



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 terrorism¹.

Much has been achieved to respond to those emerging threats and to increase Europe's security. With the Lisbon Treaty² in force, and with the guidance provided by the Stockholm Programme and its Action Plan³, the EU now has the opportunity to take further determined action. The Internal Security Strategy, adopted in early 2010 under the Spanish Presidency⁴, 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 Strategy⁶. 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 magistrates⁷. 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 sanctions⁸.

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 analyses¹⁰.

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 framework¹¹ on **confiscation**, in particular to allow more third-party confiscation¹² and extended confiscation¹³ and to facilitate mutual recognition of non-conviction-based¹⁴ confiscation orders between Member States.

Member States must¹⁵ 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 lose 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 evolving¹⁶. 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 action¹⁷. 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 experiences¹⁹.

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 GMES²⁰ 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 transport²¹. 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 Europe²² 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 partners²³. 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 responsibility²⁴. 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 domain²⁵; and
- an enhanced coordination of Member States through Frontex.

In relation to the movement of goods, the 2005 'security amendment' of the Community Customs Code²⁶ 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 level²⁷. 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-N²⁸ and CeCLAD-M²⁹. 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 smuggling³⁰.

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 management³¹, 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 Treaty³² 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 future³³. 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 functions³⁴, 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 strategy³⁵, 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		
<i>Action 1: Identify and dismantle criminal networks</i>		
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 Méditerranée (CECLAD-M), European Asylum Support Office (EASO), High Representative of the Union for Foreign Affairs and Security Policy (HR).

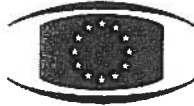
OBJECTIVES AND ACTIONS	RESPONSIBLE	TIMING
<i>Action 2: Protect the economy against criminal infiltration</i>		
Proposal on monitoring and assisting Member States anti-corruption efforts	COM	2011
Establish a network of national contact points for governmental and regulatory bodies	COM with MS	2011
Actions for enforcement of intellectual property rights and to combat sale of counterfeit goods on internet	MS and COM	Ongoing
<i>Action 3: Confiscate criminal assets</i>		
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		
<i>Action 1: Empower communities to prevent radicalisation and recruitment</i>		
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
<i>Action 2: Cut off terrorists' access to funding and materials and follow their transactions</i>		
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
<i>Action 3: Protect transport</i>		
Communication on Transport Security Policy	COM	2011

OBJECTIVES AND ACTIONS	RESPONSIBLE	TIMING
OBJECTIVE 3: Raise levels of security for citizens and businesses in cyberspace		
<i>Action 1: Build capacity in law enforcement and the judiciary</i>		
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
<i>Action 2: Work with industry to empower and protect citizens</i>		
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
<i>Action 3: Improve capability for dealing with cyber attacks</i>		
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		
<i>Action 1: Exploit the full potential of EUROSUR</i>		
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
<i>Action 2: Enhancing the contribution of Frontex at the external borders</i>		
Joint reports on human trafficking, human smuggling and smuggling of illicit goods as basis for joint operations	COM with Frontex and Europol	2011
<i>Action 3: Common risk management for movement of goods across external borders</i>		
Initiatives to improve capabilities for risk analysis and targeting	COM	2011
<i>Action 4: Improve interagency cooperation at national level</i>		
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		
<i>Action 1: Make full use of the solidarity clause</i>		
Proposal on the implementation of the solidarity clause	COM/HR	2011
<i>Action 2: An all-hazards approach to threat and risk assessment</i>		
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
<i>Action 3: Link up the different situation awareness centres</i>		
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
<i>Action 4: Develop a European Response Capacity for tackling disasters</i>		
Proposals for the development of a European Emergency Response Capacity	COM	2011



**COUNCIL OF
THE EUROPEAN UNION**

Brussels, 23 February 2010

**5842/2/10
REV 2**

JAI 90

NOTE

From:	Presidency
To:	Delegations
Subject:	Draft Internal Security Strategy for the European Union: "Towards a European Security Model"

INTRODUCTION

For fifty years the European Union, its institutions and Member States have promoted and provided freedom and security. Europe guarantees respect for human rights, the rule of law and solidarity. As Europeans, we enjoy the right to live, work and study in European countries other than our own. The removal of internal border controls in the Schengen area was an especially great step forward for Europe. In addition, technological advances have revolutionised the modes and speed of communications, with the result that not only our borders, but also our societies have opened up. Through unity in diversity, this free and prosperous Europe continues to facilitate and enrich peoples' lives.

For citizens of the European Union, security is one of the main priorities. The EU multi-annual work programmes have already provided a good pragmatic basis for strengthening operational cooperation, but now a larger consensus on the vision, values and objectives which underpin EU internal security is required.

The main crime-related risks and threats facing Europe today, such as terrorism, serious and organised crime, drug trafficking, cyber-crime, trafficking in human beings, sexual exploitation of minors and child pornography, economic crime and corruption, trafficking in arms and cross-border crime, adapt extremely quickly to changes in science and technology, in their attempt to exploit illegally and undermine the values and prosperity of our open societies.

Whilst in itself not aimed at creating any new competences, but at integrating existing strategies and conceptual approaches, and acknowledging the framework of the Stockholm Programme, the EU Internal Security Strategy is responsive to this. It demonstrates a firm commitment to continuing to make progress in the area of justice, freedom and security through a European security model which faces the following challenges: protecting rights and freedoms; improving cooperation and solidarity between Member States; addressing the causes of insecurity and not just the effects; prioritising prevention and anticipation; involving all sectors with a role to play in public protection (political, economic, social, etc.); communicating security policies to the citizens; and, finally, recognising the interdependence between internal and external security in establishing a "global security" approach with third countries.

It is thus vital that the Internal Security Strategy itself be able to adapt, both to the needs of citizens, and to the challenges of the dynamic and global twenty-first century.

The concept of internal security must be understood as a wide and comprehensive concept which straddles multiple sectors in order to address these major threats and others which have a direct impact on the lives, safety, and well-being of citizens, including natural and man-made disasters such as forest fires, earthquakes, floods and storms.

The cooperation of law-enforcement and border authorities, judicial authorities and other services in, for example, the health, social and civil protection sectors, is essential. Europe's Internal Security Strategy must exploit the potential synergies that exist in the areas of law-enforcement cooperation, integrated border management and criminal-justice systems. Indeed, these fields of activity in the European area of justice, freedom and security are inseparable: the Internal Security Strategy must ensure that they complement and reinforce one another.

Europe must consolidate a security model, based on the principles and values of the Union: respect for human rights and fundamental freedoms, the rule of law, democracy, dialogue, tolerance, transparency and solidarity.

The quality of our democracy and public confidence in the Union will depend to a large extent on our ability to guarantee security and stability in Europe and to work with our neighbours and partners to address the root causes of the internal security problems faced by the EU.

The Internal Security Strategy has been adopted in order to help drive Europe forward, bringing together existing activities and setting out the principles and guidelines for future action. It is designed to prevent crimes and increase the capacity to provide a timely and appropriate response to natural and man-made disasters through the effective development and management of adequate instruments.

1. PROTECTING PEOPLE IN EUROPE WITHIN A GLOBAL SOCIETY

The European Union (EU) in the twenty-first century consists of 500 million people across the twenty-seven countries which make up the Union. Economic growth, together with the opportunities provided by a free and democratic society based on the rule of law, generate prosperity amongst Europe's citizens – but with such opportunities also come risks, as terrorists and other types of criminals seek to abuse those freedoms in the pursuit of destructive and malicious ends. Furthermore, increased mobility of people in turn increases our common responsibility for protecting the freedoms which all citizens of the Union cherish.

Security has therefore become a key factor in ensuring a high quality of life in European society, and in protecting our critical infrastructures through preventing and tackling common threats.

There is no such thing as "zero risk" but, despite that, the Union must create a safe environment in which people in Europe feel protected. Furthermore, the necessary mechanisms must be put in place to maintain high security levels, not only within EU territory, but also as far as possible when citizens travel to third countries or find themselves in virtual environments such as the Internet.

In this context EU internal security means protecting people and the values of freedom and democracy, so that everyone can enjoy their daily lives without fear. It also reflects Europe's shared vision of today's challenges and our resolve to present a common front in dealing with those threats, where appropriate, with policies that harness the added value of the EU. The Lisbon Treaty and the Stockholm Programme enable the EU to take ambitious and concerted steps in developing Europe as an area of justice, freedom and security. Against that background, this strategy:

- sets out **the common threats and challenges** we face which make it more and more important for EU Member States and Institutions to work together in order to tackle new challenges which go beyond our national, bilateral or regional capability.

- *together we are more effective and better prepared for the threats we face*
- *an internal security strategy which reflects the values and priorities we all share*
- *actions which reflect both public security and the rights of the individual*

- sets out the **EU's common internal security policy** – and the **principles** underpinning it – in a comprehensive and transparent way.
- defines a **European Security Model**, consisting of common tools and a commitment to: a mutually reinforced relationship between security, freedom and privacy; cooperation and solidarity between Member States; involvement of all the EU's institutions; addressing the causes of insecurity, not just the effects; enhancing prevention and anticipation; involvement, as far as they are concerned, of all sectors which have a role to play in protection – political, economic and social; and a greater interdependence between internal and external security.

COMMON THREATS: The main challenges for the internal security of the EU

Crime takes advantage of the opportunities offered by a globalised society such as high-speed communications, high mobility and instant financial transactions. Likewise, there are phenomena which have a cross-border impact on security and safety within the EU. There are, therefore, a number of significant common threats which can be identified:

- **Terrorism, in any form**, has an absolute disregard for human life and democratic values. Its global reach, its devastating consequences, its ability to recruit through radicalisation and dissemination of propaganda over the Internet and the different means by which it is financed make terrorism a significant and ever-evolving threat to our security.

- *In 2007, through Eurojust, twenty-six people across Italy, France, Romania, Portugal and the UK were arrested in an international anti-terrorist operation. The organisation was planning to carry out attacks in Italy, Afghanistan, Iraq and Arab countries.*
Source: Eurojust Annual Report 2007, pp. 34-35
- *In 2008, through national, regional and EU efforts, 1009 people across thirteen countries were arrested on terrorism charges.*
Source: Europol TE-SAT Report 2009, p. 6

- *In February 2008, during Operation PIPAS (against an organisation carrying out credit card fraud), 100 people were arrested and forty-eight house searches conducted through a joint investigation between eleven countries, coordinated by Europol.*
Source: Europol Annual Report 2008, p. 24

- **serious and organised crime** is of increasing importance. In its various forms it tends to occur wherever it can reap the most financial benefit with the least risk, regardless of borders. Drug trafficking, economic crime, human trafficking, smuggling of persons, arms trafficking, sexual exploitation of

minors and child pornography, violent crimes, money-laundering and document fraud are only some of the ways in which organised and serious crime manifests itself in the EU. In addition, corruption is a threat to the bases of the democratic system and the rule of law.

- **cyber-crime** represents a global, technical, cross-border, anonymous threat to our information systems and because of that, it poses many additional challenges for law-enforcement agencies.
- **cross-border crime**, such as petty or property crime, often carried out by gangs, when it has a significant impact on the daily lives of people in Europe.
- **violence itself**, such as youth violence or hooligan violence at sports events, increases the damage already caused by crimes and can significantly harm our society.
- **natural and man-made disasters**, such as forest fires, earthquakes, floods and storms, droughts, energy shortages and major Information and Communication Technologies (ICT) breakdowns, pose safety and security challenges. In this day and age, civil protection systems represent an essential element of any modern and advanced security system.
- there are a number of other common phenomena which cause concern and pose safety and security threats to people across Europe, for example **road traffic accidents**, which take the lives of tens of thousands of European citizens every year.

THE RESPONSE TO THESE CHALLENGES

In order to cope with these phenomena, EU Member States have their own national security policies and strategies, and in response to the movement of criminals between neighbouring countries, bilateral, multilateral and regional patterns of cooperation among Member States have also been developed. However, since those efforts are not enough to prevent and fight such criminal groups and their activities, which go far beyond our borders, an EU-wide approach is increasingly required.

Joint Police and Customs Centres, such as the Centre de Coopération Policière et Douanière in Luxembourg, which support effective operational cooperation between the police, gendarmerie and customs authorities of Belgium, Germany, Luxembourg and France.

The Salzburg Forum, composed of the Interior Ministers of Austria, Bulgaria, the Czech Republic, Hungary, Poland, Slovakia, Slovenia and Romania, who meet to discuss common security issues. The Baltic Sea Task Force, including non-EU members, which was set up to combat organised crime in the Baltic Sea Region.

In July 2009, a criminal organisation of seventeen people, responsible for the counterfeiting of euros with a face value of more than EUR 16 million distributed throughout the EU, was dismantled by the Bulgarian and Spanish prosecution and police authorities, with the help of a Joint Investigation Team that included Eurojust and Europol

Source: Eurojust Press Release 3 July 2009

The Member States must continuously strive to develop instruments so that national borders, differing legislation, different languages and ways of working do not impede progress in preventing cross-border crime.

The EU has made significant progress in this area in recent years. For example, increased law-enforcement and judicial cooperation has been essential since the abolition of internal-border controls, which allows for the free movement of people within the Schengen area.

Numerous instruments for facilitating cooperation have been developed. The most relevant include:

- **analysis of future situations and scenarios: threat anticipation.** Europol and other EU Agencies produce regular threat assessments.

- **adequate response: planning, programming and handling the consequences.** Work Programmes have been developed which enable us to address the dangers to and the concerns of citizens in a methodical way. Strategies and specific work plans have also been developed on counter-terrorism, drug trafficking, trafficking in human beings, organised crime and civil protection. Furthermore, the Community Civil Protection Mechanism coordinates the response of Member States to natural and man-made disasters.
- **effectiveness in the field: the work of agencies, institutions and bodies.** A number of agencies specific to the EU have been created and these include **Europol**, whose main aims are to collect and exchange information and to facilitate cooperation between law-enforcement authorities in their fight against organised crime and terrorism, **Eurojust**, which drives coordination and increases the effectiveness of judicial authorities, and **Frontex**, which manages operational cooperation at the external borders. The EU has also created the role of the **Counter-Terrorism Coordinator**. Other bodies and networks have also been established in the fields of training, drugs, crime prevention, corruption and judicial cooperation in criminal matters.
- **tools based on mutual recognition, for information sharing and to facilitate joint investigations and operations.** Instruments based on mutual recognition include the European Arrest Warrant and provision for the freezing of assets. Data bases such as the Schengen Information System and networks have also been established for the exchange of information on criminal records, on combating hooliganism, on missing persons or stolen vehicles and on visas which have been issued or refused. The use of DNA and fingerprint data helps put a name to anonymous traces left at crime scenes. EU legal instruments facilitate operational cooperation between Member States such as the setting up of joint investigation teams, the organising of joint operations and close cooperation to ensure the security of international events, including major sporting competitions.
- **evaluation mechanisms have been developed to assess the effectiveness of our actions.** For example, peer-to-peer evaluation exercises in the field of terrorism and organised crime which have contributed to the improvement of mutual trust.

2. TOWARDS A EUROPEAN SECURITY MODEL

The success to date demonstrates great progress in the fields of justice, freedom and security in the EU. However, we must continue to pool our efforts in order to guarantee even greater protection for our citizens. The Stockholm Programme and strategies such as the European Security Strategy, the Strategy on the external dimension in the area of justice, freedom and security and the Information Management Strategy have provided a good basis for doing that.

The time has come to harness and develop common tools and policies to tackle common threats and risks using a more integrated approach: that is the main aim of the Internal Security Strategy. To achieve that aim we have chosen a security model which integrates action on law enforcement and judicial cooperation, border management and civil protection.

The principles and guidelines for action using this model are set out below.

PRINCIPLES

People in Europe expect to live in security and to enjoy their freedoms: security is in itself a basic right. The values and principles established in the Treaties of the Union and set out in the Charter of Fundamental Rights have inspired the EU's Internal Security Strategy:

- justice, freedom and security policies which are mutually reinforcing whilst respecting **fundamental rights, international protection, the rule of law and privacy.**
- **protection** of all citizens, **especially the most vulnerable**, with the focus on **victims** of crimes such as trafficking in human beings or gender violence, including victims of terrorism who also need special attention, support and social recognition.

- **transparency and accountability** in security policies, so that they can be easily understood by citizens, and take account of their concerns and opinions.
- **dialogue** as the means of resolving differences in accordance with the principles of **tolerance, respect and freedom of expression**.
- **integration, social inclusion and the fight against discrimination** as key elements for EU internal security.
- **solidarity** between Member States in the face of challenges which cannot be met by Member States acting alone or where concerted action is to the benefit of the EU as a whole.
- **mutual trust** as a key principle for successful cooperation.

STRATEGIC GUIDELINES FOR ACTION

On the basis of these principles, ten guidelines for action are laid down in order to guarantee the EU's internal security over the coming years.

-I- A wide and comprehensive approach to internal security

Internal security must be seen as encompassing a wide range of measures with both horizontal and vertical dimensions:

- **horizontal dimension:** to reach an adequate level of internal security in a complex global environment requires the involvement of law-enforcement and border-management authorities, with the support of judicial cooperation, civil protection agencies and also of the political, economic, financial, social and private sectors, including non-governmental organisations.

- likewise, we must take into account the **vertical dimension** of security at various levels: international cooperation, EU-level security policies and initiatives, regional cooperation between Member States and Member States' own national, regional and local policies.

-II- Ensuring the effective democratic and judicial supervision of security activities

Following the entry into force of the Lisbon Treaty, the involvement of the European Parliament in the development of security policies has greatly increased, which means that effective consultation at all stages is essential. National parliaments also have a greater role to play in the work of the EU through their ability to monitor application of the subsidiarity principle and through their participation in evaluation of the implementation of justice, freedom and security policies.

The European Court of Justice becomes fully competent in this area (except as regards Member States' internal law and order and their security responsibilities). Finally, the EU's accession to the European Convention on Human Rights will also contribute to improved protection for the human rights of people in Europe.

-III- Prevention and anticipation: a proactive, intelligence-led approach

Among the main objectives of the Internal Security Strategy for the EU are the prevention and anticipation of crime as well as of natural and man-made disasters, and the mitigation of their potential impact. Whilst effective

We should ensure that Member States share intelligence in time to prevent crime and bring offenders to justice.

prosecution of the perpetrators of a crime remains essential, a stronger focus on the prevention of criminal acts and terrorist attacks before they take place can help reduce the consequent human or psychological damage which is often irreparable.

Our strategy must therefore emphasise prevention and anticipation, which is based on a proactive and intelligence-led approach as well as procuring the evidence required for prosecution. It is only possible to bring successful legal action if all necessary information is available.

Furthermore, it is necessary to develop and improve prevention mechanisms such as analytical tools or early-warning systems. An applicable instrument of prevention should also be a European Passenger Names Record (PNR), that ensures a high level of data protection, for the purpose of preventing, detecting, investigating and prosecuting terrorist offences and serious crime, based on an impact assessment. This allows us to deepen our understanding of the different types of threats and their probability and to anticipate what might happen, so that we are not only prepared for the outcomes of future threats but also able to establish mechanisms to detect them and prevent their happening in the first place. For this reason, a comprehensive approach must be taken that is geared to constant detection and prevention of the threats and risks facing the EU in the various areas of internal security, and the main issues of concern to the public. A strategy to prevent and tackle threats such as organised crime is needed.

Prevention of crime means addressing the root causes and not just the criminal acts and their consequences.

Security policies, especially those of prevention, must take a broad approach, involving not only law-enforcement agencies, but also institutions and professionals at both national and local levels. Cooperation should therefore be sought with other sectors like schools, universities and other educational institutions, in order to prevent young people from turning to crime. The private sector, especially when it is involved in financial activities, can contribute to the development and effective implementation of mechanisms to prevent fraudulent activities or money laundering. Civil society organisations can also play a role in running public awareness campaigns.

EU action in the field of civil protection must be guided by the objectives of reducing vulnerability to disasters through development of a strategic approach to disaster prevention and anticipation and by further improvements in preparedness and response while recognising national responsibility. Guidelines for hazard and risk-mapping methods, assessments and analyses should be developed as well as an overview of the natural and man-made risks that the EU may face in the future. This EU-wide risk analysis should be the basis for cooperation initiatives between risk-sharing Member States and the EU in the field of civil protection and capacity planning. New risks and threats are to be identified, such as energy shortage, ICT breakdown and pandemics. Resilience of citizens as well as public and private sector to the effects of disasters are to be included in prevention policies.

-IV- Development of a comprehensive model for information exchange

An internal security policy supported by information-exchange on a basis of mutual trust and culminating in the principle of information availability. If law-enforcement authorities are to be able to prevent and act early they must have timely access to as much data as possible concerning criminal acts and their perpetrators, modus operandi, details of victim(s), vehicles used, etc.

In order to increase substantially the current levels of information exchange, we must continue to strengthen the mechanisms which build mutual trust between the authorities responsible for ensuring internal security in the EU, in order to enhance existing mechanisms, and use the Information Management Strategy to develop a secure and structured European Information Exchange Model

This model will include all the different EU databases relevant for ensuring security in the EU so that there can be interaction between them, as far as it is needed and permitted, for the purpose of providing effective information exchange across the whole of the EU and maximising the opportunities presented by biometric and other technologies for improving our citizens' security within a clear framework that also protects their privacy.

This information exchange model must always fully respect the right to privacy and protection of personal data. If a higher level of security means an increase in data exchange, it is important that that increase be managed carefully, that it be proportionate and that it respect data protection laws.

-V- Operational cooperation

The Lisbon Treaty has created the Standing Committee on Operational Cooperation on Internal Security (COSI) to ensure effective coordination and cooperation between law-enforcement and border-management authorities, including the control and protection of external borders, and when appropriate judicial cooperation in criminal matters relevant to operational cooperation. The work of this Committee will be based, above all, on national and EU threat assessments and priorities.

Stringent cooperation between EU agencies and bodies involved in EU internal security (Europol, Frontex, Eurojust, Cepad and Sitcen) must be also ensured by COSI so as to encourage increasingly coordinated, integrated and effective operations. Such players must continue to improve the provision of effective support to specialist services in Member States. In particular, Europol's capacity to support Member States' operations should be improved.

Progress should be made on the development of a cooperation framework to improve security and safety at major and mass international events.

During the Football World Cup in Germany '06, police officers from 13 European countries were on duty in Germany, wearing their regular uniforms and having been granted law-enforcement powers.

In the field of civil protection, the EU should promote an integrated approach to cover the different phases of a crisis – prevention, response, and recovery – through the implementation of European mutual assistance and solidarity.

-VI- Judicial cooperation in criminal matters

Closer cooperation between Member States' judicial authorities is essential, as is the need for EUROJUST to achieve its full potential within the framework of applicable law. At EU level, successful criminal operations and investigations must enable us to realise the potential synergies between law-enforcement and border agencies and judicial authorities in preventing cross-border crime.

-VII- Integrated border management

As well as tackling illegal immigration, integrated border management plays an important role in maintaining security. The integrated border-management mechanism must be reinforced in order, *inter alia*, to spread best practice among border guards. The feasibility of the creation of a European system of border guards must be explored on the basis of a prior analysis. Special emphasis will have to be given to the continued development of the European Border Surveillance System (EUROSUR).

The cooperation and coordination of Frontex with other EU agencies and Member States' law-enforcement agencies is a key issue for the success of this Agency.

New technologies play a key role in border management. They may make it easier for citizens to cross quickly at external-border posts through automated systems, advance registration, frequent-traveller schemes, etc. They improve security by allowing for the necessary controls to be put in place so that borders are not crossed by people or goods which pose a risk to the Union. In that context, close cooperation between law-enforcement and border-control authorities is essential. Likewise, the law-enforcement authorities should facilitate provision of the information necessary for the implementation of security measures at borders.

The entry into force of the Visa Code, further development of the Schengen Information System as well as electronic border-control systems, such as an exit-entry system, will contribute to intelligence-led integrated border management. Dialogue and cooperation with third countries of origin and transit are also essential, for example to build up border-control capacity.

-VIII- A commitment to innovation and training

It is necessary to work together to promote and develop new technologies through a common approach as well as cutting costs and increasing efficiency. In the field of technology, it is also important for the public and private sectors to work together. Building upon the outcome of research and development projects conducted under the Joint Research and Development Programme, the EU should develop technological standards and platforms tailored to its security needs.

The interoperability of different technology systems used by any agency or service must be a strategic objective so that equipment does not pose a barrier to cooperation between Member States on the sharing of information or the carrying out of joint operations.

A strategic approach to professional training in Europe: this objective is essential in establishing law-enforcement, judicial and border-management authorities that have advanced technology and are at the forefront of their specialisation, and in enabling European law-enforcement training to take a major step forward and become a powerful vehicle for promoting a shared culture amongst European law-enforcement bodies and facilitating transnational cooperation. For that to be achieved, European elements should be included in national training, and exchange programmes should be developed on the basis of the Erasmus model. To that end, highly trained European professionals sharing a similar culture will add value in the context of competition in a globalised society, as well as in the field of security. The European agencies and bodies, especially CEPOL, should play an important role.

-IX- External dimension of internal security/cooperation with third countries

A concept of internal security cannot exist without an external dimension, since internal security increasingly depends to a large extent on external security. International cooperation by the EU and its Member States, both bilaterally and multilaterally, is essential in order to guarantee security and protect the rights of our citizens and to promote security and respect for rights abroad. The EU's policies with regard to third countries need to consider security as a key factor and develop mechanisms for coordination between security and other related policies, such as foreign policy, where security issues must increasingly be taken into account in an integrated and proactive approach.

In terms of external security, the EU must not restrict itself just to cooperation between the law-enforcement agencies of Member States and other countries, especially EU neighbours. It is necessary to build relationships with other countries through a global approach to security, working closely with them and, when necessary, supporting their institutional, economic and social development. This system of working will mean establishing opportunities for dialogue through areas of mutual interest, concerns and the possibilities for cooperation that can be identified in each case.

European countries have established successful platforms in the Caribbean, Lisbon, Toulon, Accra and Dakar in cooperation with third countries in the fight against drug trafficking.

Cooperation and coordination with international organisations in the field of law enforcement, in particular with Interpol, should be enhanced. Bilateral, multilateral and regional approaches among Member States should be developed, where appropriate, to address specific threats.

The efforts to combat transnational crime outside the EU as well and to build up respect for the rule of law are of crucial importance. Cooperation with the Common European Security and Defence Policy, especially between the EU agencies and the respective missions, must therefore be enhanced even further. It is also very important to strengthen the participation of law enforcement agencies and Justice Freedom and Security bodies at all stages of civilian crisis-management missions, so that they can play a part in resolving conflicts by working together with all other services involved on the ground (military, diplomatic, emergency services, etc.). Special attention will have to be paid to "weak and failed States" so that they do not become hubs of organised crime or terrorism.

In this context, the Internal Security Strategy serves as an indispensable complement to the EU Security Strategy, developed in 2003 under the EU's Security and Defence Policy to address global risks and threats and to make a commitment to the social, political and economic development of global society as the most effective way of achieving effective and long-lasting security.

-X- Flexibility to adapt to future challenges

A broad, pragmatic, flexible and realistic approach, continually adapting to reality, taking into account risks and threats which could impact on citizens in a wider perspective, not focusing only on criminal aspects but taking into account risks of any kind which might create a security problem in the broader sense, as well as being attentive to the detection of any need to adapt to these changing circumstances and guaranteeing the highest levels of security for the people of Europe.

3. NEXT STEPS

Following the Action Plan for the implementation of the Stockholm Programme, the Commission will adopt a Communication on the Internal Security Strategy which will include action oriented proposals. Further developing, monitoring and implementing the Internal Security Strategy must become one of the priority tasks of the Standing Committee on Operational Cooperation on Internal Security (COSI). Furthermore, according to the Stockholm Programme, the Commission will consider the feasibility of setting up an Internal Security Fund to promote the implementation of the Internal Security Strategy.
