Council of the European Union

Brussels, 5 May 2015
(OR. en)

8293/15

JAI 249

COVER NOTE

From:	Secretary-General of the European Commission, signed by Mr Jordi AYET PUIGARNAU, Director
date of receipt:	30 April 2015
To:	Mr Uwe CORSEPIUS, Secretary-General of the Council of the European Union
No. Cion doc.:	COM(2015) 185 final
Subject:	The European Agenda on Security

Delegations will find attached document COM(2015) 185 final.

Encl.: COM(2015) 185 final

EUROPEAN
COMMISSION

Strasbourg, 28.4.2015
COM(2015) 185 final

COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS

The European Agenda on Security

The European Union aims to ensure that people live in an area of freedom, security and justice, without internal frontiers. Europeans need to feel confident that, wherever they move within Europe, their freedom and their security are well protected, in full compliance with the Union's values, including the rule of law and fundamental rights.

In recent years new and complex threats have emerged highlighting the need for further synergies and closer cooperation at all levels. Many of today's security concerns originate from instability in the EU's immediate neighbourhood and changing forms of radicalisation, violence and terrorism. Threats are becoming more varied and more international, as well as increasingly cross-border and cross-sectorial in nature.

These threats require an effective and **coordinated response at European level.** All the EU institutions have agreed that we need a renewed Internal Security Strategy for the coming five years.[1]

To meet this objective, this **European Agenda on Security** sets out how the Union can bring **added value** to support the Member States in ensuring security. As President Jean-Claude Juncker said in his Political Guidelines, *"Combating cross-border crime and terrorism is a common European responsibility".*[2] Member States have the front line responsibility for security, but can no longer succeed fully on their own. While respecting national responsibilities for upholding the law and safeguarding internal security, all relevant EU and national actors need to work better together to tackle cross-border threats. The European Agenda on Security must therefore be a **shared agenda** between the Union and Member States. The result should be **an EU area of internal security** where individuals are protected in full compliance with fundamental rights.

This Agenda will drive better information exchange, increased operational cooperation and mutual trust, drawing on the full range of EU policies and tools. It will ensure that the internal and external dimensions of security work in tandem. Whilst the EU must remain vigilant to other emerging threats that might also require a coordinated EU response, the Agenda prioritises **terrorism, organised crime** and **cybercrime** as interlinked areas with a strong cross-border dimension, where EU action can make a real difference.

1. WORKING BETTER TOGETHER ON SECURITY

The EU has already put in place a range of legal, practical, and support tools to underpin a European area of internal security. The strategic objectives set out in the Internal Security Strategy 2010-2014 remain valid and should continue to be pursued.[3] The Treaty of Lisbon has put the EU on the right footing to achieve this, reinforcing the legal framework to pool efforts and ensure liberty and security, internal free movement and an effective European response to cross-border threats. The Treaty strengthened the protection of fundamental rights and democratic control over Union policies on internal security, and made the European Parliament an equal co-legislator on police and judicial cooperation in criminal matters. Since 1 December 2014, police and judicial cooperation in criminal matters fall within the normal EU legal order. Judicial control by the

[1] European Council Conclusions EUCO 79/14 of 27.6.2014; European Parliament Resolution 2014/2918 of 17.12.2014; Council Conclusions of 4.12.2014 on the development of a renewed EU Internal Security Strategy.

[2] A New Start for Europe. My Agenda for Jobs, Growth, Fairness and Democratic Change. Political Guidelines for the next European Commission, 15.7.2014.

[3] Council Conclusions of 25.2.2010 on the Internal Security Strategy for the European Union: Towards a European security model; COM(2014) 154 final of 11.3.2014.

European Court of Justice and the Commission's role as Guardian of the Treaties now apply in full[4], which will ensure individuals' rights are upheld, and increase legal certainty and confidence.

Now it is time to work better and more closely together. The success of the tools that the Union has put in place in recent years relies, first of all, on responsibility-sharing, mutual trust and effective cooperation between all actors involved: EU institutions and agencies, Member States and national authorities.

To this end, the Agenda sets out a shared approach for the EU and its Member States that is comprehensive, results-oriented and realistic. To maximise the benefits of existing EU measures and, where necessary, deliver new and complementary actions, all actors involved have to work together based on **five key principles.**

First, we need to ensure full compliance with fundamental rights. Security and respect for fundamental rights are not conflicting aims, but consistent and complementary policy objectives.[5] The Union's approach is based on the common democratic values of our open societies, including the rule of law, and must respect and promote fundamental rights, as set out in the Charter of Fundamental Rights. All security measures must comply with the principles of necessity, proportionality and legality, with appropriate safeguards to ensure accountability and judicial redress[6]. The Commission will strictly test that any security measure fully complies with fundamental rights whilst effectively delivering its objectives. The impact of any new initiative on free movement and the protection of personal data must be fully in line with the proportionality principle, and fundamental rights. This is a shared responsibility for all EU and Member State actors. EU bodies such as the EU Agency for Fundamental Rights (FRA) and the European Data Protection Supervisor have an important role in assisting EU institutions and other EU agencies to uphold and promote our values.

Second, we need more transparency, accountability and democratic control, to give citizens confidence. The European Parliament has taken up its full role as co-legislator, ensuring democratic oversight. The specific role of national parliaments in the area of freedom, security and justice[7] is reflected in the Commission's wider commitment to a renewed political dialogue with national parliaments. Twice a year the Commission will update the European Parliament and the Council on the implementation of this Agenda. The Commission will also develop performance indicators for key EU instruments. To further enhance transparency and participation, the Commission will set up in 2015 an EU Security Consultative Forum bringing together Member States, the European Parliament, EU agencies, and representatives of civil society, academia and the private sector.

Third, we need to ensure better application and implementation of existing EU legal instruments. One of the Commission's priorities will be to help Member States to further develop mutual trust, fully exploit existing tools for information sharing and foster cross-border operational cooperation between competent authorities. Peer evaluation and effective monitoring of the implementation of European measures both have a role to play.

---

4 Subject to the specific terms of Protocol 22 as concerns Denmark and Protocol 21and 36 as concerns the United Kingdom and Ireland.

5 Article 6 of the Charter of Fundamental Rights and Judgment of the European Court of Justice of 8 April 2014, in joined cases C-293/12 and C-594/12, paragraph 42.

6 Article 52(1) of the Charter of Fundamental Rights; judgment of the European Court of Justice of 8 April 2014, quoted above.

7 Article 69 TFEU.

Fourth, we need a more joined-up inter-agency and a cross-sectorial approach. Given the increasing nexus between different types of security threats, policy and action on the ground must be fully coordinated among all relevant EU agencies, in the area of Justice and Home Affairs[8] and beyond. These agencies provide a specialised layer of support and expertise for Member States and the EU. They function as information hubs, help implement EU law and play a crucial role in supporting operational cooperation, such as joint cross-border actions. It is time to deepen cooperation between these agencies. The Commission will launch a reflection on how to maximise their contribution, through closer inter-agency cooperation, coordination with Member States, comprehensive programming, careful planning and targeting of resources.

Specific actions in a wide range of EU policies contribute to security objectives, including in the area of transport, finance, customs, education, maritime security policy, information technologies, energy and public health. Actions in the Digital Single Market and the European Neighbourhood Policy will complement and reinforce the European Agenda on Security. The Agenda builds also on existing sectoral strategies that can contribute – directly or indirectly – to a high level of security.[9]

This Agenda has to be seen in conjunction with the forthcoming European Agenda on Migration,[10] which will address issues directly relevant to security, such as smuggling of migrants, trafficking in human beings, social cohesion and border management.

Fifth, we need to bring together all internal and external dimensions of security. Security threats are not confined by the borders of the EU. EU internal security and global security are mutually dependent and interlinked. The EU response must therefore be comprehensive and based on a coherent set of actions combining the internal and external dimensions, to further reinforce links between Justice and Home Affairs and Common Security and Defence Policy. Its success is highly dependent on cooperation with international partners. Preventive engagement with third countries is needed to address the root causes of security issues.

We should maximise the added value of existing policy **dialogues on security** conducted by the EU – and the linked EU financial instruments and activities – with enlargement and neighbourhood countries, key strategic partners, and relevant international and regional organisations. Dialogues should be extended to include priorities such as cooperation in fight against transnational organised crime and terrorism, smuggling of migrants and trafficking in human beings. This should lead to specific joint action plans with key third countries and be reflected in the targeted use of EU financial instruments.

---

8 The EU law enforcement agency Europol, the EU agency for the management of operational cooperation at the external borders Frontex, the EU judicial cooperation agency Eurojust, the European police college Cepol, the EU agency for large-scale IT systems eu-LISA, and the European Monitoring Centre for Drugs and Drug Addiction EMCDDA.

9 EU Maritime Security Strategy (Council Conclusions of 24.6.2014); the Cyber Security Strategy (JOIN(2013) 1 final of 7.2.2013); the Strategy for Customs Risk Management (COM(2014) 527 final of 21.8.2014); the Strategic Framework for European Cooperation in Education and Training (Council Conclusions of 12.5.2009); the EU Youth Strategy (COM(2009) 200 final of 27.4.2009); EU strategy to step up the fight against cigarette smuggling and other forms of illicit trade in tobacco products (COM(2013) 324 final of 6.6.2013). The Agenda also complements ongoing initiatives such as the review of strategic export controls (COM(2014) 244 final of 24.4.2014).

10 The European Agenda on Migration is one of the initiatives of the Commission Work Programme for 2015.

EU Delegations in third countries are important for the dialogues on security, and therefore require expertise and stronger local coordination. The ongoing **deployment of security experts** in EU Delegations in European Neighbourhood Policy countries and other targeted non-EU countries should be a priority. We should also explore how to make full use of the expertise of Member State law enforcement officials seconded to non-EU countries, as well as consider the feasibility of posting EU agencies' liaison officers and magistrates in key third countries.

Mutual legal assistance (MLA) agreements with third countries (United States, Japan[11]) are key instruments for international judicial cooperation, and the Commission will assess whether it is necessary to develop other bilateral or multilateral agreements with key third countries.

Finally, the Union should further develop its relations with international organisations, such as the UN, the Council of Europe, and Interpol, and use multilateral forums such as the Global Counter Terrorism Forum more actively to promote best practices and meet common objectives.

External aspects of security will be more comprehensively developed in the framework of the Strategic Review that the High Representative for Foreign Affairs and Security Policy/Vice-President of the Commission has initiated, as well as in the ongoing review of the European Neighbourhood Policy.

2. STRENGTHENING THE PILLARS OF THE EU ACTION

In operational terms, working better and more closely together means, above all, that all actors involved – be it EU institutions and agencies, Member States or national law enforcement authorities – fully implement existing instruments. This also calls, where necessary, for new or more developed tools to maximise the added value of EU measures for information exchange, operational cooperation and other support.

2.1 Better information exchange

The Union provides a number of tools to facilitate the exchange of information between national law enforcement authorities. They should be used to the full by the Member States. Where there are still critical gaps, we should assess whether additional EU tools are necessary.

The **Schengen Information System** (SIS) is the most widely used information-sharing instrument today. Competent national authorities can use it to consult alerts on wanted or missing persons and objects, both inside the Union and at the external border. The SIS was upgraded in early 2015 to improve information exchange on terrorist suspects and to reinforce the efforts of Member States to invalidate the travel documents of persons suspected of wanting to join terrorist groups outside the EU. The Commission will look into possibilities to help Member States to implement travel bans set at national level. The Commission will evaluate the SIS in 2015-2016 to assess whether new operational needs require legislative changes, such as introducing additional categories to trigger alerts.

[11] Council Decisions 2009/820/CFSP of 23.10.2009 and 2010/88/CFSP/JHA of 30.11.2009.

To further strengthen security at the external borders, there should be fuller use of the SIS together with Interpol's database on **Stolen and Lost Travel Documents (SLTD)**. The Commission will help Member States to use automated border controls with checks of the SIS and the SLTD, and it will continue to monitor if Member States implement their obligation to provide data to the SLTD.[12] The Commission is also updating the handbook for border guards to better target border checks and to promote the full use of the SIS and the SLTD.

Member States bear responsibility for the entire Union when they control their part of the external borders. This is why **common risk indicators** should support the work of national border authorities when conducting checks on persons. On the basis of contributions from Member States, the Commission will finalise a first set of common risk indicators, in respect of foreign terrorist fighters, in the first half of 2015. Europol and Frontex will play a key role in the future maintenance of these risk indicators. The Commission will continue to monitor the effectiveness of the Schengen Border Code, and examine any emerging need for improvements.

Common high standards of **border management**, in full respect of the rule of law and of fundamental rights, are essential to preventing cross-border crime and terrorism. The European Agenda on Migration will further address border management. The revised proposal on Smart Borders which the Commission intends to present by the beginning of 2016 will help increase efficiency and effectiveness.

Complementary measures to improve security in relation to the **movement of goods** also contribute to tackle illegal activities at the border, such as trafficking of weapons, illicit drug and cigarette smuggling or illegal currency transfers. The Customs Advance Cargo Information System provides customs authorities with advance notification for security risk assessment of cargo arriving into and departing from the EU. This system should be fully exploited by ensuring effective sharing of information between customs and with other law enforcement authorities. The Anti-Fraud Information System (AFIS) provides a crucial platform for exchange of customs anti-fraud information supporting customs law enforcement to fight cross border crime.[13]

The **Prüm** framework[14] is another example of an information exchange tool at EU level that is yet to be used to its full potential. It can offer automated comparison of DNA profiles, fingerprint data and vehicle registration data – which are key to detecting crime and building an effective case. The system is falling short of its potential because at this stage only a limited number of Member States have implemented their legal obligations and integrated the network with their own systems. This impedes the overall effectiveness of the Prüm framework in catching and prosecuting criminals. Member States have received significant financial and technical support for implementation. The Commission will treat this area as a priority in using its powers to ensure the correct implementation of EU law.

12 Common Position 2005/69/JHA of 24.1.2005.
13 AFIS is run by the European Anti-Fraud Office (OLAF).
14 Council Decision 2008/615/JHA of 23.6.2008 and Council Decision 2008/616/JHA of 23.6.2008.

Of course, legal implementation of EU instruments at national level is not enough. The tools of the EU security framework will only take full effect when national law enforcement agencies feel confident in existing instruments and share information readily. The proposal for a new legal basis for **Europol**,[15] currently before the co-legislators, seeks to enhance Europol's analytical capabilities, trigger operational action on the part of Member States, and reinforce the agency's data protection regime. Member States should use Europol as their channel of first choice for law enforcement information sharing across the EU. Europol's Secure Information Exchange Network Application (SIENA) allows Member States to exchange information in a swift, secure and user-friendly way with each other, with Europol, or with third parties that have a cooperation agreement with Europol. The active use of information exchange instruments also needs the right interface between the EU's tools and national law enforcement systems, such as **Single Points of Contact**. Member States must put the right structures in place at national level to integrate and coordinate the work of the relevant authorities.

Tracking the movements of offenders is key to disrupting terrorist and criminal networks. It is now urgent that the co-legislators finalise their work on the establishment of an **EU Passenger Name Record (PNR)** system for airline passengers that is fully compatible with the Charter of Fundamental Rights while providing a strong and effective tool at EU level. Analysis of PNR information provided at the time of booking and check-in helps to identify high risk travellers previously unknown to law enforcement authorities. PNR data has proven necessary to identify high risk travellers in the context of combatting terrorism, drugs trafficking, trafficking in human beings, child sexual exploitation and other serious crimes. Once adopted, the PNR Directive will ensure better cooperation between national systems and reduce security gaps between Member States. Common risk indicators for the processing of PNR data will help to prevent criminals escaping detection by travelling through another Member State. Europol and Frontex can again play a key role in developing and distributing such risk indicators on the basis of information received from Member States.

The EU has concluded **PNR agreements** with the United States, Canada and Australia. Such cooperation has real added value in identifying and apprehending foreign terrorist fighters, drug traffickers or travelling sex offenders. The Union’s future approach to the exchange of PNR data with non-EU countries will take into account the need to apply consistent standards and specific fundamental rights protections. Once the European Court of Justice has issued its opinion on the draft PNR Agreement with Canada, and based on the Court's conclusions, the Commission will finalise its work on legally sound and sustainable solutions to exchange PNR data with other third countries, including by considering a model agreement on PNR setting out the requirements third countries have to meet to receive PNR data from the EU.

[15] COM(2013) 173 final of 27.3.2013. Part of the proposal was replaced by the proposal for a Regulation establishing a European Union agency for law enforcement training Cepol (COM(2014) 465 final of 16.7.2014).

Common rules on **data protection** will enable law enforcement and judicial authorities to cooperate more effectively with each other, as well as building confidence and ensuring legal certainty. Agreement by the end of 2015 on the Data Protection reform as a whole is key, and particularly on the proposal for a Data Protection Directive for police and criminal justice authorities. In addition, the European Union is negotiating with the United States government an international framework agreement ("Data Protection Umbrella Agreement") in order to ensure a high level of protection of personal data transferred between the EU and the US for the prevention, detection, investigation and prosecution of criminal offences, including terrorism.

Communications data can also contribute effectively to the prevention and prosecution of terrorism and organised crime. Following the judgment of the European Court of Justice on the Data Retention Directive[16], the Commission will continue monitoring legislative developments at national level.

Fighting criminal organisations active in several EU countries also requires information exchange and cooperation between judicial authorities. 26 Member States are using the **European Criminal Records Information System** (ECRIS), which allows for information exchange on previous convictions for EU nationals. However, it does not work effectively for non-EU nationals convicted in the EU. The Commission will accelerate the work already under way to improve ECRIS for non-EU nationals and is ready to contribute to its effective implementation.

The real-time availability of existing data across Member States is an area for future work on information exchange. In response to a request made by the Council[17], the Commission will assess the necessity and potential added value of a **European Police Record Index System (EPRIS)** to facilitate cross-border access to information held in national police records. In the meantime, the Commission is supporting the launch of a pilot project planned by a group of Member States to establish the mechanisms for automated cross-border searches in national indexes on a 'hit'/'no hit' basis.[18]

Finally, the **Maritime Common Information Sharing Environment** (CISE) will enable interoperability of relevant security data in areas such as piracy, terrorism, arms and drugs smuggling, human trafficking, environmental pollution, civil protection and natural disasters between competent authorities within their existing mandates.

*EU action must focus first of all on the **full implementation of rules already in place** – such as the Prüm framework – and **adoption of proposals already on the table** – such as the EU PNR Directive, the Europol Regulation and the Data Protection reform. This will already constitute a major step forward by putting in place a clear, secure, and properly-regulated set of tools to give the authorities the information they need – as long as these tools are used to their full potential. **Key instruments** like the Schengen Information System, the Schengen Border Code and ECRIS should also be kept under review and any gaps in coverage filled.*

16 Judgment of the European Court of Justice of 8 April 2014, quoted above.

17 See Council Conclusions of 4.12.2014, mentioned above.

18 The automated reply to a search in the index would only indicate if data is available ('hit') or not ('no hit') in the police record of another country. In case of a hit, additional data would need to be requested using existing channels for police cooperation.

2.2 Increased operational cooperation

The Lisbon Treaty provides legal and practical arrangements to make operational cooperation between authorities of different Member States effective.

Through the **EU Policy Cycle for serious and organised crime**, Member States authorities coordinate common priorities and operational actions. The Standing Committee on Operational Cooperation on Internal Security (COSI) plays a central role. The Policy Cycle provides a methodology for an intelligence-led approach to internal security, based on joint threat assessments coordinated within Europol. It targets available resources in view of immediate, mid-term and long-term security threats and risks. The Policy Cycle should be used more by Member States to launch concrete law enforcement operations to tackle organised crime, including with third countries. Operation Archimedes, coordinated by Europol in September 2014 to address a variety of serious crimes across Member States and third countries, provided a practical example of how this can help.[19] Such operations should be evaluated regularly in order to identify best practices for future action.

EU agencies play a crucial role in supporting operational cooperation. They contribute to the assessment of common security threats, they help to define common priorities for operational action, and they facilitate cross-border cooperation and prosecution. Member States should make full use of the support of the agencies to tackle crime through joint action. Increased cooperation between the agencies should also be promoted, within their respective mandates. The revised cooperation agreement between Europol and Frontex, once implemented, will allow such synergies by enabling the two agencies to share personal data with appropriate data protection safeguards. Eurojust and Europol should further enhance their operational cooperation.

Based on contributions from EU agencies and in close cooperation with Member States, the Commission has acquired specific expertise in developing **risk assessments.** The Commission has developed Risk Assessment and Mapping Guidelines for Disaster Management[20] as well as Guidelines on the Assessment of Member States' Risk management capability, and conducted risk assessments on explosives in air cargo from third countries and on passenger checks at airports in Member States. The Commission intends to apply this methodology in other areas, such as critical infrastructures, money laundering and terrorist financing, and to assess in particular the cascading effects of systemic risks.

Coordination hubs can facilitate a coherent **European response during crises and emergencies**, avoiding unnecessary and expensive duplication of efforts. In the framework of the **Solidarity Clause**[21], a Member State can request EU assistance in case of crisis, including terrorist attacks. The EU Emergency Response Coordination Centre acts as the main 24/7 coordination and support platform for all crises under the Union

[19] Operation Archimedes took place in September 2014; law enforcement authorities from 34 countries took part; coordination was provided by Europol. The operation targeted organised criminal groups and resulted in over 1000 arrests made across Europe.

[20] SEC(2010) 1626 final of 21.12.2010.

[21] Article 222 TFEU.

Civil Protection Mechanism[22], the Solidarity Clause and the Integrated Political Crisis Response arrangements (IPCR). It relies on inputs from the Commission, EU agencies and Member States. With increasing and new disaster risks, Member States and the Commission need to work together to fully implement and operationalize the 2013 civil protection legislation,[23] including following up on the Sendai Framework for Disaster Risk Reduction 2015-2030.[24] The EU should continue reinforcing crisis management preparedness for a more efficient and coherent EU response to crises sparked by criminal acts, impacting on borders, public security and critical systems. This includes running more joint field exercises.

Cross-border tools are available at EU level to support operational cooperation. **Joint Investigation Teams** (JITs) provide a ready-made framework for cooperation between Member States, set up for a fixed period to investigate specific cases. JITs are a successful tool that should be used more regularly and draw systematically on the agencies. Where criminal cases have an international dimension, Member States should make use of the possibility to involve third countries in JITs. Similarly, **Joint Customs Operations** (JCOs) allow customs authorities to tackle cross-border crime in the customs area, using a multi-disciplinary approach. The Commission and the Member States have jointly developed common risk criteria for security risk assessments by customs of international goods movements. In line with the EU Strategy and Action Plan for customs risk management, the EU should continue to strengthen its capacity for detection of illicit trade in goods or cash.

Cooperation in **networks of national specialised units** is another effective way of ensuring operational cooperation across borders. Cross-border cooperation between national Financial Intelligence Units (FIUs) and national Asset Recovery Offices (AROs) helps to combat money laundering and to access the illicit proceeds of crime. Similarly, c**ustoms** authorities cooperate in the management of risks in the international supply chain while facilitating legitimate trade.[25] Enhanced coordination and cooperation between Coast Guard Functions performed at national level reinforces maritime security. Experts from different parts of the enforcement chain in the Member States also cooperate through various networks to tackle environmental crime. The Commission will support this approach in other areas.

Police and Customs Cooperation Centres (PCCCs) in border regions bring together on one site the law enforcement authorities of different Member States. The EU supports the growing number of PCCCs with co-funding and annual conferences to exchange experience and best practices. Although most of the information exchanged in PCCCs does not concern serious and organised crime, it is important that information on such cases is passed up to the national level and, where appropriate, to Europol.

As regards **regional cooperation**, the necessity and added value of measures under Article 89 TFEU relating to the operation of the competent authorities of one Member State in the territory of another could be considered after evaluating the existing tools, including hot pursuit and cross-border surveillance.

---

22 The Union Civil Protection Mechanism was established in 2001 to foster cooperation among national civil protection authorities across Europe.

23 Decision 1313/2013/EU of 17.12. 2013 on a Union Civil Protection Mechanism.

24 This encompasses making local and national level infrastructure more disaster-resilient, promoting innovation, creating more effective linkages between research, policy and operations, developing partnerships with the private sector and mainstreaming disaster risk management.

25 COM(2014) 527 final of 21.8.2014.

Judicial cooperation in criminal matters also relies on effective cross-border instruments. Mutual recognition of judgments and judicial decisions is a key element in the security framework. Tools like the European Arrest Warrant have proved effective but other instruments, such as freezing and confiscation of criminal assets, are not yet used systematically in all appropriate cases. National judges should take advantage of the European Judicial Network (EJN) for the execution of European Arrest Warrants and freezing and confiscation orders. The implementation of the European Investigation Order will add a further essential tool. Member States should use Eurojust more often to coordinate cross-border investigations and prosecutions. Eurojust can also be a great help for complex mutual legal assistance requests with countries outside the EU, especially with the network of the Eurojust contact points.

Finally, establishing the European Public Prosecutor's Office will provide a new dimension to the specific issue of protecting losses to the EU budget from criminal activity.

The EU's institutions, agencies and existing cooperation tools already provide an effective set of instruments to make EU security policy an ***operational reality****. More synergies between EU agencies, more systematic coordination and full use of tools like the Joint Investigation Teams, can make a real difference in the prevention, detection and reaction to security threats.*

2.3 Supporting action: training, funding, research and innovation

In addition to information exchange and operational cooperation, the EU provides support to security-related actions through training, funding and the promotion of security-related research and innovation. The Commission seeks to target this support in a strategic and cost-effective way.

The effectiveness of cooperation tools relies on law enforcement officers in Member States knowing how to use them. Training is essential to allow authorities on the ground to exploit the tools in an operational situation. The European police college **CEPOL** organises courses, defines common curricula on cross-border cooperation and coordinates exchange programmes. The current legislative proposal on CEPOL would further reinforce its ability to prepare police officers to cooperate effectively and to develop a common law enforcement culture.[26] CEPOL should adapt its yearly training programmes to the priorities set out in this Agenda. National police academies should also use EU funding to make **cross-border cooperation** an integral part of their own training and practical exercises. Training for the judiciary and judicial staff should also be better aligned with EU priorities, building on existing structures and networks and with the support of the European Judicial Training Network (EJTN) and of the European e-Justice Portal and e-learning. The Commission has also established a European Security Training Centre that enables Member States to improve their capabilities in detecting and identifying illicit nuclear or radioactive materials for threat prevention.

[26] COM(2014) 465 final of 16.7.2014.

The recently created **Internal Security Fund** provides a responsive and flexible tool to address the most crucial challenges up to 2020. This Agenda provides strategic direction for the Fund, with a focus on those areas where financial support will bring most value added. Priority uses of the fund should include updating national sections of the Schengen Information System, implementing the Prüm framework and setting up Single Points of Contact. The Fund should also be used to strengthen cross-border operational cooperation under the EU Policy Cycle for serious and organised crime, and to develop 'exit strategies' for radicalised persons with the help of best practices exchanged in the Radicalisation Awareness Network. Other EU funding instruments, such as Horizon 2020 for research and innovation[27], the European Structural and Investment Funds, the EU Justice Programmes, the Customs 2020 Programme and financial instruments for external action can also contribute, in their respective areas, to support the priorities of the Agenda on Security.

The **mid-term review** of the Internal Security Fund in 2018 will provide an opportunity to take stock of how funding has helped to deliver the priorities of the Agenda and re-prioritise as necessary.

Research and innovation is essential if the EU is to keep up-to-date with evolving security needs. Research can identify new security threats and their impacts on European societies. It also contributes to creating social trust in research-based new security policies and tools. Innovative solutions will help to mitigate security risks more effectively by drawing on knowledge, research and technology. Horizon 2020 can play a central role in ensuring that the EU's research effort is well targeted, including factoring in the needs of law enforcement authorities by further involving **end-users** at all stages of the process, from conception to market. More focus on innovation is also needed in the area of **civil protection,** where the creation of a knowledge centre in the framework of the EU Emergency Response Coordination Centre, as well as the building of a community of users, will contribute to building an interface between research and end-users in Member States.

The Commission recently mandated European standardization organisations to produce a **'privacy by design'** standard aimed to promote the embedding of high standards of security and fundamental rights at the earliest stage in technological design. Compliance with this standard will ensure that EU security products and services respect individuals' rights and thereby enhance consumer confidence.

A competitive **EU security industry** can also contribute to the EU's autonomy in meeting security needs. The EU has encouraged the development of innovative security solutions, for example through standards and common certificates.[28] The Commission is considering further action, such as on alarm systems and airport screening equipment, to remove barriers to the Single Market and to enhance the competitiveness of the EU security industry in export markets.

---

27 Horizon 2020, the EU Research and Innovation programme for the period from 2014 to 2020, section on "Secure societies – Protecting freedom and security of Europe and its citizens".

28 COM(2012) 417 of 26.7.2012.

Forensic science is critical to law enforcement and prosecution. Law enforcement and judicial authorities must be confident that the forensic data they rely on is of high quality, including if the data comes from another Member State. It is therefore important to ensure that the forensic data exchanged through information exchange systems, such as the Prüm framework for fingerprints and DNA profiles, can be effectively used in court. A **European Forensic Area**, to align the processes of forensic service providers in Member States, would foster cooperation and ensure confidence. The Commission will first engage with the relevant stakeholders in a stocktaking exercise end then define priorities and possible measures to achieve this goal. This may include exchange of best practices and the definition of common minimum standards.

*Security should be a **key priority** in a wide range of **funding instruments, research** and **innovation programmes** as well as **training initiatives**. Existing priorities should be adjusted as required.*

3. THREE PRIORITIES

In the coming five years, this framework for working better and more closely together should be deployed to address three main priorities for European security, while it is adaptable to other major threats that might evolve in future.

- Terrorist attacks in Europe – most recently in Paris, Copenhagen, Brussels –have highlighted the need for a strong EU response to **terrorism** and **foreign terrorist fighters**. European citizens continue to join terrorist groups in conflict zones, acquiring training and posing a potential threat to European internal security on their return. While this issue is not new, the scale and the flow of fighters to ongoing conflicts, in particular in Syria, Iraq and Libya, as well as the networked nature of these conflicts, are unprecedented.

- At the same time, **serious and organised cross-border crime** is finding new avenues to operate, and new ways to escape detection. There are huge human, social and economic costs – from crimes such as trafficking in human beings, trade in firearms, drug smuggling, and financial, economic and environmental crime. Organised crime groups involved in the smuggling of migrants exploit the vulnerabilities of people seeking protection or better economic opportunities and are responsible for the loss of lives in the name of profit. Organised crime also feeds terrorism and cybercrime through channels like the supply of weapons, financing through drug smuggling, and the infiltration of financial markets.

- Finally, **cybercrime** is an ever-growing threat to citizens' fundamental rights and to the economy, as well, as to the development of a successful Digital Single Market.[29] As commerce and banking shift online, cybercrime can represent a huge potential gain to criminals and a huge potential loss to citizens. Cybercriminals can act from outside the Union to harm critical infrastructures and simultaneously target a large number of victims across Member States, with minimum effort and risk. Similarly, threats such as those posed by cyber-terrorism and hybrid threats could increase in the years to come. Criminals abuse

[29] Internet users in the EU remain very concerned about cybercrime. 85% agree that the risk of becoming a victim of cybercrime is increasing (Eurobarometer on cyber-security published in February 2015).

- anonymisation techniques and anonymous payment mechanisms for illicit online trade in drugs or weapons, for criminal transactions and money laundering. Cybercrime is also closely linked to child sexual exploitation, with a growing and alarming trend of child abuse through live streaming.

Terrorism, organised crime and cybercrime are the three **core priorities** which are highlighted in this Agenda for immediate action. They are clearly **interlinked and cross-border threats**, and their multi-faceted and international dimension shows the need for an effective and coordinated response at EU level.

3.1 Tackling terrorism and preventing radicalisation

Citizens and Member States expect the EU's support in fighting terrorism and radicalisation and facilitating coordination and cooperation between relevant authorities. **Europol** has developed a growing expertise on terrorism issues and this should be taken a step further by bringing together its anti-terrorism law enforcement capabilities, pooling resources and maximising the use of already existing structures, services and tools available to the Agency with a view to achieving economies of scale. This could be brought together as a **European Counter-Terrorism Centre** within Europol to step up the support provided at EU level for Member States, within a secure environment with the highest confidentiality in its communication.

The Centre would include (1) Europol's Focal Point Travellers on foreign terrorist fighters and related terrorist networks, (2) the EU-US Terrorist Financing Tracking Programme (TFTP), (3) FIU.NET, the decentralised computer network supporting Financial Intelligence Units, which will be embedded in Europol in 2016, and (4) Europol's existing capabilities on firearms and explosive devices. **Eurojust** should be fully involved in the activities of the Centre to improve coordination of investigations and prosecutions. Such a Centre would operate strictly within the legal mandate of Europol, and would not affect Member States' sole responsibility for safeguarding national security, nor the role of the EU Intelligence Analysis Centre (INTCEN) in the area of intelligence-based assessment of the terrorist threat.

The **Internet Referral Unit** (EU IRU), to be established in Europol by July 2015, would also be part of the Centre. The Unit will build upon Europol and Member States' experience to act as an EU centre of expertise, helping Member States to identify and remove violent extremist content online, in cooperation with industry partners.

Furthermore, the Commission will launch in 2015 an **EU-level Forum** with IT companies to bring them together with law enforcement authorities and civil society. Building upon the preparatory meetings organised in 2014, the Forum will focus on deploying the best tools to counter terrorist propaganda on the internet and in social media. In cooperation with IT companies, the Forum will also explore the concerns of law enforcement authorities on new encryption technologies.

Tracking financial operations can be central to identifying terrorist networks, as terrorists rely on finance for travel, training and equipment. FIUs can help to identify financial operations of terrorist networks across borders and detect their financial backers. The EU-US Terrorist Financing Tracking Programme (TFTP) allows Member States to request a search of financial data when there is reasonable suspicion of terrorist

activity. To date, TFTP has provided leads relating to numerous terrorist suspects and their support networks. Member States and their competent authorities should make more active use of the possibilities under the TFTP. The forthcoming embedment of FIU.NET with Europol will further enhance capabilities in the fight against terrorist financing.

The Commission will also explore the need for and possible benefits of additional measures in the area of **terrorism financing**, including measures relating to the freezing of terrorist assets under Article 75 TFEU, to illicit trade in cultural goods, to the control of forms of payment such as internet transfers and pre-paid cards, to illicit cash movements and to the strengthening of the cash controls Regulation[30].

The EU needs a solid **criminal justice response** to terrorism, covering investigation and prosecution of those who plan terrorist acts or are suspected of recruitment, training, and financing of terrorism as well as incitement to commit a terrorist offence. Many Member States already have or plan laws to criminalise these acts. More coherent laws against foreign terrorist fighters-related offences across the EU would address the cross-border practical and legal challenges in the gathering and admissibility of evidence in terrorism cases, and to deter departures to conflict zones. The Commission will launch an impact assessment in 2015 with a view to updating the **2008 Framework Decision on Terrorism** in 2016.[31] UN Security Council Resolution 2178 requires states to criminalise travel to a conflict zone for terrorist purposes , helping to build a common understanding of the offences of foreign terrorist fighters.The new legislative framework should open the door to intensified **cooperation with third countries** on foreign terrorist fighters – building on recent positive experiences of cooperation with Turkey.

One way to disrupt the activities of terrorist networks is to make it more difficult to attack targets and to access and deploy dangerous substances, such as Chemical, Biological, Radiological and Nuclear materials and explosives precursors. Protecting **critical infrastructures**, such as transport infrastructure, and **soft targets,** for instance at mass public events, present real challenges for law enforcement, public health authorities and civil protection authorities. The EU and the Member States cooperate to assess risks, evaluate mitigation strategies, gather best practices and produce guidance. The Commission helps practitioners by developing handbooks to assist their daily work, for example in the area of aviation security.

Terrorism in Europe feeds on extremist ideologies. EU action against terrorism therefore needs to **address the root causes of extremism** through preventive measures. Throughout the EU, the link between radicalisation and extremist violence is becoming ever clearer. Extremist propaganda has been shown to lead foreign terrorist fighters from Europe to travel abroad to train, fight and commit atrocities in combat zones, and to threaten the internal security of the EU on their return. Strengthening the EU's own strategic communication with common narratives and factual representation of conflicts is an important aspect of the EU's response.

[30] Regulation 1889/2005 of 26.10.2005.

[31] This will take into account the negotiations on an Additional Protocol supplementing the Council of Europe Convention on the Prevention of Terrorism.

The EU **response to extremism** must not lead to the stigmatisation of any one group or community. It must draw on common European values of tolerance, diversity and mutual respect, and promote free and pluralist communities. The EU must cut the support base of terrorism with a strong and determined counter-narrative. The Commission will ensure enforcement of relevant EU legislation in this area.[32] It will assess any gaps in legislation and support the monitoring of online hate speech and other actions. It will also assist Member States in developing proactive investigation and prosecution practices on the ground. EU funding will increasingly be used to support specific training of public officials and encourage monitoring, reporting and recording of incidents of hate crime and hate speech.

Education, **youth participation, interfaith** and **inter-cultural dialogue**, as well as **employment** and **social inclusion**, have a key role to play in preventing radicalisation by promoting common European values, fostering social inclusion, enhancing mutual understanding and tolerance. Inclusive education can make a major contribution in tackling inequalities and preventing marginalization. Youth work, volunteering, sport and cultural activities are particularly effective in reaching out to young people. Against this background, the Commission will prioritise combating radicalisation, marginalisation of youth and promoting inclusion with a series of concrete actions under the Strategic Framework for European Cooperation on Education and Training ("ET 2020"), the European Youth Strategy, the EU Work Plan for Sport and the Culture Work Plan.

To underpin these actions, the Commission will mobilise funding under the Erasmus+ and Creative Europe programmes, inter alia by increased support to mobility of teachers and youth workers, youth exchanges and volunteering, strategic partnerships in the field of education and youth policy, transnational networks, school cooperation platforms, joint projects on citizenship education, and collaborative partnerships in sport. Furthermore, the European Social Fund provides financial support to Member States to promote social inclusion, combatting poverty and any discrimination. The Commission will also initiate further research under Horizon 2020 to gain a better understanding of the causes and manifestations of radicalisation.

The EU has been a pioneer in helping communities under pressure to learn from other parts of the Union. In 2014, the Commission set out ten areas to structure efforts to address the root causes of extremism.[33] The **Radicalisation Awareness Network** (RAN), an EU-wide umbrella network launched in 2011, connects organisations and networks across the Union, linking up more than 1000 practitioners directly engaged in preventing radicalisation and violent extremism. The network enables the exchange of experience and practices facilitating early detection of radicalisation and the design of preventive and disengagement strategies at local level.

The Commission is now in the process of setting up a **RAN Centre of Excellence**. This will act as an EU knowledge hub to consolidate expertise and foster the dissemination and exchange of experiences and cooperation on anti-radicalisation. It will add a new practical dimension to the cooperation between stakeholders on anti-radicalisation.

---

32 Framework Decision 2008/913/JHA of 28.11.2008, Directive 2000/43/EC of 29.6.2000, Directive 2000/78/EC of 27.11.2000, and Directive 2010/13/EU of 10.3.2010.

33 COM(2013) 941 final of 15.1.2014.

The EU has also felt the effects of radicalisation in its neighbourhood. To counter this, RAN will develop its work with stakeholders in third countries, with a priority on Turkey and countries in the Western Balkans, Middle East and North Africa. At the same time, coordination should be ensured with EU external action, for example through a Round of Eminent Persons from Europe and the Muslim world, to encourage intellectual exchanges and a wider dialogue between societies.

Local actors are the people in direct contact with those most at risk of radicalisation. They need to be properly equipped to recognise the signs of radicalisation and assess what intervention might be needed, and to ensure the right cooperation with community leaders. Many Member States have launched training focused on the traditional target groups of law enforcement personnel and prison staff – and the evidence of prison as a focal point for radicalisation makes this a priority. With the support of the European Organisation of Prison and Correctional Services (EUROPRIS), the Commission will promote the exchange of best practices and training on de-radicalisation and prevention of radicalisation in prisons. Training and support can usefully be extended to other actors, such as social workers, teachers and healthcare workers. The RAN will also help to develop similar approaches for de-radicalisation and disengagement ('exit strategies').

The Commission and the European External Action Service will cooperate with the EU Counter-terrorism Coordinator to maintain an overview of all the instruments at the Union's disposal and will closely monitor their implementation.

Actions:

- *Reinforcing Europol`s support functions by bringing together its anti-terrorism law enforcement capabilities in a European Counter-Terrorism Centre within Europol;*
- *Launching an EU Forum with IT companies to help counter terrorist propaganda and addressing concerns about new encryption technologies;*
- *Taking further measures to improve the fight against terrorism financing;*
- *Addressing any gaps in the response to incitement to hatred online;*
- *Reviewing the Framework Decision on terrorism with a proposal in 2016;*
- *Re-prioritising the EU's policy frameworks and programmes for education, youth and culture;*
- *Focusing on the prevention of radicalisation in prisons, and developing effective disengagement/de-radicalisation programmes;*
- *Launching the RAN centre of excellence and extending anti-radicalisation work with Turkey, the Western Balkans, the Middle East and North Africa.*

3.2 Disrupting organised crime

The **EU Policy Cycle for serious and organised crime** has succeeded in delivering a more coordinated strategic direction and joint operations on the ground. **Neighbourhood countries** are already associated to the Policy Cycle, and their involvement in operational activities of the Policy Cycle should be intensified. One of the priorities of the Policy Cycle is to disrupt organised criminal networks involved in smuggling of migrants by stepping up cross-border investigations with the support of EU agencies. The joint operation MARE coordinated by Europol is a good example of how the Union can become more effective in identifying and tackling organised crime groups involved in the smuggling of migrants.

The primary goal of organised crime is profit. Law enforcement must therefore have the capacity to turn the spotlight on the **finance of organised crime**, often inherently linked to corruption, fraud, counterfeiting and smuggling. International criminal networks use legal business structures to conceal the source of their profits, so action is needed to address the infiltration of the licit economy by organised crime.

The recently-agreed Anti-Money Laundering package[34] will help to identify and follow up on suspicious transfers of money and facilitate the efficient exchange of information between Financial Intelligence Units (FIUs). The Commission will support the implementation of this legislation to make it harder for criminals to abuse the financial system, and work on a supranational assessment of risks that will address, among others, terrorist financing and virtual currencies. It will also establish a coherent policy towards third countries that have deficient anti-money laundering and counter-terrorist financing regimes. Linking up the work of national **Asset Recovery Offices** will improve cross-border freezing and confiscation of criminal assets. It is necessary to align and reinforce the powers of FIUs, as differences in their roles hinders cooperation and information exchange. Eurojust could also offer more expertise and assistance to the national authorities when conducting financial investigations. M**utual recognition of freezing and confiscation orders** should be improved. In 2016, as requested by the co-legislators, the Commission will issue a feasibility study on common rules on non-conviction based confiscation of property derived from criminal activities.

Recent terrorist attacks have focused attention on how organised criminals are able to access and trade **firearms** in Europe, even military-grade firearms, in large numbers. The decision on who can hold a firearm and when they can be used is a societal choice for Member States. However, differences in national legislation are an obstacle to controls and police cooperation. As a priority, a common approach is needed on the neutralisation and de-activation of firearms to prevent reactivation and use by criminals. The Commission will review the existing legislation on firearms in 2016 to improve the sharing of information (e.g. by uploading information on seized firearms in Europol's information system), to reinforce traceability, to standardise marking, and to establish common standards for neutralising firearms. In the context of the on-going evaluation, the Commission will consider whether to include weapons designed for self-protection (alarm weapons) in the new provisions, as well as any other relevant aspect.

Trafficking of firearms has a critical **external dimension**, given that many illegal firearms in the EU have been imported from neighbouring countries where large stockpiles of military weapons remain. The recent operational action plan with the Western Balkans should be implemented to the full and, if effective, be replicated with other neighbours, in particular countries in the Middle East and North Africa.[35]

---

34 4th Anti-Money Laundering Directive and Regulation on information accompanying transfers of funds; see related Commission proposals COM(2013) 45 final of 5.2.2013 and COM(2013) 44 final of 5.2.2013.

35 December 2014 operational action plan between the EU and the Western Balkans on the fight against illegal trafficking in firearms.

The market for **illicit drugs** remains the most dynamic of criminal markets, with a recent trend being the proliferation of new psychoactive substances (NPS). The production of NPS increasingly takes place in the EU and points to the urgency of adopting a new EU legislative framework. The EU should continue to support Member States' activities in fighting illicit drugs, including prevention, using the expertise of the European Monitoring Centre for Drugs and Drug Addiction (EMCDDA) and Europol. The Commission will assess the progress made in implementing the EU Drugs Action Plan 2013-2016, which also frames the EU external policy in the field of drugs, with its focus on drug demand and drug supply reduction. On this basis, the Commission will decide whether to propose a new EU Action Plan for the period 2017-2020.

One of the major problems the EU is currently facing is that criminal networks exploit individuals' need for protection or their desire to come to Europe. The more that such criminal smuggling can be stopped early, the less the risk of human tragedies as seen recently in the Mediterranean. Preventive action against the facilitation of irregular migration requires better information gathering, sharing and analysis. The key lies in **cooperation against the smuggling of migrants** inside the EU and with third countries. The EU should make this a priority in its partnership with third countries, offering assistance to help key transit countries to prevent and detect smuggling activities as early as possible. Reinforced action against the smuggling of migrants between the EU and key third countries will be part of the forthcoming European Agenda on Migration.

Trafficking in human beings is an extremely pernicious but highly lucrative form of crime. The EU has a dedicated legal and policy framework[36] to maximise cooperation and make this a priority for bodies such as Europol and Eurojust. Through a coordinated and coherent approach, the current strategy has contributed to the combating of trafficking in human beings at regional, national, European and international levels. The Commission intends to develop a post-2016 strategy that builds on the existing framework.

Environmental crimes can cause significant damage to the environment and human health, reduce government revenues and impose clean-up costs on taxpayers, for instance by illegal shipments and subsequent dumping of hazardous waste. The illegal trade in wildlife threatens biodiversity, as well as, in source regions such as in Africa, sustainable development and regional stability.[37] The Commission will consider the need to strengthening compliance monitoring and enforcement, for instance by increasing training for enforcement staff, support for relevant networks of professionals, and by further approximating criminal sanctions throughout the EU.

Local authorities have a critical role to play in tackling organised crime, alongside the work of law enforcement and judicial authorities. Organised crime often thinks globally but acts locally and thus requires a multi-disciplinary approach to effectively prevent and counter it. The EU has accordingly developed an approach that combines tools at administrative level to prevent infiltration in the public sector or the economy. In many cases, local authorities are in the front line to identify and prevent the infiltration of the licit economy by criminal networks, for example when allocating public tenders or granting casino licences, and they should have the tools to share information with other

[36] Directive 2011/36/EU of 5.4.2011; COM(2012) 286 final of 19.6.2012.
[37] COM (2014) 64 final of 7.2.2014.

public administrative authorities or law enforcement. More prominence should also be given to the work of the **European Union Crime Prevention Network**. With financial support from the EU, the network shares best practices in preventing crime.

Preventing and fighting **corruption** in the European Union requires a comprehensive approach. The Commission published the first EU Anti-Corruption Report in 2014. The report provides an EU-wide overview, identifies trends and best practice, and analyses developments in each EU Member State, aiming to support governments, civil society and other stakeholders in preventing and combating corruption. The EU has taken a series of steps to fight corruption: policy and monitoring initiatives (including recognising the economic cost in the European semester), legislation, and funding programmes.

Actions:

- *Extending the work of the EU Policy Cycle to neighbouring countries;*
- *Reviewing possible measures for non-conviction based confiscation;*
- *Reviewing legislation on firearms with proposals in 2016;*
- *Adopting a post-2016 strategy on human trafficking;*
- *Launching joint actions and cooperation strategies with key third countries to combat smuggling of migrants;*
- *Reviewing existing policy and legislation on environmental crime, for proposals in 2016.*

3.3 Fighting cybercrime

Cybersecurity is the first line of defence against cybercrime. The 2013 EU Cybersecurity Strategy focuses on identifying high-risk areas, working with the private sector to close loopholes, and providing specialised training. An important element in implementing the Strategy will be the swift adoption of the proposal for a Directive on network and information security.[38] The implementation of this Directive would not only promote better cooperation between law enforcement and cybersecurity authorities, but also provide for cyber-security capacity building of competent Member States' authorities and cross-border incident notification. The EU Agency for Network and Information Security also contributes to the EU's response to cybersecurity issues by working towards a high level of network and information security.

Ensuring full implementation of existing EU legislation is the first step in confronting cybercrime. The 2013 Directive[39] on attacks against information systems criminalises the use of tools such as malicious software and strengthens the framework for information exchange on attacks. The 2011 Directive[40] on child sexual exploitation approximates national legislation to prevent child sexual abuse online. The Commission is working with the Member States to ensure correct implementation of these Directives. Rules also have to be kept up to date. Citizens are concerned about issues like payment fraud. However, the 2001 framework decision combating fraud and counterfeiting of non-cash means of payments[41] no longer reflects today's realities and new challenges such as

38 COM(2013) 48 final of 7.2.2013.
39 Directive 2013/40/EU of 12.8.2013.
40 Directive 2011/92/EU of 13.12.2011.
41 Council Framework Decision 2001/413/JHA of 28.5.2001.

virtual currencies and mobile payment. The Commission will assess the level of implementation of the current legislation, consult relevant stakeholders and assess the need for further measures.

Cybercrime is by its nature borderless, flexible and innovative. In prevention, detection and prosecution, law enforcement has to be able to match and anticipate the ingenuity of the criminals. Cyber criminality requires competent judicial authorities to rethink the way they cooperate within their jurisdiction and applicable law to ensure swifter cross-border access to evidence and information, taking into account current and future technological developments such as cloud computing and Internet of Things. Gathering electronic evidence in real time from other jurisdictions on issues like owners of IP addresses or other e-evidence, and ensuring its admissibility in court, are key issues. It also requires highly-skilled law enforcement staff able to keep pace with the considerable increase in the scope, sophistication and types of cybercrime.

Clear rules are needed to ensure that data protection principles are respected in full, while law enforcement gains access to the data it needs to protect the privacy of citizens against cybercrime and identity theft. **Cooperation** with the **private sector** is also of critical importance, with public-private partnerships to structure a common effort to fight online crime. The response to cybercrime (e.g. phishing) must involve the entire chain: from Europol's European Cybercrime Centre, Computer Emergency Response Teams in the Member States concerned by the attack, to internet service providers that can warn end-users and provide technical protection. In short, cybercrime demands a new approach to law enforcement in the digital age.

Europol's **European Cybercrime Centre** can build on its existing work to become a central information hub for law enforcement in this area. The Council of Europe's Budapest Convention on Cybercrime, ratified by most Member States, remains the international standard for cooperation and a model for national and EU legislation. All Member States should ratify the Convention. Initiatives such as the EU-US Working Group on Cybersecurity and Cybercrime and the Global Alliance against Child Sexual Abuse Online show the value of international cooperation and should be promoted, whilst synergies with cyber capacity building actions funded under external assistance instruments should be enhanced.

Eurojust should continue to facilitate the exchange of best practice and identify the challenges regarding the collection and use of e-evidence in investigations and prosecutions of Internet-facilitated crimes, with the necessary safeguards. The Commission will work to ensure that relevant modern means of communication (such as voice-over internet protocol) can be covered by judicial investigation, prosecution and mutual legal assistance. Different standards on the admissibility of evidence must not constitute an impediment to the fight against terrorism and organised crime.

Actions:

- *Giving renewed emphasis to implementation of existing policies on cybersecurity, attacks against information systems, and combatting child sexual exploitation;*
- *Reviewing and possibly extending legislation on combatting fraud and counterfeiting of non-cash means of payments to take account of newer forms of crime and counterfeiting in financial instruments, with proposals in 2016;*
- *Reviewing obstacles to criminal investigations on cybercrime, notably on issues of competent jurisdiction and rules on access to evidence and information;*
- *Enhancing cyber capacity building action under external assistance instruments.*

4. THE WAY FORWARD

The European Agenda on Security sets out the actions necessary to deliver a high level of internal security in the EU. It must be a **shared agenda**. Its successful implementation depends on the political commitment of all actors concerned to do more and to work better together. This includes EU institutions, Member States and EU agencies. It requires a global perspective with security as one of our main external priorities. The EU must be able to react to unexpected events, seize new opportunities and anticipate and adapt to future trends and security risks.

The Commission invites the European Parliament and the Council to endorse this Agenda as the renewed Internal Security Strategy, with a view to the forthcoming European Council of June 2015. The Commission invites active engagement in implementation of the Agenda, in close cooperation with all relevant actors. It invites EU institutions and Member States to take this agenda as the **basis for cooperation and joint action by the Union** on security in the next five years, with the aim to develop a genuine area of EU internal security.