COUNCIL OF THE EUROPEAN UNION

Brussels, 23 November 2010

16797/10

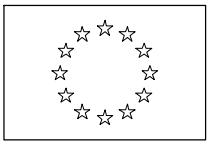
JAI 990

COVER NOTE

from:	Secretary-General of the European Commission, signed by Mr Jordi AYET PUIGARNAU, Director
date of receipt:	22 November 2010
to:	Mr Pierre de BOISSIEU, Secretary-General of the Council of the European Union
Subject:	Communication from the Commission to the European Parliament and the Council - The EU Internal Security Strategy in Action: Five steps towards a more secure Europe

Delegations will find attached document COM(2010) 673 final.

Encl.: COM(2010) 673 final



EUROPEAN COMMISSION

Brussels, 22.11.2010
COM(2010) 673 final

COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT AND THE COUNCIL

The EU Internal Security Strategy in Action: Five steps towards a more secure Europe

COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT AND THE COUNCIL

The EU Internal Security Strategy in Action: Five steps towards a more secure Europe

1. THE EUROPEAN SECURITY MODEL: WORKING TOGETHER FOR A MORE SECURE EUROPE

Most Europeans are able to go about their daily lives in relative safety. At the same time, our societies are facing serious security threats that are growing in scale and sophistication. Many of today's security challenges are cross-border and cross-sectoral in nature. No single Member State is able to respond to these threats on its own. This is something that worries our citizens and businesses. Four out of five Europeans want more action at EU level against organised crime and terrorism[1].

Much has been achieved to respond to those emerging threats and to increase Europe's security. With the Lisbon Treaty[2] in force, and with the guidance provided by the Stockholm Programme and its Action Plan[3], the EU now has the opportunity to take further determined action. The Internal Security Strategy, adopted in early 2010 under the Spanish Presidency[4], set out the challenges, principles and guidelines for how to deal with these issues within the EU and called on the Commission to propose actions for implementing the strategy. This communication – the EU Internal Security Strategy in Action - therefore builds on what Member States and EU institutions have already agreed, and proposes how we over the next four years can work together to be more effective in fighting and preventing **serious and organised crime**, **terrorism** and **cybercrime**, in strengthening the **management of our external borders** and in building **resilience to natural and man-made disasters**.

A shared agenda for common challenges

The EU's role in our internal security consists of common policies, legislation and practical cooperation in the areas of police and judicial cooperation, border management, and crisis management. In striving to reach our security objectives, the contribution from both EU internal and external policies is crucial.

The EU Internal Security Strategy in Action therefore puts forward a shared agenda for Member States, the European Parliament, the Commission, the Council and agencies and others, including civil society and local authorities. This agenda should be supported by a solid EU security industry in which manufacturers and service providers work closely

---

1 Standard Eurobarometer 71.

2 Treaty on the Functioning of the European Union (TFEU).

3 The Stockholm Programme: An Open and Secure Europe Serving and Protecting the Citizens (Council Document 17024/09); Delivering an area of freedom, security and justice: Action plan implementing the Stockholm Programme - COM(2010) 171. The Stockholm Programme is the EU's programme for justice and home affairs for the period 2010-14.

4 Council Document, 5842/2/2010, Internal Security Strategy for the European Union: Towards a European Security Model.

together with end-users. Our common efforts to deliver responses to the security challenges of our time will also contribute to strengthening and developing the European model of a social market economy put forward in the Europe 2020 strategy.

Security policies based on common values

The Internal Security Strategy in Action, and the tools and actions for implementing it must be based on common values including the rule of law and respect for fundamental rights as laid down in the **EU Charter of Fundamental Rights**[5]. Solidarity must characterise our approach to crisis management. Our counter terrorism policies should be proportionate to the scale of the challenges and focus on preventing future attacks. Where efficient law enforcement in the EU is facilitated through information exchange, we must also protect the privacy of individuals and their fundamental right to protection of personal data.

Internal security with a global perspective

Internal security cannot be achieved in isolation from the rest of the world, and it is therefore important to ensure coherence and complementarity between the internal and external aspects of EU security. The values and priorities in the Internal Security Strategy, including our commitment to promoting human rights, democracy, peace and stability in our neighbourhood and beyond, are an integral component of the approach laid down in the European Security Strategy[6]. As that Strategy recognises, relationships with our partners, in particular the United States, are of fundamental importance in the fight against serious and organised crime and terrorism.

Security should be integrated in relevant strategic partnerships, and taken into account in the dialogue with our partners when programming EU funding in partnership agreements. In particular, internal security-related priorities should feature in political dialogues with third countries and regional organisations where appropriate and relevant for combating multiple threats, such as trafficking in human beings, drugs trafficking and terrorism. The EU will moreover pay special attention to third countries and regions which may require EU and Member State support and expertise in the interests of not only the external but also internal security. With the European External Action Service it will be possible to integrate further action and expertise using the skills and knowledge of Member States, the Council and the Commission. Security expertise should be deployed to EU Delegations, particularly in priority countries, including Europol liaison officers and liaison magistrates[7]. Appropriate responsibilities and functions for these experts will be defined by the Commission and the European External Action Service.

---

5 'Strategy for the effective implementation of the Charter of Fundamental Rights by the European Union' - COM(2010) 573.

6 'European Security Strategy: A Secure Europe in a Better World' was adopted in 2003 and reviewed in 2008.

7 In accordance with Council Decision on Eurojust 2009/426/JHA, to be transposed by June 2011.

2. FIVE STRATEGIC OBJECTIVES FOR INTERNAL SECURITY

This communication identifies the most urgent challenges to EU security in the years to come. It proposes five strategic objectives and specific actions for 2011-2014 which, alongside ongoing efforts and initiatives, will help make the EU more secure.

Serious and organised crime takes a variety of forms: trafficking in human beings, drugs and firearms trafficking, money laundering and the illegal shipment and dumping of waste inside and outside Europe. Even seemingly petty crimes such as burglary and car theft, sale of counterfeit and dangerous goods and the actions of itinerant gangs are often local manifestations of global criminal networks. These crimes require concerted European action. Likewise with **terrorism**: our societies remain vulnerable to the sorts of attacks suffered with the bombings of public transport in Madrid in 2004 and in London in 2005. We must work harder and more closely to prevent new attacks recurring.

Another growing threat is **cybercrime**. Europe is a key target for cybercrime because of its advanced Internet infrastructure, the high number of users, and its internet-mediated economies and payment systems. Citizens, businesses, governments and critical infrastructure must be better protected from criminals who take advantage of modern technologies. **Border security** also requires more coherent action. With common external borders, smuggling and other cross-border illegal activity must be targeted at European level. Efficient control of the EU's external borders is thus crucial for the area of free movement.

Furthermore, in recent years we have seen an increase in the frequency and scale of natural and man-made **disasters** in Europe and in its immediate neighbourhood. This has demonstrated the need for a stronger, more coherent and better integrated European crisis and disaster response capacity as well as for the implementation of existing disaster prevention policies and legislation.

OBJECTIVE 1: Disrupt international crime networks

Despite growing cooperation between law enforcement authorities and the judiciary within as well as between Member States, international crime networks remain highly active, creating vast criminal profits. Alongside corruption and intimidation of local populations and authorities these profits are often used to penetrate the economy and undermine public trust.

To prevent crime it is therefore essential to disrupt criminal networks and combat the financial incentive which drives them. To that end, practical law enforcement cooperation should be strengthened. Authorities across all sectors and at different levels should work together to protect the economy, and criminal profits should be effectively traced and confiscated. We also need to overcome the, obstacles posed by divergent national approaches, where necessary through legislation on judicial cooperation to strengthen mutual recognition and common definitions of criminal offences and minimum levels of criminal sanctions[8].

[8] Recent proposals for Directives on trafficking in human beings, sexual exploitation of children and cybercrime represent an important first step in this direction. Article 83(1) TFEU lists the following other serious crimes: terrorism, illicit drug trafficking, illicit arms trafficking, money laundering, corruption, counterfeiting of means of payment and organised crime.

Action 1: Identify and dismantle criminal networks

To identify and disrupt criminal networks, it is essential to understand their members' methods of operating and their financing.

The Commission will therefore propose in 2011 EU legislation on the collection of **Passenger Name Records** of passengers on flights entering or leaving the territory of the EU. These data will be analysed by the authorities in Member States to prevent and prosecute terrorist offences and serious crimes.

Understanding the criminal source of finances and their movements depends on information about the owner of the companies, as well as the trusts that those finances pass through. In practice, law enforcement and judicial authorities, administrative investigative bodies such as OLAF and private sector professionals have difficulty obtaining such information. The EU should therefore consider by 2013, in the light of discussions with its international partners in the Financial Action Task Force, revising the **EU Anti-Money Laundering legislation** to enhance the transparency of legal persons and legal arrangements. To help trace the movement of criminal finances, some Member States have set up a central register of bank accounts. To maximise the usefulness of such registers for law enforcement purposes, the Commission will in 2012 develop guidelines. In order to investigate effectively criminal financial transactions, law enforcement and judicial authorities should be equipped and trained to collect, analyse and, where appropriate, share information making full use of national centres of excellence for criminal financial investigation and the European Police College (CEPOL) training programmes. The Commission will propose a strategy in this area in 2012.

Additionally, the international nature of criminal networks calls for more **joint operations** involving police, customs, border guards and judicial authorities in different Member States working alongside Eurojust, Europol and OLAF. Such operations, including **Joint Investigation Teams**[9], should be set up - where necessary at short notice - with the full support of the Commission in line with the priorities, strategic goals and plans established by the Council on the basis of relevant threat analyses[10].

Moreover, the Commission and Member States should continue to ensure effective implementation of and to report on the **European Arrest Warrant**, including its effects on fundamental rights.

Action 2: Protect the economy against criminal infiltration

Criminal networks rely on corruption to invest their profits in the lawful economy, eroding trust in public institutions and the economic system. Sustaining political will to combat corruption is of key importance. Action at EU level and sharing of best practices is therefore necessary, and the Commission will table a proposal in 2011 on how to monitor and assist **Member States' anti-corruption efforts**.

---

9 Article 88(2)(b) of the TFEU and Council Decision 2008/615/JHA on the stepping up of cross-border cooperation, particularly in combating terrorism and cross-border crime.

10 Council Conclusions 15358/10 on the creation and implementation of a EU policy cycle for organised and serious international crime.

Policies to engage governmental and regulatory bodies responsible for granting licences, authorisations, procurement contracts or subsidies should be developed (the **'administrative approach'**) to protect the economy against infiltration by criminal networks. The Commission will give practical support to Member States by establishing in 2011 a network of national contact points to develop best practices, and by sponsoring pilot projects on practical issues**.**

Counterfeit goods generate large profits for organised crime groups, distort the single market's trade patterns, undermine European industry and put the health and safety of European citizens at risk. The Commission will therefore, in the context of its forthcoming action plan against counterfeiting and piracy, take all appropriate initiatives to foster more effective **enforcement of intellectual property rights**. Meanwhile, to combat the sale of counterfeit goods on the internet, Member States' customs administrations and the Commission should adapt laws where necessary, establish contact points in national customs and exchange best practices.

Action 3: Confiscate criminal assets

To combat the financial incentive of criminal networks Member States must do all they can to seize, freeze, manage and confiscate criminal assets, and ensure that they do not return to criminal hands.

To this end the Commission will propose **legislation** in 2011 to strengthen the EU legal framework[11] on **confiscation**, in particular to allow more third-party confiscation[12] and extended confiscation[13] and to facilitate mutual recognition of non-conviction-based[14] confiscation orders between Member States.

Member States must[15] by 2014 **establish Asset Recovery Offices** equipped with the necessary resources, powers and training, and the ability to exchange information. The Commission will develop common indicators by 2013, against which Member States should evaluate the performance of these offices. Moreover, Member States should also by 2014 make the necessary institutional arrangements, for example by creating asset management offices, to ensure that frozen assets do not loose their value before they are eventually confiscated. In parallel, the Commission will in 2013 provide best practice guidance on how to prevent criminal groups from reacquiring confiscated assets.

---

11 Framework Decision 2001/500/JHA on money laundering and confiscation.

12 Third party confiscation involves the confiscation of assets that have been transferred by an investigated or convicted person to third parties.

13 Extended confiscation is the ability to confiscate assets which go beyond the direct proceeds of a crime so that there is no need to establish a connection between suspected criminal assets and a specific criminal conduct.

14 Non-conviction based procedures allow to freeze and confiscate asset irrespective of a prior conviction of the owner in a criminal court.

15 Council Decision 2007/845/JHA requires each Member State to set up at least one Asset Recovery Office on its territory.

OBJECTIVE 2: Prevent terrorism and address radicalisation and recruitment

The threat from terrorism remains significant and is constantly evolving[16]. Terrorist organisations adapt and innovate, as demonstrated by the 2008 Mumbai attacks, the attempted attack on a flight from Amsterdam to Detroit on Christmas Day 2009 and plots uncovered recently affecting several Member States. Threats now come both from organised terrorists and from so-called 'lone wolves', who may have developed their radical beliefs on the basis of extremist propaganda and found training materials on the internet. Our efforts to combat terrorism need to evolve to stay ahead of the threat with a coherent European approach including preventive action[17]. Furthermore, the EU should continue to designate critical infrastructure and put in place plans to protect those assets, including transport services and energy generation and transmission, which are essential to the functioning of society and the economy.[18]

Member States have the primary role in delivering on this objective through coordinated and effective efforts, with the full support of the Commission, and assisted by the EU Counter-Terrorism Coordinator.

Action 1: Empower communities to prevent radicalisation and recruitment

Radicalisation which can lead to acts of terrorism is best contained at a level closest to the most susceptible individuals in the most affected communities. It requires close cooperation with local authorities and civil society and empowering key groups in vulnerable communities. The core of the action on radicalisation and recruitment is - and should remain - at national level.

Several Member States are developing work streams in this area, and certain cities within the EU have developed local community-based approaches and prevention policies. These initiatives have often been successful and the Commission will continue to assist in facilitating the sharing of such experiences[19].

Firstly, by 2011, and in partnership with the Committee of the Regions, the Commission will promote the creation of an **EU radicalisation-awareness network**, supported by an online forum and EU-wide conferences, to pool experiences, knowledge and good practices to enhance awareness of radicalisation and communication techniques for challenging terrorist narratives. This network will consist of policy makers, law enforcement and security officials, prosecutors, local authorities, academics, field experts and civil society organisations, including victims groups. Member States should use ideas generated through the network to create physical and virtual community spaces for open debates which encourage credible role

---

16 For the latest figures, see Europol's 2010 Terrorism Situation and Trend (TESAT) Report.

17 EU Counter-Terrorism Strategy Doc. 14469/4/05 of November 2005 sets out a four-fold approach consisting of Prevent, Protect, Pursue and Respond. For a more detailed discussion, see 'The EU Counter-Terrorism Policy: main achievements and future challenges' - COM(2010) 386.

18 Directive on European Critical Infrastructures (2008/114/EC), part of the wider European Programme for Critical Infrastructure Protection, whose scope extends beyond protection against terrorist threats.

19 As part of the EU strategy for combating radicalisation and recruitment to terrorism (CS/2008/15175) the Commission has supported research and the establishment of the European Network of Experts on Radicalisation to study the phenomenon of radicalisation and recruitment, Member State-led projects on for example community policing, communication and radicalisation in prisons, and provided around € 5m for projects on behalf of victims and supports the network of associations of victims of terrorism.

models and opinion leaders to voice positive messages offering alternatives to terrorist narratives. The Commission will also support the work of civil society organisations which expose, translate and challenge violent extremist propaganda on the internet.

Secondly, the Commission will in 2012 organise **a ministerial conference** on the prevention of radicalisation and recruitment at which Member States will have the opportunity to present examples of successful action to counter extremist ideology.

Thirdly, in the light of these initiatives and discussions, the Commission will develop a **handbook of actions and experiences** to support Member States' efforts, from upstream prevention of radicalisation to disrupting recruitment and how to enable disengagement and rehabilitation.

Action 2: Cut off terrorists' access to funding and materials and follow their transactions

The Commission will in 2011 consider devising a framework for administrative measures under Article 75 of the Treaty as regards freezing of assets to prevent and combat terrorism and related activities. The EU action plans for preventing access to explosives (2008) and Chemical, Biological, Radiological and Nuclear (CBRN) substances (2009) need to be implemented as a priority, by way of both legislative and non legislative action. This includes the adoption of a regulation, proposed by the Commission in 2010, limiting general access to chemical precursors used to make explosives. It also means setting up a European network of specialised CBRN law enforcement units, ensuring that Member States take CBRN risks into consideration in their national planning. Another measure is to establish a law enforcement Early Warning System at Europol for incidents related to CBRN materials. These actions require close coordination with Member States, and should involve public private partnerships, where appropriate. To minimise the risk of terrorist organisations and state actors getting access to those items which could be used to make explosives and weapons of mass destruction (biological, chemical or nuclear), the EU should strengthen the dual-use export control system and its enforcement at EU borders and internationally.

Following the signature of the Terrorist Financing Tracking Programme agreement with the United States, the Commission will in 2011 **develop a policy for the EU to extract and analyse financial messaging data** held on its own territory.

Action 3: Protect transport

The Commission will further develop the EU regime for aviation and maritime security, based on continuous assessment of threats and risks. It will take into account progress in security research techniques and technology, by making use of EU programmes such as Galileo and the GMES[20] initiative on European earth observation. It will work to ensure public acceptance by seeking an ever better balance between the highest possible level of security and travel comfort, cost control, and the protection of privacy and health; and it will emphasise continued strengthening of the inspections and enforcement regime, including the monitoring of cargo operations. International cooperation is essential and can help to promote improved security standards worldwide, while ensuring efficient use of resources and limiting unnecessary duplication of security checks.

[20] GMES stands for Global Monitoring for Environment and Security.

There is scope, and justification, for a more active European approach to the broad and complex area of **land transport security**, and in particular to the security of passenger transport[21]. The Commission intends to extend existing work on urban transport security to cover (a) local and regional rail and (b) high-speed rail, including related infrastructure. To date, EU level activity has been limited to exchanging information and best practice, reflecting subsidiarity concerns and the absence of an international organisation comparable to the International Maritime Organisation or International Civil Aviation Organisation requiring a co-ordinated European approach. The Commission considers that as a first step towards further action, it would be useful to explore the establishment of a standing committee on land transport security, chaired by the Commission and involving experts in transport and in law enforcement, and of a forum for exchanging views with public and private stakeholders, taking account of previous experience in aviation and maritime transport security. Ongoing work to refine and strengthen procedures for monitoring air cargo in transit from third countries has been accelerated in the light of recent events.

Transport security issues will be addressed in detail in a communication on Transport Security Policy to be issued in 2011.

OBJECTIVE 3: Raise levels of security for citizens and businesses in cyberspace

Security of IT networks is one essential factor for a well-functioning information society. This is recognised in the recently published Digital Agenda for Europe[22] which addresses issues related to cybercrime, cyber security, safer internet and privacy as the main components in building trust and security for network users. The rapid development and application of new information technologies has also created new forms of criminal activity. Cybercrime is a global phenomenon causing significant damage to the EU internal market. While the very structure of the internet knows no boundaries, jurisdiction for prosecuting cybercrime still stops at national borders. Member States need to pool their efforts at EU level. The High Tech Crime Centre at Europol already plays an important coordinating role for law enforcement, but further action is needed.

Action 1: Build capacity in law enforcement and the judiciary

By 2013, the EU will establish, within existing structures, **a cybercrime centre**, through which Member States and EU institutions will be able to build operational and analytical capacity for investigations and cooperation with international partners[23]. The centre will improve evaluation and monitoring of existing preventive and investigative measures, support the development of training and awareness-raising for law enforcement and judiciary, establish cooperation with the European Network and Information Security Agency (ENISA) and interface with a network of national/governmental Computer Emergency Response Teams (CERTs). The cybercrime centre should become the focal point in Europe's fight against cybercrime.

At national level, Member States should ensure common standards among police, judges, prosecutors and forensic investigators in investigating and prosecuting cybercrime offences.

---

21 European Council, March 2004, Declaration on Combating Terrorism.

22 COM(2010) 245.

23 The Commission will complete a feasibility study for the centre in 2011.

In liaison with Eurojust, CEPOL and Europol, Member States are encouraged by 2013 to develop their national cybercrime awareness and training capabilities, and set up centres of excellence at national level or in partnership with other Member States. These centres should work closely with academia and industry.

Action 2: Work with industry to empower and protect citizens

All Member States should ensure that people can easily **report cybercrime incidents**. This information, once evaluated, would feed into national and, if appropriate, the European cybercrime alert platform. Building on the valuable work under the Safer Internet Programme, Member States should also ensure that citizens have easy access to guidance on cyber threats and the basic precautions that need to be taken. This guidance should include how people can protect their privacy online, detect and report grooming, equip their computers with basic anti-virus software and firewalls, manage passwords, and detect phishing, pharming, or other attacks. The Commission will in 2013 set up a real-time central pool of shared resources and best practices among Member States and the industry.

Cooperation between the public and private sector must also be strengthened on a European level through the European Public-Private Partnership for Resilience (EP3R). It should further develop innovative measures and instruments to improve security, including that of critical infrastructure, and resilience of network and information infrastructure. EP3R should also engage with international partners to strengthen the global risk management of IT networks.

The handling of illegal internet content – including incitement to terrorism – should be tackled through guidelines on cooperation, based on authorised notice and take-down procedures, which the Commission intends to develop with internet service providers, law enforcement authorities and non-profit organisations by 2011. To encourage contact and interaction between these stakeholders, the Commission will promote the use of an internet based platform called the Contact Initiative against Cybercrime for Industry and Law Enforcement.

Action 3: Improve capability for dealing with cyber attacks

A number of steps must be taken to improve prevention, detection and fast reaction in the event of cyber attacks or cyber disruption. Firstly, every Member State, and the EU institutions themselves should have, by 2012, a well-functioning **CERT**. It is important that, once they are set up, all CERTs and law enforcement authorities cooperate in prevention and response. Secondly, Member States should network together their national/governmental CERTs by 2012 to enhance Europe's preparedness. This activity will also be instrumental in developing, with the support of the Commission and ENISA, a European Information Sharing and Alert System (EISAS) to the wider public by 2013 and in establishing a network of contact points between relevant bodies and Member States. Thirdly, Member States together with ENISA should develop national contingency plans and undertake regular national and European exercises in incident response and disaster recovery. Overall, ENISA will provide support to these actions with the aim of raising standards of CERTs in Europe.

OBJECTIVE 4: Strengthen security through border management

With the Lisbon Treaty in force the EU is better placed to exploit synergies between border management policies on persons and goods, in a spirit of solidarity and sharing of responsibility[24]. In relation to movement of persons, the EU can treat migration management and the fight against crime as twin objectives of the integrated border management strategy. It is based on three strategic strands.

- An enhanced use of new technology for border checks (the second generation of the Schengen Information System (SIS II), the Visa Information System (VIS), the entry/exit system and the registered traveller programme);
- an enhanced use of new technology for border surveillance (the European Border Surveillance System, EUROSUR) with the support of GMES security services, and the gradual creation of a common information sharing environment for the EU maritime domain[25]; and
- an enhanced coordination of Member States through Frontex.

In relation to the movement of goods, the 2005 'security amendment' of the Community Customs Code[26] laid down a basis for the border to become safer and yet more open for trade of trusted goods. All cargo entering the EU is subject to risk analysis for security and safety purposes based on common risk criteria and standards. Use of resources is more efficient as they focus more on potentially risky cargos. The system relies on advance information of trade movements from economic operators, the establishment of a common risk management framework, as well as an Authorised Economic Operators scheme to be applied to all goods entering or leaving the EU. These instruments are complementary and create a comprehensive architecture, which is being further developed to cope with the increasingly sophisticated criminal organisations that Member States cannot tackle on their own.

Action 1: Exploit the full potential of EUROSUR

The Commission will present a legislative proposal to **set up EUROSUR** in 2011 to contribute to internal security and the fight against crime. EUROSUR will establish a mechanism for Member States' authorities to share operational information related to border surveillance and for cooperation with each other and with Frontex at tactical, operational and strategic level[27]. EUROSUR will make use of new technologies developed through EU funded research projects and activities, such as satellite imagery to detect and track targets at the maritime border, e.g. tracing fast vessels transporting drugs to the EU.

---

24 Article 80 of the TFEU.

25 Commission communication, 'Towards the integration of maritime surveillance: A Common information environment for the EU maritime domain', COM (2009) 538

26 Council Regulation (EC) No 648/2005 amending Council Regulation (EC) No 2913/92 establishing the Community Customs Code.

27 Commission proposals for the development of the EUROSUR system and for the development of a common information sharing environment (CISE) for the EU maritime domain are set out in COM (2008) 68 and COM(2009) 538 respectively. A six step road map for establishing the CISE was recently adopted - COM(2010) 584.

In recent years, two major initiatives on operational cooperation at the maritime borders have been launched – one on human trafficking and human smuggling under the umbrella of Frontex and the second on drugs smuggling in the framework of MAOC-N[28] and CeCLAD-M[29]. As part of the development of integrated and operational action at the EU's maritime border, the EU will launch in 2011 a pilot project at its southern or south-western border, involving those two centres, the Commission, Frontex and Europol. This pilot project will explore synergies on risk analysis and surveillance data in common areas of interest concerning different types of threats, such as drugs and people smuggling[30].

Action 2: Enhancing the contribution of Frontex at the external borders

During its operations, Frontex comes across key information on criminals involved in trafficking networks. Currently, however, this information cannot be further used for risk analyses or to better target future joint operations. Moreover, relevant data on suspected criminals do not reach the competent national authorities or Europol for further investigation. Likewise, Europol cannot share information from its analytical work files. Based on experience and in the context of the EU's overall approach to information management[31], the Commission considers that enabling Frontex to process and use this information, with a limited scope and in accordance with clearly defined personal data management rules, will make a significant contribution to dismantling criminal organisations. However, this should not create any duplication of tasks between Frontex and Europol.

From 2011 onwards, the Commission, with joint input from Frontex and Europol, will present a report by the end of each year on specific cross-border crimes such as human trafficking, human smuggling and smuggling of illicit goods. This annual report will serve as a basis for assessing the need for Frontex and its joint operations and joint operations between police, customs and other specialised law enforcement authorities to be carried out from 2012 onwards.

Action 3: Common risk management for movement of goods across external borders

Significant legal and structural developments have taken place in recent years to improve the security and safety of international supply chains and movement of goods crossing the EU border. The Common Risk Management Framework (CRMF), implemented by customs authorities, entails continuous screening of electronic pre-arrival (and pre-departure) trade data to identify the risk of security and safety threats to the EU and its inhabitants, as well as dealing with these risks appropriately. The CRMF also provides for application of more intensive controls targeting identified priority areas, including trade policy and financial risks. It also requires systematic exchange of risk information at EU level.

A challenge in the coming years is to ensure uniform, high-quality performance of risk management, associated risk analysis, and risk-based controls in all Member States. In

---

28 MAOC-N - Maritime Analysis and Operations Centre – Narcotics.

29 CeCLAD-M - Centre de Coordination pour la lutte antidrogue en Méditerranée.

30 This project will complement the other integrated maritime surveillance projects such as BlueMassMed and Marsuno, which aim to optimise the efficiency of maritime surveillance in the Mediterranean Sea, Atlantic and the northern European sea basins.

31 Overview in the area of information management in the area of freedom, security and justice - COM(2010) 385.

addition to the annual report on the smuggling of illicit goods referred to above, the Commission will develop EU level customs assessments to address common risks. Pooling information at EU-level should be used to reinforce border security. In order to strengthen customs security to the required level at external borders, the Commission will work in 2011 on options to **improve EU level capabilities for risk analysis and targeting** and come forward with proposals as appropriate.

Action 4: Improve interagency cooperation at national level

Member States should by the end of 2011 start developing **common risk analyses**. This should involve all relevant authorities with a security role, including police, border guards and customs authorities who identify hot spots and multiple and cross-cutting threats at external borders, for example repeated smuggling of people and drugs from the same region at the same border crossing points. These analyses should complement the yearly report by the Commission on cross-border crimes with joint contributions from Frontex and Europol. By the end of 2010 the Commission will finalise a study to identify best practices on cooperation between border guards and customs administrations working at EU external borders and consider the best way to disseminate them. In 2012, the Commission will make suggestions on how to **improve coordination of border checks** carried out by different national authorities (police, border guards, and customs). Further to that, by 2014 the Commission will develop, together with Frontex, Europol and the European Asylum Support Office, minimum standards and best practices for interagency cooperation. These shall particularly be applied to joint risk analysis, joint investigations, joint operations and exchanging intelligence.

OBJECTIVE 5: Increase Europe's resilience to crises and disasters

The EU is exposed to an array of potential crises and disasters, such as those associated with climate change and those caused by terrorist and cyber attacks on critical infrastructure, hostile or accidental releases of disease agents and pathogens, sudden flu outbreaks and failures in infrastructure. These cross-sectoral threats call for improvements to long-standing crisis and disaster management practices in terms of efficiency and coherence. They require both solidarity in response, and responsibility in prevention and preparedness with an emphasis on better risk assessment and risk management at EU level of all potential hazards.

Action 1: Make full use of the solidarity clause

The solidarity clause in the Lisbon Treaty[32] introduces a legal obligation on the EU and its Member States to assist each other when a Member State is the object of a terrorist attack or a natural or man-made disaster. Through the implementation of this clause the EU aims to be better organised and more efficient in managing crises, in terms of both prevention and response. On the basis of a cross cutting proposal by the Commission and the High Representative – to be presented in 2011 – the EU's collective task will be to **put the solidarity clause into practice**.

[32] Article 222 TFEU.

Action 2: An all-hazards approach to threat and risk assessment

By the end of 2010 the Commission will develop, together with Member States, EU **risk assessment** and mapping guidelines for disaster management, based on a multi-hazard and multi-risk approach, covering in principle all natural and man-made disasters. By the end of 2011, Member States should develop national approaches to risk management, including risk analyses. On this basis, the Commission will prepare, by the end of 2012, a cross-sectoral overview of the major natural and man-made risks that the EU may face in the future[33]. Furthermore the Commission initiative on health security planned for 2011 will seek to reinforce the coordination of the EU risk management and will strengthen the existing structures and mechanisms in the public health area.

On **threat assessment**, the Commission will support efforts to improve mutual understanding of the various definitions of threat levels and to improve communication when these levels are subject to change. In 2012, Member States are invited to produce their own threat assessments on terrorism and other malicious threats. From 2013 the Commission will, in liaison with the EU Counter-Terrorism Coordinator and Member States prepare regular overviews of current threats, based on national assessments.

The EU should establish by 2014 a coherent **risk management policy** linking threat and risk assessments to decision making.

Action 3: Link up the different situation awareness centres

An effective and coordinated response to crises depends on being able to quickly pull together a comprehensive and accurate overview of the situation. Information on a situation inside or outside the EU must be drawn from all relevant sources, analysed, assessed and shared with Member States and the operational and policy branches in EU institutions. With fully networked secure facilities, the right equipment and properly trained staff, the EU can **develop an integrated approach based on a common and shared appreciation in a crisis situation**.

Based on existing capabilities and expertise, the Commission will, by 2012, reinforce the links between sector-specific early warning and crisis cooperation functions[34], including those for health, civil protection, nuclear risk monitoring and terrorism, and make use of EU-led operational programmes. These arrangements will help improve links with EU agencies and the European External Action Service, including the Situation Centre, and enable better information sharing and, where required, joint EU threat and risk assessment reports.

Effective coordination between the EU institutions, bodies and agencies requires a coherent general framework to protect classified information. The Commission intends therefore to come forward with a proposal to address this in 2011.

---

33 Council Conclusions on a Community framework on disaster prevention within the EU, November 2009.

34 The Commission will continue to use and further develop ARGUS - see COM(2005) 662 - and related procedures for cross-hazard multi-sectoral crises as well as for coordination across all Commission services.

Action 4: Develop a European Emergency Response Capacity for tackling disasters

The EU should be able to respond to disasters both inside and outside the EU. Lessons learnt from recent events suggest that there is room for further improvement in terms of rapidity of deployment and appropriateness of action, operational and political coordination and visibility of the EU's response to disasters internally as well as externally.

In line with the recently-adopted disaster response strategy[35], the EU should **establish a European Emergency Response Capacity** based on pre-committed Member States' assets on-call for EU operations and pre-agreed contingency plans. Efficiency and cost-effectiveness should be improved through shared logistics, and simpler and stronger arrangements for pooling and co-financing transport assets. Legislative proposals will be tabled in 2011 to implement the key proposals.

3. IMPLEMENTING THE STRATEGY

The realisation of the Internal Security Strategy in Action is the shared responsibility of the EU institutions, Member States and EU agencies. This requires an agreed process for implementing the strategy with clear roles and responsibilities, with the Council and the Commission, in close liaison with the European External Action Service, driving progress towards meeting the strategic objectives. In particular, the Commission will support the activities of the Standing Committee on Operational Cooperation on Internal Security (COSI) to ensure that operational cooperation is promoted and strengthened, and that coordination of the action of Member States' competent authorities is facilitated.[36]

Implementation

Priorities shall be reflected both in the operational planning of EU agencies, at national level, and in Commission work programmes. The Commission will ensure that security-related activities, including security research, industrial policy and projects under EU internal security-related funding programmes, are coherent with the strategic objectives. Security research will continue to be funded under the multiannual research and development framework programme. To ensure a successful implementation the Commission will establish an internal working group. The European External Action Service will be invited to participate to ensure consistency with the wider European Security Strategy and to exploit synergies between internal and external policies, including risk and threat assessments. For the same purpose, COSI and the Political and Security Committee should work together and meet regularly.

EU funding that might be necessary for the period 2011-2013 will be made available within the current ceilings of the multiannual financial framework. For the period post-2013, 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 will consider the feasibility of setting up an Internal Security Fund.

---

35 'Towards a stronger European disaster response: the role of civil protection and humanitarian assistance' - COM(2010) 600.

36 Article 71 TFEU; see also Council Decision 2010/131/EU on setting up the Standing Committee on operational cooperation on internal security.

Monitoring and evaluation

The Commission will, with the Council, monitor progress on the Internal Security Strategy in Action. The Commission will produce an annual report to the European Parliament and the Council on the strategy on the basis of contributions from Member States and EU agencies and using as far as possible existing reporting mechanisms. The annual report will highlight the main developments for each of the strategic objectives, assessing whether actions at EU and Member State level have been effective, and making Commission recommendations as appropriate. The annual report will also include an annex describing the state of internal security. It will be produced by the Commission, supported by contributions from the relevant agencies. The report could inform annually the European Parliament and Council debates on internal security.

CONCLUDING REMARKS

Our world is changing, and so are the threats and challenges around us. The response from the European Union should evolve correspondingly. By working together to implement the actions outlined in this strategy, we are on the right path. At the same time, it is inevitable that however strong and well-prepared we are, threats can never be entirely eliminated. That is why it is all the more important that we step up our efforts.

With the Lisbon Treaty as a new legal framework, the Internal Security Strategy in Action should become the shared agenda for the EU over the next four years. Its success is dependent on the combined efforts of all EU actors, but also on cooperation with the outside world. Only by joining forces and working together to implement this strategy can Member States, EU Institutions, bodies and agencies provide a truly coordinated European response to the security threats of our time.

Annex: Summary of objectives and actions

INTERNAL SECURITY STRATEGY

OBJECTIVES AND ACTIONS

OBJECTIVES AND ACTIONS	RESPONSIBLE	TIMING
OBJECTIVE 1: Disrupt international crime networks		
Action 1: Identify and dismantle criminal networks		
Proposal on the use of EU Passenger Name Records	COM[37]	2011
Possible revision of EU anti-money laundering legislation to enable identification of owners of companies and trusts	COM	2013
Guidelines on use of bank account registers for tracing movement of criminal finances	COM	2012
Strategy on collection, analysis and sharing of information on criminal financial transactions, including training	COM with MS and CEPOL	2012
More use of Joint Investigation Teams set up at short notice	MS with COM, Europol and Eurojust	Ongoing

[37] Key to abbreviations: European Commission (COM), Member States (MS), European Police College (CEPOL), European Network and Information Security Agency (ENISA), Maritime Analysis and Operations Centre – Narcotics (MAOC-N), Centre de coordination pour la lutte antidrogue en Méditérranée (CECLAD-M), European Asylum Support Office (EASO), High Representative of the Union for Foreign Affairs and Security Policy (HR).

OBJECTIVES AND ACTIONS	RESPONSIBLE	TIMING
Action 2: Protect the economy against criminal infiltration		
Proposal on monitoring and assisting Member States anti-corruption efforts	COM	2011
Establish a network of national contact points for governmental and regulatory bodies	COM with MS	2011
Actions for enforcement of intellectual property rights and to combat sale of counterfeit goods on internet	MS and COM	Ongoing
Action 3: Confiscate criminal assets		
Proposal on third-party confiscation, extended confiscation and non-conviction-based confiscation orders	COM	2011
Establishment of effective Asset Recovery Offices and necessary arrangement for asset management	MS	2014
Common indicators for evaluating performance of Asset Recovery Offices and guidance on preventing criminals reacquiring confiscated assets	COM	2013

OBJECTIVES AND ACTIONS	RESPONSIBLE	TIMING
OBJECTIVE 2: Prevent terrorism and address radicalisation and recruitment		
Action 1: Empower communities to prevent radicalisation and recruitment		
Create an EU radicalisation-awareness network with an online forum and EU-wide conferences. Support civil society to expose, translate and challenge violent extremist propaganda	COM with Committee of Regions	2011
Ministerial conference on the prevention of radicalisation and recruitment	COM	2012
Handbook on prevention of radicalisation, disrupting recruitment and enabling disengagement and rehabilitation	COM	2013-14
Action 2: Cut off terrorists' access to funding and materials and follow their transactions		
Framework for freezing terrorist assets	COM	2011
Implement action plans for preventing access to explosives and chemical, biological radiological and nuclear substances	MS	Ongoing
Policy for EU extraction and analysis of financial messaging data	COM	2011
Action 3: Protect transport		
Communication on Transport Security Policy	COM	2011

OBJECTIVES AND ACTIONS	RESPONSIBLE	TIMING
OBJECTIVE 3: Raise levels of security for citizens and businesses in cyberspace		
Action 1: Build capacity in law enforcement and the judiciary		
Establishment of an EU cybercrime centre	Subject to the COM's feasibility study 2011	2013
Develop capacities for investigation and prosecution of cybercrime	MS with CEPOL, Europol and Eurojust	2013
Action 2: Work with industry to empower and protect citizens		
Establishment of cybercrime incident reporting arrangements and provide guidance for citizens on cyber security and cybercrime	MS, COM, Europol, ENISA and the private sector	Ongoing
Guidelines on cooperation in handling illegal content online	COM with MS and the private sector	2011
Action 3: Improve capability for dealing with cyber attacks		
Establishment of a network of Computer Emergency Response Teams in every MS and one for EU institutions, and regular national contingency plans and response and recovery exercises.	MS and EU institutions with ENISA	2012
Establishment of European information sharing and alert system (EISAS)	MS with COM and ENISA	2013

OBJECTIVES AND ACTIONS	RESPONSIBLE	TIMING
OBJECTIVE 4: Strengthen security through border management		
Action 1: Exploit the full potential of EUROSUR		
Proposal for the establishment of EUROSUR	COM	2011
Pilot operational project at the southern or south-western border of the EU	COM, Frontex, Europol, MAOC-N and CeCLAD-M	2011
Action 2: Enhancing the contribution of Frontex at the external borders		
Joint reports on human trafficking, human smuggling and smuggling of illicit goods as basis for joint operations	COM with Frontex and Europol	2011
Action 3: Common risk management for movement of goods across external borders		
Initiatives to improve capabilities for risk analysis and targeting	COM	2011
Action 4: Improve interagency cooperation at national level		
Development of national common risk analyses involving police, border guards and customs authorities to identify hot spots at the external borders	MS	2011
Suggestions for improving the coordination of checks at the border carried out by different authorities	COM	2012
Development of minimum standards and best practices for interagency cooperation	COM, Europol, Frontex, EASO	2014

OBJECTIVES AND ACTIONS	RESPONSIBLE	TIMING
OBJECTIVE 5: Increase Europe's resilience to crises and disasters		
Action 1: Make full use of the solidarity clause		
Proposal on the implementation of the solidarity clause	COM/HR	2011
Action 2: An all-hazards approach to threat and risk assessment		
Risk assessment and mapping guidelines for disaster management	COM with MS	2010
National approaches to risk management	MS	2011-12
Cross-sectoral overview of possible future natural and man-made risks	COM	2012
Proposal on health threats	COM	2011
Regular overviews of current threats	COM with MS and CTC	2013
Establish a coherent risk management policy	COM with MS	2014
Action 3: Link up the different situation awareness centres		
Reinforce links between sector-specific early warning and crisis cooperation functions	COM	2012
Proposal for a coherent general framework for the protection of classified information	COM	2011
Action 4: Develop a European Response Capacity for tackling disasters		
Proposals for the development of a European Emergency Response Capacity	COM	2011