2. Strategic objective 2: Prevent terrorism and address radicalisation and recruitment

According to Europol, although the overall number of terrorist attacks in the EU Member States has been decreasing in recent years, the terrorist threat currently presents a highly diverse picture (Al-Qaeda-inspired, right- and left-wing or anarchist, separatist and single-issue terrorism), with a possible increase in plots by lone actors and small, autonomous groups. In addition, the geopolitical developments in the Middle East, the Sahel region and the Horn of Africa will impact on the security situation in Europe. Especially, radicalised EU

citizens travelling to and participating in conflict zones, referred to as foreign fighters, returning to Europe with conflict experience, will continue to pose a threat to the EU.

Combating terrorism has remained a priority for the European Union in a year when the attacks in Toulouse and Burgas tragically highlighted the reality of the terrorist threat.

In the aftermath of the Burgas attack, **Europol** provided highly appreciated operational support to the Bulgarian authorities. In addition, the EU AirPol network, consisting of police authorities responsible for security at airports and surrounding areas, issued guidance on new security measures and procedures to prevent similar attacks within 24 hours.

The AirPol network received its mandate on the basis of a Council Decision in the aftermath of the Yemen cargo attacks in 2010 and works to share best practices and undertake capacity-building on the basis of the Commission's crime prevention funding programme (ISEC).

Terrorism remains one of the priorities in the operational work of **Eurojust**[11]. Moreover, in 2012 Eurojust developed further the concept and contents of its Terrorism Convictions Monitor (TCM), which provides an overview of terrorism-related judicial developments in the Member States, as well as judicial analysis on selected cases.

A practitioners' workshop co-organised by Eurojust and Europol in December 2012 brought together counter-terrorism specialists from India and from the EU. Its objective was to promote judicial cooperation by defining common interests and reflecting on standards.

The European counter-terrorism policy is based on prevention. **The EU Radicalisation Awareness Network** (RAN) was established to connect actors involved on the ground in countering radicalisation and violent extremism throughout Europe (first-line practitioners, field experts, social workers, academics, NGOs, etc.). With eight thematic groups, the RAN offers a unique opportunity to share experience and results. The outcomes of the RAN's work so far were also reported back to policy makers and discussed at a High Level Conference at the end of January 2013.

The RAN recommendations, and in particular those provided by the working group on foreign fighters, will also contribute to the EU's efforts to strengthen **the synergies between internal and external security policies**.

The ISEC programme has been supporting projects which address the issue of radicalisation and violent extremism in particular through better training and awareness-raising for practitioners, disengagement and de-radicalisation, increasing the response capacity of citizens and civil society, disseminating terrorist victims' testimonies and countering terrorist propaganda. Such projects are being carried out by participating organisations from amongst others Belgium, Denmark, Germany and the United Kingdom.

As another example of terrorist prevention efforts, the EU has, via its **Regulation on the use and marketing of explosives precursors**[12], established the most advanced system on a global scale to prevent access to precursors to explosives that may be used by terrorists.

The Commission, in cooperation with the Member States, is currently working on new proposals on **Chemical, Biological, Radiological, Nuclear and Explosives (CBRN-E) security** at EU level. The focus is on the most pertinent actions to be implemented in the

[11] All in all 32 terrorism-related cases were registered at Eurojust in 2012, including cases concerning terrorism financing.

[12] 2010/0246 (COD).

coming years, and on obtaining synergies from the work done in the areas of CBRN-E, including detection, based on two progress reports published in 2012.

The Commission has started a review of the **Critical Infrastructure Protection Directive**[13], with a view to proposing a new approach in the first half of 2013. The aim is to ensure that services vital to society remain operational. Loss or failure of critical infrastructure could have severe consequences for society.

Project Poseidon, co-funded by the Critical Infrastructure Protection Programme, identified threats and vulnerabilities in both critical infrastructures and decision-making mechanisms to improve security in cross-border passenger traffic in the Baltic Sea Region. The results are contained in the pilot study (Preventing Terrorism in Maritime regions — Case Analysis of Project Poseidon) and they concern for instance counter-terrorism strategies as regards ferry traffic.

Integral connections between different transport modes require a robust counter-terrorism strategy to protect the stability of commerce and maintain confidence in the security and safety of the transport network. In 2012 the Commission issued a paper on **transport security**[14], highlighting a number of areas of key significance to the effective mitigation of terrorist threats. Among other things, the paper suggests the creation of a general security framework for transport operators, such as security programmes, security awareness training and exercises, contingency and recovery planning.

As regards aviation security, the developments are threat-driven and the **detection technology** needs to keep up with the continuous innovation demonstrated by terrorist groups. The establishment of an EU harmonised certification system for airport screening equipment is being finalised, and international coordination is on-going to streamline the scientific work. The Commission and the Member States are actively supporting innovative technology trials to improve detection of the different threats (for example in cargo, in baggage and on persons).

In addition to several research activities on testing innovative technologies, the Commission, jointly with the Member States, has launched pro-active detection activities with a number of **operational trials**, both during the Euro 2012 Football Championships and in areas of mass transit and public buildings security to develop the most effective security models.

For example, the Commission is implementing the ITRAP (Illicit Trafficking Radiation Assessment Programme) with the aim of providing an independent assessment of the available radiation detection equipment on the market used for the detection and identification of nuclear and radioactive materials.

Training is a cornerstone of effective implementation of security systems. An example of a concrete action supported by the Commission in this field is the establishment of the European Security Training Centre (EUSECTRA) the aim of which is to develop a security training programme applicable to the law enforcement community.

ATLAS, an EU network of anti-terrorist intervention forces established and funded by the Commission via the ISEC programme since 2008, improves the cooperation between special intervention units in the EU and support its functioning in crisis situations (for example a terrorist attack or a hostage taking) when a Member State needs assistance. It also establishes

[13] Directive 2008/114/EC on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection.

[14] SWD(2012) 143 final.

common platforms for training, sharing equipment, and close cooperation in the Member States' border areas.

The way forward in 2013

The Commission will:

- **update the EU approach to counter violent extremism by developing a European 'toolbox' based on best practices in the Member States;**
- **propose actions on CBRN-E;**
- **develop tools to enhance the detection of terrorist threats in all areas, including standards for aviation security;**
- **propose a new approach on European Critical Infrastructure protection.**

Member States are encouraged to:

- **step up efforts to prevent and counter violent extremism;**
- **implement the Action Plan on air cargo security;**
- **set up the necessary administrative structures to implement the Regulation on explosives precursors.**

2.3. Strategic objective 3: Raise levels of security for citizens and businesses online

A variety of activities relating to internet fraud are becoming more prominent, including illicit internet transactions, use of money mules and fake websites. The past two years have also witnessed an increase in the number of hackings and internet-driven illegal activities.

The fight against cybercrime is not only about reducing crime in the online environment, but also about ensuring a secure cyberspace within which economic and social activity can flourish. This remains a priority for the Commission and the Member States and is pursued also through the Digital Agenda Europe. It is important to pool resources at EU level for better prevention and a stronger response capacity. Significant measures have been taken at both strategic and operational level.

The **Cybersecurity Strategy for the European Union**, adopted in February 2013[15], sets out a comprehensive vision and puts forward the actions required, based on strong protection and promotion of citizens' rights, to make the EU the safest online environment in the world. The strategy aims to strengthen resilience and network and information security; drastically reduce cybercrime; develop an EU cyberdefence policy; foster the industrial and technological resources for cybersecurity; promote Research and Development (R&D); and enhance the EU international cyberspace policy.

The strategy highlights the need for reinforced cooperation and exchange of information between the relevant actors to provide early detection and a more coordinated response. The objectives of the strategy are mutually reinforcing. For example, the resilience and network and information security objective includes actions aimed at strengthening public-private partnerships and at setting up National Computer Emergency Response Teams (CERTs). This will in turn support the fight against cybercrime.

[15] JOIN(2013) 1 final.

These objectives were highlighted in a proposal for a **Directive on network and information security**[16] accompanying the Strategy. The main objective of the proposal is to ensure the smooth functioning of the internal market. The proposal aims to raise national preparedness, strengthen EU-level cooperation and ensure that operators of essential services and infrastructure carry out appropriate risk management and report serious incidents to the national competent authorities.

An important step in the fight against cybercrime was the creation of the **European Cybercrime Centre (EC3) at Europol** in early 2013. The Centre, in close cooperation with Eurojust, will bolster the EU's capacity to confront the growing and complex threat posed by cybercrime and become a focal point for cybercrime-related issues. It will provide better operational support capacity at the EU level for cross-border cybercrime, specialised strategic and threat assessments, and more targeted training and R&D that result in the development of specialised tools to tackle cybercrime. The Centre will also develop cooperation with all stakeholders including those outside the law enforcement community. In view of the inherently cross-border nature of the phenomenon and the need for international cooperation, the EC3 will able to engage the EU's law enforcement community with other international actors such as Interpol and draw upon efforts of other actors such as the ICT industry or the Internet Corporation for Assigned Names and Numbers (ICANN).

The EC3 will be able to voice concerns and make suggestions, through the Commission, on questions relating to internet governance. The EC3 will also liaise with the European Network and Information Security Agency (ENISA), which gathers and generates network and information security analysis, supports Member States in developing harmonised breach reporting approaches, in building CERT capacities and in raising end-users' awareness. The foreseen renewal of ENISA's mandate will cater for its support to the Member States and the Commission also in the coming years.

Another example of strategic initiatives undertaken in 2012 was the EU-US initiative to launch a **Global Alliance against Child Sexual Abuse Online**. The Alliance — including 48 countries around the world at its launch — will help foster global cooperation in the fight against child pornography online. By uniting countries behind a shared set of targets and goals, it is expected to result in more child victims being identified and rescued, more effective prosecution of perpetrators, better prevention of offences and a reduction in the availability of child sexual abuse images online. The European strategy for a better internet for children[17] strengthens the preventive measures even further by setting out child safety actions built on empowerment and protection, thereby encouraging children to make responsible use of the internet.

The proposal for a **Directive on attacks against information systems**[18], which is now being negotiated between the European Parliament and the Council, aims to approximate criminal legislation in the Member States in the area of cybercrime and introduces definitions of and sanctions for illegal access to information systems, illegal system and data interference and illegal interception. In addition, the proposal penalises the production, sale, procurement for use, import and distribution of tools used for committing these offences. Only six EU Member States still have to ratify the Budapest Convention on Cybercrime.

In addition, cybercrime is one of the eight fields of operational cooperation within the **EU policy cycle for organised and serious international crime**. Specific actions to be

16 COM(2013) 48 final.
17 COM (2012) 196.
18 COM(2010) 517 final.

implemented by the Member States under the leadership of Romania include the establishment of national reporting systems in each Member State on data breaches/cyber incidents/cybercrimes for legal entities and citizens, reinforcing internet governance so that users in cyberspace can be identified by Member States' authorities for legitimate law enforcement reasons, and mitigation of tools (botnets) that facilitate large-scale cyber-attacks.

The ISEC programme provides co-funding to assist the Member States with building their capacity to deal with cybercrime and promote cross-border and public-private cooperation. Recent successful projects involve the setting-up of a network of national centres of excellence to promote cooperation initiatives between research, academia and law enforcement practitioners that result in tangible tools for understanding, detecting and fighting cybercrime. There are currently a total of eight such centres receiving funding from the Commission. To date, the Commission has contributed almost €5 million to building cybercrime training and research capacities in the Member States.

The way forward in 2013

The Commission will:

- **make sure that the European Cybercrime Centre (EC3) at Europol takes important steps towards becoming fully operational;**
- **implement the EU Cybersecurity Strategy for the European Union;**
- **support the adoption of the proposed Directive laying down measures to ensure a high common level of network and information security across the EU and pursue the new mandate of ENISA;**
- **continue to support, develop and enlarge the Global Alliance against Child Sexual Abuse Online.**

Member States are encouraged to:

- **work closely with the European Cybercrime Centre (EC3);**
- **work closely with Eurojust and ENISA;**
- **implement the Operational Action Plan on cybercrime within the policy cycle;**
- **pursue the shared policy targets of the Global Alliance against Child Sexual Abuse Online, and take specific actions to achieve them;**
- **support the ratification and implementation of the Council of Europe Budapest Convention on Cybercrime**.

2.4. Strategic objective 4: Strengthen security through border management

In December 2011, the Commission presented a legislative proposal for a **European Border Surveillance System (Eurosur)**. Its adoption is foreseen in 2013 and it will provide the Member States and the EU agencies with a common framework for near real-time information sharing and interagency cooperation at national and European level for the purpose of fighting irregular migration and cross-border crime. Eurosur will also contribute to enhancing the protection and saving the lives of migrants.

National coordination centres for border surveillance involving a number of national authorities, such as border guards, police, coast guards and the navy, were established by the 18 Schengen countries located at the southern and eastern external borders that are the first to

join Eurosur. These 18 national coordination centres have been connected by Frontex to the Eurosur network on a pilot basis.

Within the framework of Eurosur, the External Borders Fund (EBF) has financed important regional surveillance systems, enabling better control of the external borders of the Schengen area. EBF contributions were given to the Spanish integrated surveillance system SIVE (Sistema Integrado de Vigilancia Exterior), which focused in particular on the Strait of Gibraltar, the Canary and Balearic islands and the southern Mediterranean coast. The EBF also contributed significantly to the French coast surveillance system.

With the dual objective of enhancing security at borders and facilitating travel and access for non-EU nationals, the Commission adopted early 2013 two legislative proposals for an **Entry/Exit System (EES)** and a **Registered Traveller Programme (RTP),** the so-called **Smart Borders Package**.

After many years of development and testing, the Schengen Information System II (SISII) will become fully operational and provide additional means of border management. In parallel, the completion of worldwide roll-out of the Visa Information System (VIS) will further strengthen security.

The Commission is assisting Greece in the implementation of the Action plan on asylum and migration management which also includes a border management component, in order to improve the capacity of Greece to better control its external borders, in particular the external border with Turkey.

In the area of customs border management, the work on the implementation of common risk management continued and the Commission presented a Communication on Risk Management and supply chain security[19]. The aim of this Communication is to foster the debate with the institution on the recommendations in order to ensure the conditions to collectively improve the current situation. Furthermore, and following the High Level Air Cargo security plan work continues with transport authorities and traders to ensure the improvement of the data quality being already received by customs.

Frontex has supported security through various activities facilitated by its reinforced mandate. In particular, in close cooperation with the border management services of Member States, it has further developed the Frontex Risk Analysis Network and provided for regular and ad hoc risk analysis in relation to irregular migration at the external borders of the EU. Joint operations were carried out at all main hot-spots at the external borders. Frontex pursued operational cooperation with other relevant EU agencies, such as Europol, the European Asylum Support Office and the Fundamental Rights Agency. Frontex has also assisted the Member States in organising joint return operations in line with the EU's return policy.

Following successful cooperation in the Frontex-coordinated Joint Operation INDALO in 2011 and 2012, addressing irregular migration and smuggling of drugs, the Commission encouraged Frontex, Europol, the Centre de Coordination pour la Lutte Antidrogue en Méditerranée (CeCLAD-M) and the Maritime Analysis and Operation Centre Narcotics (MAOC-N) to formalise their cooperation in line with the proposed Eurosur Regulation.

Furthermore, following the entry into force of the amended Frontex Regulation at the end of 2011, the Commission encouraged Frontex and Europol to finalise the necessary arrangements for allowing the transfer from Frontex to Europol of personal data related to cross-border criminal activities facilitating irregular migration or human trafficking.

[19] COM(2012) 793 final.

In 2012, important progress has been made in implementing the new fundamental rights provisions of the revised Frontex Regulation. The Fundamental Rights Forum has been established and has stated its work, and a Fundamental Rights Officer has been appointed.

The efforts to improve cooperation between border guards and customs remained important fields of activity in 2012. The aim is to facilitate trade and travel and enhance the security of the EU through, inter alia, synchronised checks, information exchange, training, joint risk analysis and joint operations. Advanced solutions already exist in some Member States and serve as best practice. Finland, for example, has set up police-customs-border guard intelligence, investigation and analysis units which make for greater effectiveness in the fight against serious crime.

The European Borders Fund supported Member States in their efforts to fight the use of fake and falsified identity and travel documents, in particular for purchasing specific equipment used by border guards and in consular offices to verify the authenticity of documents. The EBF also contributed to the development of FADO (False and Authentic Documents Online), a web-based tool facilitating the exchange of information between the Member States on detected document fraud.

The way forward in 2013

The Commission will:

- **support the launch of Eurosur as of 1 October 2013;**
- **ensure that Schengen Information System II (SISII) becomes fully operational during the spring.**

Member States are encouraged to:

- **ensure that all national authorities with responsibility for border surveillance cooperate via the national coordination centres;**
- **make swift progress in negotiating the proposals on the Entry/Exit System (EES) and the Registered Travellers Programme (RTP);**
- **agree on common recommendations and best practices in border guards-customs cooperation in order to guarantee the same level of security and service at all EU external borders and to reduce the costs of checks;**
- **discuss and agree on common recommendations to improve Customs Risk Management and supply chain security;**
- **implement the Operational Action Plan on irregular immigration within the policy cycle.**

The agencies should:

- **further step up their cooperation to detect and prevent irregular migration and cross-border crime at the external borders (Frontex, Europol, MAOC-N and CeCLAD-M);**
- **take the necessary steps to allow the transfer of personal data to Europol in accordance with the amended Frontex Regulation (Frontex and Europol).**

2.5. Strategic objective 5: Increase Europe's resilience to crises and disasters

In the field of both natural and man-made risks, the EU has enhanced its risk management capacity in order to allocate resources more efficiently, reinforce the EU's prevention and preparedness capacity.

The proposal for the implementation arrangements for the **solidarity clause** (Article 222 TFEU) will provide an umbrella framework for situations of extraordinary threat or damage that overwhelm the response capacities of the affected Member State(s). A joint proposal by the Commission and the High Representative of the Union for Foreign Affairs and Security Policy for the arrangements for implementing the solidarity clause was adopted in December 2012[20].

A robust risk assessment methodology needs to be established and applied to ensure that security risks are managed effectively. The EU is developing a shared methodological approach to assess these security risks. Significant work has been conducted in the field of risks assessment related to intentional malicious threats, not least in the aviation security field (air cargo, liquids ban). In December 2012 the Council called upon the Commission to extend this methodological approach to the whole of **aviation security**.

In relation to building resilience to natural and man-made disasters, a number of actions have been carried out to implement the EU disaster risk management policy framework[21]. Member States have achieved varying progress in undertaking **national risk assessments** in line with the 2010 Commission's Guidelines[22]**.** To date, the Commission has received contributions from 12 countries participating in the EU Civil Protection Mechanism (Czech Republic, Denmark, Estonia, Germany, Hungary, Italy, Netherlands, Norway, Poland, Slovenia, Sweden and UK) with varying degrees of detail of the national risk analysis which highlight the need for more robust disaster data and comparative risk management approaches. On this basis, the Commission is currently preparing a first **cross-sectoral overview of natural and man-made risks** which the Union will face in the future, expected in 2013. This could be followed in 2014 by more extensive work integrating more in depth security risks.

The Commission's proposal for a new Union Civil Protection Mechanism[23] further places prevention on equal footing with preparedness and response actions and includes provisions to further develop risk assessment in civil protection policy.

The Commission has also consistently promoted the use of **peer reviews** as an effective way of exchanging experience and improving governance and policy-making in the area of disaster risk management. In 2012, the UK was the first country which volunteered to undertake such a 'pilot' peer review that was carried out by three 'peers' (from Italy, Finland and Sweden) with the support and facilitation provided by the Commission in cooperation with UNISDR and OECD. A report of the findings is expected in spring 2013, including good practices, areas for improvement and recommendations on how to achieve further progress. The results will also feed into the on-going work of the Commission in developing guidance **for disaster prevention** based on good practice.

---

20 JOIN(2012) 39 final.

21 Set out in Communication 'A community approach on the prevention of natural and man-made disasters, COM(2009) 82 final.

22 SEC(2010) 1626 final, available at: http://ec.europa.eu/echo/civil_protection/civil/pdfdocs/prevention/COMM_PDF_SEC_2010_1626_F_staff_working_document_en.pdf

23 COM(2011) 934 final.

The Commission will also open in 2013 the Emergency Response Centre, on the basis of the existing Monitoring and Information Centre (DG ECHO), which will further strengthen the EU capacity to respond to disasters.

Substantial work has been conducted to better rationalise and reinforce synergies between the different EU crisis management capacities. A more integrated and effective approach is the goal of the revised EU Crisis Coordination Arrangement procedures and the establishment of an integrated awareness and analysis capacity.

In 2012 several important actions were undertaken to reinforce the networking of multi-sector and sector-specific centres in the Commission and relevant agencies. These include the conclusion of agreements on risk and crisis management cooperation and the establishment of new high-performing and resilient means of communication. The setting-up in 2012 of the Commission's Strategic Analysis and Response Centre in DG HOME enabled new security risk assessment and management methodologies and practices to be established that bring together the expertise of relevant Commission departments and expert communities, e.g. in the areas of transport and energy, and draw on threat assessments by the EU Intelligence Centre, EU agencies and the Members States' services.

Enhancing the EU crisis management and risk assessment capability requires the capacity to **exchange classified information**. From this point of view, the establishment of a legal framework allowing the EU agencies to exchange classified information represents an important step forward.

The way forward in 2013

The Commission will:

- **support efforts to improve risk assessment methodologies and exchange and transfer experience between EU Member States and also with non-member countries on risk management related activities;**
- **produce a first cross-sectoral EU overview of natural and man-made risks;**
- **produce guidance on disaster prevention based on good practices**;
- **continue to foster the EU capacity to conduct the assessment of security risks**.

Member States are encouraged to:

- **finalise and regularly update their national risk assessments and undertake initiatives to improve the understanding of disaster and security risk, to promote risk management planning, and to disaster-proof EU-supported infrastructure investments and volunteer to undertake peer reviews of their national risk management policies;**
- **adopt the proposal for the implementation arrangements for the solidarity clause.**

3. STREAMLINING AND RATIONALISING THE IMPLEMENTATION OF SECURITY POLICIES

The internal security policy is based on a shared agenda involving all actors: EU institutions, Member States and EU agencies. In 2012, the European Parliament issued its first opinion on the Internal Security Strategy, broadly endorsing the Strategy's five objectives[24].

In meeting the threats to internal security in the EU, cooperation between Member States will be of great value. Pooling resources and streamlining actions at EU level can be more effective and less costly than acting alone. The EU agencies have a special role to play in this regard.

3.1. Streamlining work

The Commission has tabled in March 2013 a proposal on the reform of Europol and Cepol, proposing the merging of the two agencies into one, and a Communication on a European Law Enforcement Training Scheme (LETS).

The overall goal in **reforming Europol** as well as **Eurojust** is to improve the operational efficiency and effectiveness of the agencies in addressing the security threat posed by serious and organised crime and terrorism. Improving Europol's capabilities to map criminal threats and trends will further strengthen both the EU's and the Member States' response to criminal networks and their detrimental effects on society and the economy, by improving the support Europol can provide to Member States, enhancing coordination and synergies between operations carried out by Member States, and better supporting the EU Policy Cycle on serious and organised crime.

Cepol and Europol have complementary missions, with Cepol supporting the development of an EU law enforcement cooperation culture through training. The proposed **merger of Cepol and Europol** would make training more focused and aligned with actual training needs, as set out in the **European Law Enforcement Training Scheme (LETS)**, which the Commission adopted at the same time. It would pool scarce financial and human resources, allowing the EU to provide more training courses overall. By making Europol's services more operational, and by targeting training towards EU priority needs, resources can be freed at national level and redirected as necessary.

The European Cybercrime Centre is another example of streamlining for the purpose of tackling cybercrime more efficiently. Investigations into online fraud, child abuse and other crimes regularly involve hundreds of victims at a time, and suspects in many different parts of the world. Operations of this scale cannot be successfully concluded by national police forces alone. No crime is as borderless as cybercrime, requiring law enforcement authorities to adopt a coordinated and collaborative approach across borders, together with public and private stakeholders alike.

Streamlining funding arrangements is a means to ensure more targeted use of resources. In 2012 the Commission issued proposals for the Internal Security Fund for the new financial perspectives 2014-2020. One of the innovations proposed is to apply shared management to all the funds (previously the ISEC fund was not included), which means that an increasing part of the available resources will be managed directly by the Member States.

[24] Borsellino report, European Parliament resolution of 22 May 2012 on the European Union's Internal Security Strategy ((2010)2308 (INI)).

3.2. Ensuring consistency between the internal and external dimension

With threats partly stemming from outside the boundaries of the EU, **enhanced cooperation with external security actors, non-member countries and organisations** is crucial in conducting successful security policies.

As part of a broader effort to enhance consistency between the internal and external dimensions of security, work was taken forward through the Political and Security Committee (PSC) and the Standing Committee on Internal Security (COSI) to implement the roadmap on strengthening ties between the Common Security and Defence Policy and actors dealing with Freedom, Security and Justice, and to further develop synergies in other areas such as cyber security, critical infrastructure protection and counter-terrorism. Closer linkages between the EEAS and relevant agencies (e.g. Europol and Frontex) have also been established. Two PSC-COSI meetings were organised in 2012 in which exchanges on geographical dimensions (Western Balkans, Sahel and Libya) of EU activities have been addressed, and a PSC-COSI meeting concentrating on the security situation in Mali took place in February 2013.

Internal security issues are now systematically added to the agenda of political dialogues with relevant non-member countries and organisations, and are also addressed in relevant strategic partnerships and agreements. The launch of the dialogues towards **Mobility, Migration and Security Partnerships** with southern Mediterranean countries represents other channels to strengthen cooperation on internal security matters with external partners. Equally, the pre-accession process and in particular on-going work in the context of the post-visa liberalisation monitoring mechanism with five Western Balkan countries, the implementation of the visa liberalisation roadmap with Kosovo and the Positive Agenda with Turkey are powerful tools to assist non-member countries in aligning their legal framework and operational capacity with the EU *acquis* and standards in the field of security.

Specific actions countering global threats that enhance the EU's internal security are financed equally outside the EU under the EU Instrument for Stability.

3.3. Preparing the future: the FP7 Security Research programme and beyond

Since 2007 the Commission has funded the FP7 Security Research programme up to 1.4 billion of euros. More than 250 projects have been funded with a significant involvement of stakeholders. A majority of the topics contained in the scope of this report have been addressed, such as counter explosive actions, CBRN action, radicalisation, and border security.

The Commission published in July 2012 a Communication for a Security Industrial Policy – Action Plan for an innovative and competitive Security Industry[25]. The Action Plan foresees further measures to harmonise the EU security market and close the gap between research and market, notably through standardisation activities in the area of CBRN protection, border security and crisis management/civil protection.

4. CONCLUSION

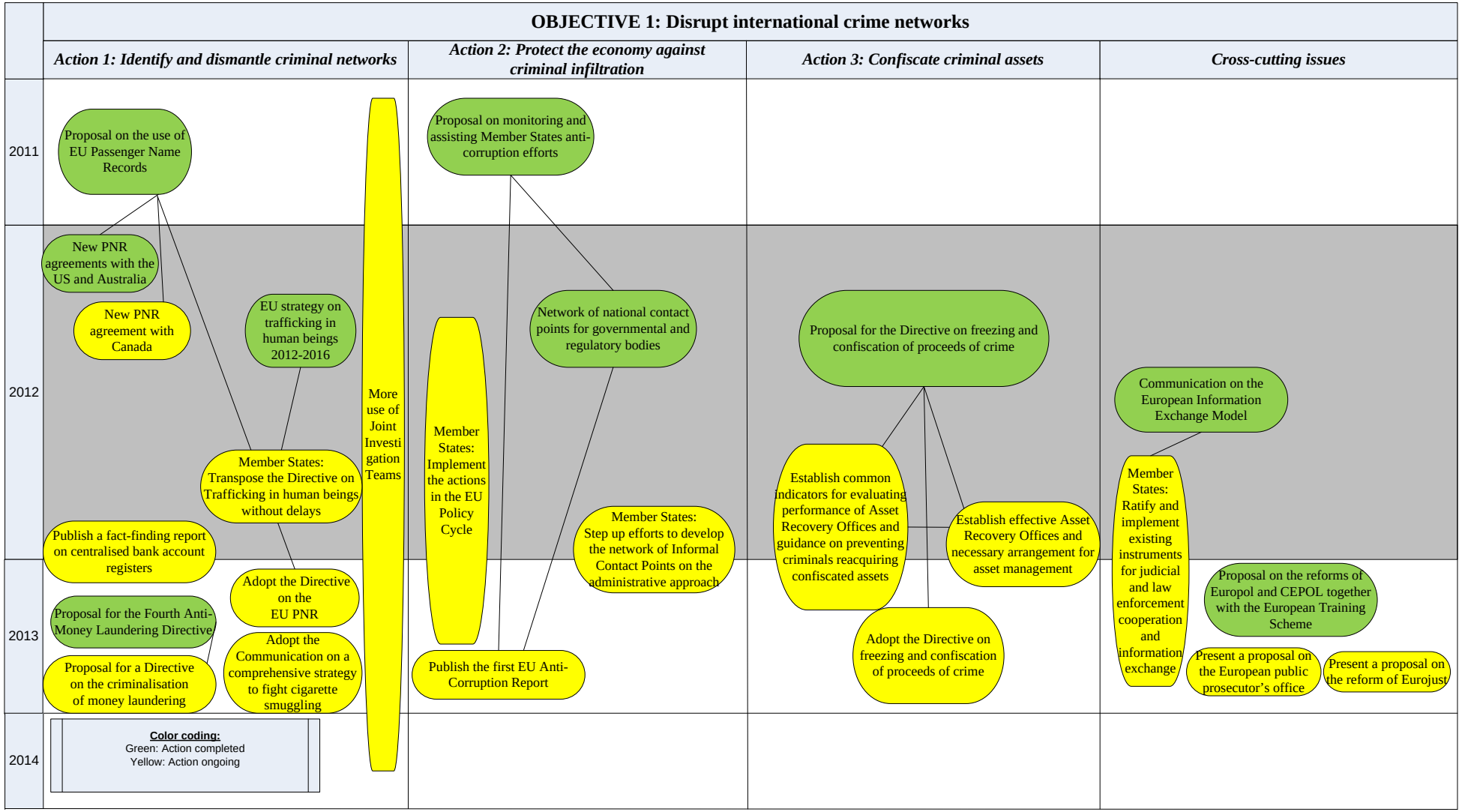
Implementation of the Internal Security Strategy is well on its way. As this report has shown, a lot has been done under the five objectives. However, we still have a way to go. For 2013 organised crime is still considered to be one of the major challenges for EU internal security to address. Money laundering, corruption, trafficking and mobile organised crime groups are

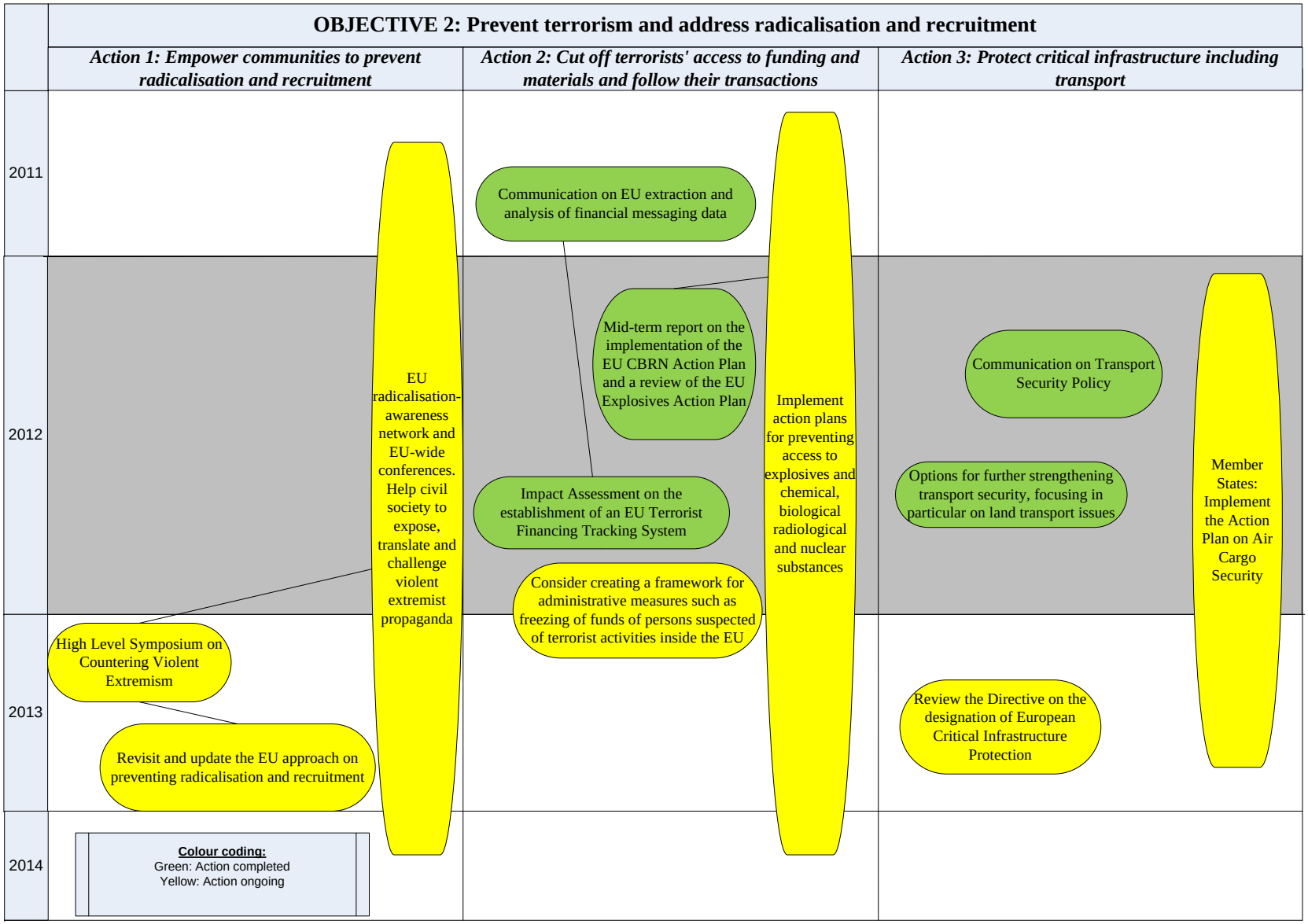
[25] COM(2012) 417 final.

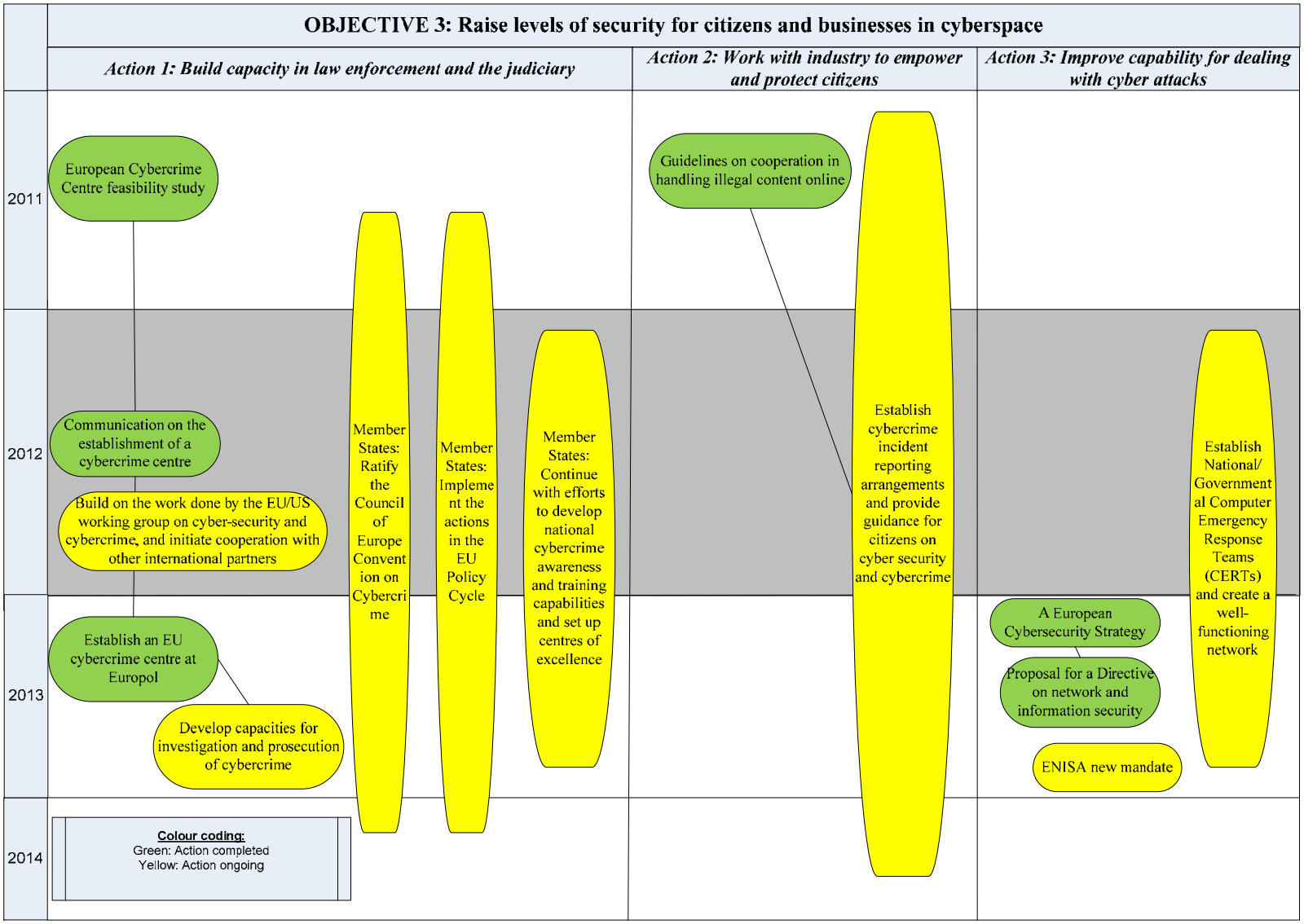
just some of the threats foreseen. Cybercrime continues to be of particular concern. Another important challenge for 2013 is to improve tools to better counter growing violent extremism.

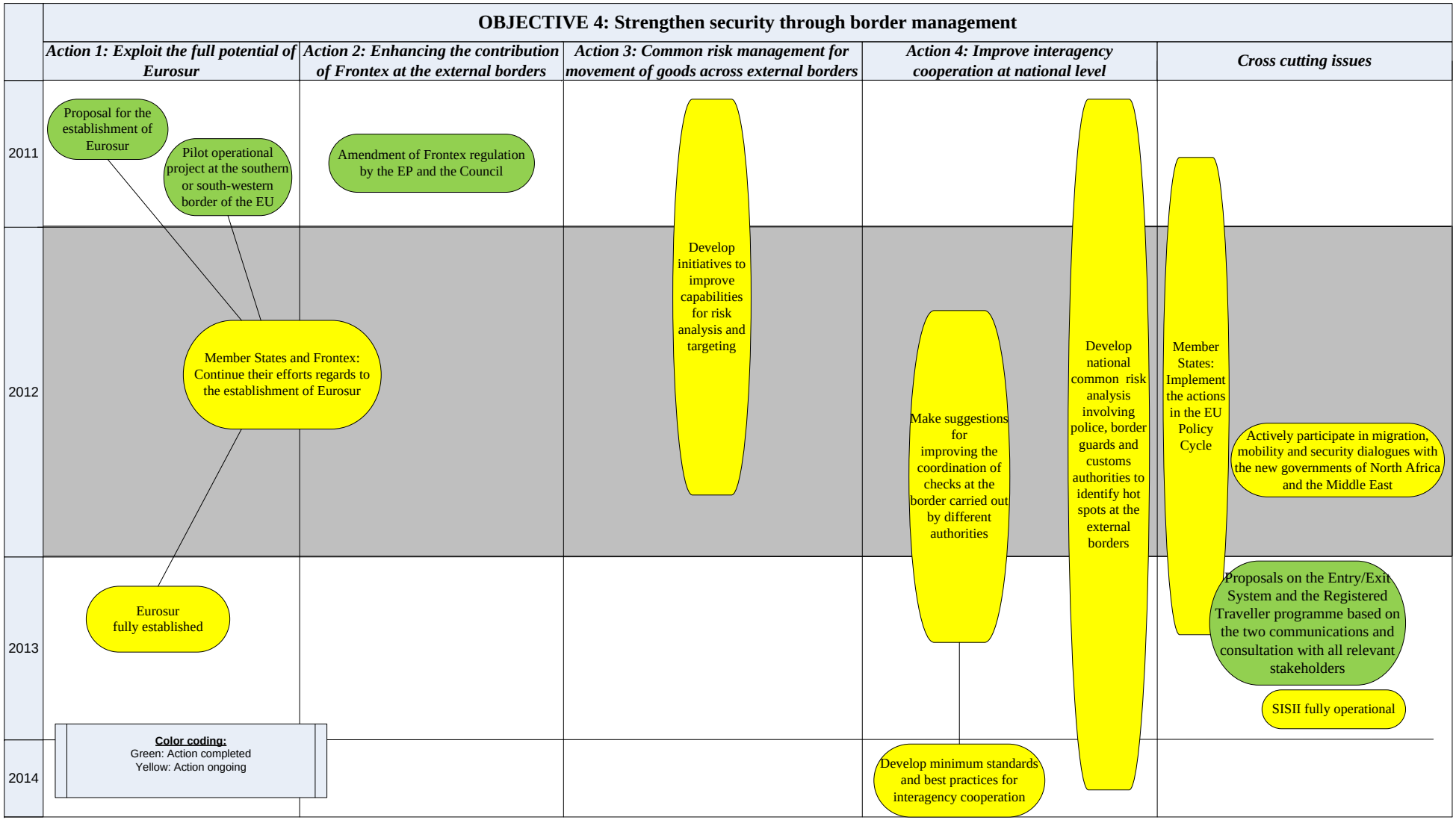
The next and last report on implementation of the ISS will be presented in mid-2014. The report will assess whether the objectives of the ISS have been met and also consider future challenges within the field of internal security.

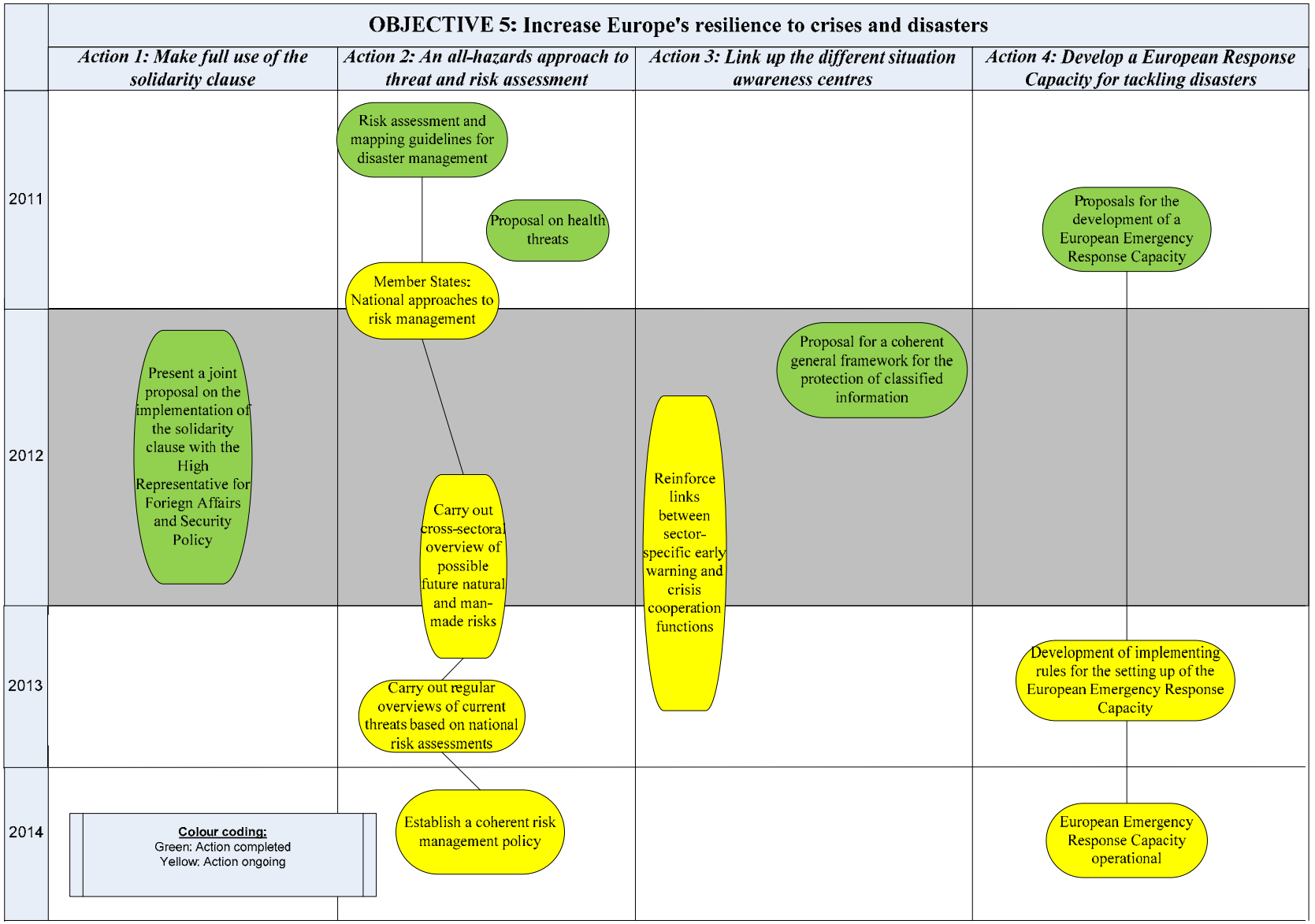
Annex 1: Graphic overview of all the planned actions for 2011-2014




OBJECTIVE 2: Prevent terrorism and address radicalisation and recruitment
Action 1: Empower communities to prevent radicalisation and recruitment
Action 2: Cut off terrorists' access to funding and materials and follow their transactions
Action 3: Protect critical infrastructure including transport
2011
2012
2013
2014
Communication on EU extraction and analysis of financial messaging data
Mid-term report on the implementation of the EU CBRN Action Plan and a review of the EU Explosives Action Plan
Impact Assessment on the establishment of an EU Terrorist Financing Tracking System
Consider creating a framework for administrative measures such as freezing of funds of persons suspected of terrorist activities inside the EU
EU radicalisation-awareness network and EU-wide conferences. Help civil society to expose, translate and challenge violent extremist propaganda
Implement action plans for preventing access to explosives and chemical, biological radiological and nuclear substances
Communication on Transport Security Policy
Options for further strengthening transport security, focusing in particular on land transport issues
Member States: Implement the Action Plan on Air Cargo Security
High Level Symposium on Countering Violent Extremism
Revisit and update the EU approach on preventing radicalisation and recruitment
Review the Directive on the designation of European Critical Infrastructure Protection
Colour coding:
Green: Action completed
Yellow: Action ongoing


OBJECTIVE 3: Raise levels of security for citizens and businesses in cyberspace
Action 1: Build capacity in law enforcement and the judiciary
Action 2: Work with industry to empower and protect citizens
Action 3: Improve capability for dealing with cyber attacks
2011
2012
2013
2014
European Cybercrime Centre feasibility study
Communication on the establishment of a cybercrime centre
Build on the work done by the EU/US working group on cyber-security and cybercrime, and initiate cooperation with other international partners
Establish an EU cybercrime centre at Europol
Develop capacities for investigation and prosecution of cybercrime
Member States: Ratify the Council of Europe Convention on Cybercrime
Member States: Implement the actions in the EU Policy Cycle
Member States: Continue with efforts to develop national cybercrime awareness and training capabilities and set up centres of excellence
Guidelines on cooperation in handling illegal content online
Establish cybercrime incident reporting arrangements and provide guidance for citizens on cyber security and cybercrime
A European Cybersecurity Strategy
Proposal for a Directive on network and information security
ENISA new mandate
Establish National/ Governmental Computer Emergency Response Teams (CERTs) and create a well-functioning network
Colour coding:
Green: Action completed
Yellow: Action ongoing


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
Cross cutting issues
2011
2012
2013
2014
Proposal for the establishment of Eurosur
Pilot operational project at the southern or south-western border of the EU
Amendment of Frontex regulation by the EP and the Council
Develop initiatives to improve capabilities for risk analysis and targeting
Member States and Frontex: Continue their efforts regards to the establishment of Eurosur
Make suggestions for improving the coordination of checks at the border carried out by different authorities
Develop national common risk analysis involving police, border guards and customs authorities to identify hot spots at the external borders
Member States: Implement the actions in the EU Policy Cycle
Actively participate in migration, mobility and security dialogues with the new governments of North Africa and the Middle East
Eurosur fully established
Proposals on the Entry/Exit System and the Registered Traveller programme based on the two communications and consultation with all relevant stakeholders
SISII fully operational
Develop minimum standards and best practices for interagency cooperation
Color coding:
Green: Action completed
Yellow: Action ongoing


OBJECTIVE 5: Increase Europe's resilience to crises and disasters
Action 1: Make full use of the solidarity clause
Action 2: An all-hazards approach to threat and risk assessment
Action 3: Link up the different situation awareness centres
Action 4: Develop a European Response Capacity for tackling disasters
2011
2012
2013
2014
Risk assessment and mapping guidelines for disaster management
Proposal on health threats
Member States: National approaches to risk management
Proposals for the development of a European Emergency Response Capacity
Present a joint proposal on the implementation of the solidarity clause with the High Representative for Foriegn Affairs and Security Policy
Carry out cross-sectoral overview of possible future natural and man-made risks
Proposal for a coherent general framework for the protection of classified information
Reinforce links between sector-specific early warning and crisis cooperation functions
Carry out regular overviews of current threats based on national risk assessments
Development of implementing rules for the setting up of the European Emergency Response Capacity
Establish a coherent risk management policy
European Emergency Response Capacity operational
Colour coding:
Green: Action completed
Yellow: Action ongoing