EUROPEAN
COMMISSION

Brussels, 26.7.2017
SWD(2017) 278 final

PART 1/2

COMMISSION STAFF WORKING DOCUMENT

Comprehensive Assessment of EU Security Policy

Accompanying the document

COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE EUROPEAN COUNCIL AND THE COUNCIL

Ninth progress report towards an effective and genuine Security Union

{COM(2017) 407 final}

Comprehensive Assessment of EU Security Policy

Table of Contents

I. EXECUTIVE SUMMARY

1. Introduction

This comprehensive assessment reviews the Union's action in the area of internal security. The focus is on currently applicable EU policies and instruments, as well as those developed over the last 15 years. The aim is to assess if the acquis and supporting activities are satisfactory when set against today's reality, and to identify any gaps requiring further action[1].

The assessment is based on detailed reports and studies focussing on the implementation, functioning and effectiveness of Justice and Home Affairs policies developed over recent years.[2] The assessment builds on specific reviews, evaluation, assessments and reports of individual policies and instruments with a view to presenting a broad overview. A combination of sources were used including: a comprehensive, in house, desk analysis; replies to a questionnaire addressed to Member States and EU agencies in the Justice and Home Affairs (JHA) area and stakeholder dialogues with Member States, EU agencies, the European Parliament, national Parliaments, civil society, think tanks, academia and industry representatives.[3]

The scope of the assessment reflects the three priorities of the European Agenda on Security for the period 2015-2020[4], confirmed by the Council in its Conclusions on the Renewed European Union Internal Security Strategy[5]: **tackling terrorism and preventing radicalisation, disrupting organised crime** and **fighting cybercrime**. The assessment covers the main areas of EU action: policy framework and strategies, legislation, soft law supporting measures (e.g. training, funding, research and innovation) and other measures to foster information exchange and operational cooperation. When directly relevant, EU policies and instruments from other policy areas are also covered.

In the area of freedom, security and justice, competences are shared between the EU and the Member States. This assessment fully recognises that Member States have the operational responsibility for ensuring security in the EU, with EU institutions and agencies performing a vital supporting role as set out in the Treaties and in secondary legislation. The assessment covers actions taken at EU level to support Member States It does not analyse the performance of individual Member States in implementing EU legislation nor the contribution that specific Member States make to wider EU internal security.

2. Main findings

2.1. Overall assessment

The comprehensive assessment broadly confirms an **overall positive appreciation** of EU action in this area and highlights the relevance of the main instruments of EU security policy. The broad consensus amongst stakeholders is that the Union's intervention and tools are both

1 The comprehensive assessment covers policy developments until 1 July 2017.
2 https://ec.europa.eu/home-affairs/e-library/documents_en.
3 For the scope and methodology of the assessment and summaries of the events of the consultation process please see Annex I Methodology and Annex VI Workshops of SWD (2017) (26.07.2017).
4 COM(2015) 185 final.
5 Council document 9798/15.

appropriate and have delivered positive outcomes and results. The assessment found no substantial negative side effects or significant duplications or overlaps.

Need for proper and full implementation

Although the comprehensive assessment reveals overall satisfaction with the acquis, some concerns were raised relating to the lack of full and effective implementation, which could in some cases limit the beneficial impact of the acquis and constrain the full exploitation of existing instruments. Recent EU policy initiatives in the security area have revealed the need for proper implementation of the acquis. Existing instruments and tools at EU level have been developed over a long period of time, under different applicable Treaty frameworks and in response to different needs, resulting in a complex set of frameworks and tools. This in turn has made it difficult for end-users to have complete knowledge of the instruments available with knock on effects for their ability and willingness to use them. The need for proper implementation of already adopted legislation was confirmed during the dialogue with Member States on counter-terrorism and organised crime, and during the exchange of views with the European Parliament's Committee on Civil Liberties, Justice and Home Affairs (LIBE) and national Parliaments.

The assessment revealed that full implementation was undermined by a number of factors including: the complexity of the rules governing the use of EU instruments; the costs incurred by Member States (e.g. for complex IT systems) and lack of specialised human resources in the relevant services in Member States. Lack of resources both at technical and financial level were identified as an important reason for the delay of implementing information systems by Member States.

The very limited enforcement powers of the Commission and the Court of Justice until 1st of December 2014 with regard to Police and Judicial cooperation in criminal matters is likely to have contributed to an uneven implementation of the various instruments across different Member States. Following the entry into force of the Lisbon Treaty, the Commission and the Court of Justice have acquired full powers to ensure the correct application of EU law on Police cooperation and Judicial cooperation in criminal matters and are now actively using these enforcement powers[6] to ensure more consistent implementation and better understanding across the EU.

[6] The Commission invited all Member States to notify their national measures for transposing the instruments applicable to them by 15 March 2015. Some Member States failed to notify any measures to transpose a number of these instruments. In December 2015 the Commission used the EU-Pilot framework to contact those which had failed to notify complete measures for transposing the following instruments[6]: Council Framework Decision 2006/960/JHA (also called the 'Swedish initiative'); Council Framework Decision 2008/841/JHA on the fight against organised crime; Framework Decision 2009/315/JHA on exchange of information extracted from criminal records between Member States (ECRIS). In 2016 the enforcement work continued with the launch of first infringement procedures concerning instruments of the former "third pillar". In this context,the Commission initiated one case for non-communication of measures implementing the 'Swedish initiative' on simplifying the exchange of information and intelligence between EU law enforcement authorities (Council Framework Decision 2006/960/JHA), and five cases for failure to comply with the Prüm Decisions on information-sharing to combat terrorism and serious crime (Decisions 2008/615/JHA and 2008/616/JHA). In 2017 three reasoned opinions were issued in the Prüm cases.

2.2 Fostering operational cooperation and building trust

EU level action is judged to have delivered clear added value in information exchange and operational cooperation by helping to build "cross border" trust among stakeholders. The assessment found that EU measures have contributed to the improvement of national capabilities in the fight against organised crime, including cybercrime, and terrorism through a combination of training, exchange of best practices, and cross-border cooperation in the framework of the EU Policy cycle for serious international and organised crime.

A key element emerging from the assessment is the central importance of EU policies to building mutual trust between Member States' law enforcement and judicial authorities as well as towards EU agencies. This is especially the case in the fight against terrorism where traditional channels for structured information exchange and operational cooperation have been bilateral, rather than at EU level. Stakeholders cited EU tools such as: peer evaluations, twining and the exchange of best practices as particularly valuable.

The assessment also highlighted the importance in areas such as cybersecurity of strengthened partnership between public authorities and industry. Similar engagement with non-traditional security actors such as local practitioners, academics, and researchers is vital to the prevention of violent radicalisation.

2.3 Exploiting synergies and pooling capacities

The comprehensive assessment found further scope for exploiting synergies at EU level in highly technical areas (e.g. cyber, big data and open source analysis, special intervention units) where not all Member States were able to invest the necessary resources. EU agencies had a key role to play with further scope for gains in this area from the instruments they offer.

The creation of a specific Commissioner portfolio for the Security Union supported by a cross cutting Task Force drawing on the expertise of the whole Commission services and the European External Action Service has helped to foster a more joined-up approach thereby countering the fragmentation previously criticised by practitioners. The Task Force has launched several sub-groups allowing the different Commission services to work together to identify practical solutions to address the current security challenges.

2.4 Fundamental rights

In a European Union founded on respect for human dignity, freedom, democracy, equality, the rule of law and human rights, protecting and fostering citizens' security and complying with fundamental rights are complementary and mutually reinforcing.

In order to guarantee a high level of security while ensuring that the measures adopted comply with fundamental rights, a number of safeguards are built in the EU policy making processes, including the oversight exercised by the Court of Justice of the European Union.

Over the period assessed, and in particular since the adoption of its Strategy on the effective implementation of the Charter[7], the Commission has ensured that fundamental rights are fully respected in all its legislative and policy proposals. As part of its Better Regulation policy, the Commission has progressively developed over the last decade instruments and mechanisms aiming at improving the evidence-basis of its proposals, including reinforcing its systematic

[7] See in particular the Communication from the Commission - Strategy for the effective implementation of the Charter of Fundamental Rights by the European Union, COM(2010) 573 final.

assessment of their impact on fundamental rights.[8] Fundamental rights have also been assessed in the evaluation of the impact and effectiveness of EU instruments and policies to ensure that the instruments remain necessary, proportionate and fit for purpose, having regard to the possible evolution overtime of threats and available technology, as well as their interaction with other factors, including societal considerations[9]. The Court of Justice examines not only the compatibility of EU legislation with fundamental rights, but also the compatibility with fundamental rights of measures taken at national level by the Member States to apply or comply with EU law[10].

At the same time, the Commission has strengthened its role in ensuring that Member States respect the Charter when implementing Union law. This includes stepping up its preventive approach by assisting national authorities to ensure compliance with the Charter in implementing relevant EU legislation.

For specific initiatives, specialised bodies such as the European Data Protection Supervisor (EDPS) are involved. The specific expertise of the EU Agency for Fundamental Rights, established in 2007, is also increasingly relied upon by EU institutions in order to better address fundamental rights challenges, including through targeted consultations or requests for opinions on specific topics or proposals.

Fundamental rights safeguards are often an important focus in the legislative process involving the European Parliament and the Council. Negotiations between the co-legislators have led on various occasions to further strengthening of fundamental rights safeguards.[11] Tools and mechanisms have been developed to deal with issues of compatibility with fundamental rights arising during the legislative process.[12]

Overall, the assessment shows the importance of promoting the existing legal and policy framework to ensure that EU action in the area of security, and related national measures, fully comply with fundamental rights as enshrined in the Charter.

---

8 See in particular the Commission Staff Working Paper - Operational Guidance on taking account of Fundamental Rights in Commission Impact Assessments SEC(2011) 567 final.

9 This is reflected, for example, in the prominence given to preventive measures aimed at promoting common European values, fostering social inclusion, enhancing mutual understanding and tolerance, tackling inequalities and preventing marginalization and the stigmatisation of groups or communities in the context of the EU actions to address the root causes of extremism (see in particular the Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions – Supporting the prevention of radicalisation leading to violent extremism, COM(2016) 379 final).

10 Examples include the invalidation of the Data Retention Directive (Directive 2006/24/EC); the decision that national legislation in the UK and Sweden imposing "general and indiscriminate" requirements on telecommunication operators to retain users' traffic and location data is inconsistent with the Electronic Communications Directive (Directive 2002/58/EC) as read together with the provisions of Articles 7 (Respect for private and family life) and 8 (Protection of personal data) of the Charter; the review of the compatibility of the Framework Decision on the European Arrest Warrant with Articles 47 (Right to effective remedy and to a fair trial) and 48 (Presumption of innocence and right of defence) of the Charter; annulling Council Regulation (EC) No 881/2002 by clarifying that when imposing sanctions at EU level the duty to state "individual, specific, and concrete" reasons (Article 296 TFEU) and the level of intensity of judicial review of errors of fact in human rights cases and on the content of the rights of defence of suspected terrorists.

11 There were also examples where the European Parliament has withheld its consent for the conclusion of international agreements which led to re-negotiations in view of improving the guarantees for fundamental rights of EU citizens.

12 See in particular the Council Guidelines on methodological steps to be taken to check fundamental rights compatibility at the Council's preparatory bodies, 19.5.2001, available at: http://register.consilium.europa.eu/pdf/en/11/st10/st10140.en11.pdf and the Interinstitutional Agreement between the European Parliament, the Council of the European Union and the European Commission on Better Law-Making, OJ L 123 of 12.5.2016.

3. Conclusions

3.1 Areas where EU intervention was opportune and adequate

The overarching conclusion of the Comprehensive Assessment is that EU action in the area of security is both opportune and adequate. Some EU policy interventions were singled out by stakeholders as being particularly valuable such as the Schengen Information System, Joint Investigation Teams, the European Arrest Warrant and mutual legal assistance support of national authorities in collecting and exchanging information and evidence, in terms of allowing Member States to carry out coordinated operational action, and help bring offenders to justice.

The work done at EU level to facilitate the exchange of information and support operational cooperation was also assessed positively.

The positive contribution of **EU agencies** in the area of Justice and Home Affairs was highlighted by stakeholders as particularly valuable. In recent years, Europol's support has proven its added value, including through the agency's ability to adapt its structure to evolving security threats[13] and to provide new tools and services to support Member States' law enforcement services. Eurojust has increasingly been asked to coordinate criminal investigations and prosecutions and is regularly called upon to undertake more activities with the EU institutions, for instance in the implementation of the European Arrest Warrant and the European Investigation Order (EIO). Training of law enforcement officials is an essential component of EU security policies implementation. Lack of knowledge of EU tools has been highlighted as hindering their effective implementation and use. In this regard, the role of CEPOL to assist Member States in developing bilateral and regional cooperation as well as the organisation of thematic training was also valued positively. Other appropriate operational support mentioned by stakeholders included the risk analysis and situational awareness capability provided by the European Borders and Coast Guard Agency (EBCGA) and the support provided by the European Monitoring Centre for Drugs and Drug Addiction (EMCDDA) as a hub for early warning on synthetic drugs.

According to the Assessment, the added value of enhanced information exchange among Member States and with EU agencies and EU bodies, like the European Anti-Fraud Office (OLAF), has contributed to more and better quality information being exchanged across borders. Information sharing on counterterrorism between the Member States, as well as through and with Europol and Eurojust[14], "reached an all-time peak in 2016"[15]. The Schengen Information System (SIS) has also played a vital role in this regard by enabling competent authorities from the Member States to exchange information more effectively and more efficiently. The system currently contains approximately 73.5 million alerts on persons posing a security risk, including those who are sought in relation to terrorism and other serious crime, lost or stolen objects and documents as well as missing persons. It currently operates in 30 European countries and was accessed almost 4 billion times in 2016.

---

13 With the creation of the European Cybercrime Centre EC3, the European Counter-Terrorism Centre, the European Migrants Smuggling Centre or 24/7 services.

14 Including through the use of Council Decision 2005/671/JHA.

15 See: Press release by Europol, 30 January 2017, https://www.europol.europa.eu/newsroom/news/information-sharing-counter-terrorism-in-eu-has-reached-all-time-high.

The importance of instruments facilitating operational cooperation was stressed by stakeholders. Many Member States referred to the practical benefits resulting from Joint Investigation Teams (JITs). This includes improved information exchange, exchange of best practices, enhanced collection of evidence, and optimisation of the procedures within the investigation by mutual recognition of the actions carried out by the parties. Eurojust played an important role in increasing the number of JITs by providing financial, logistical and legal assistance and by hosting the JIT Network Secretariat. Taking account of the positive experience from the first full Policy Cycle, and the results of the evaluation, Member States agreed to launch a new Policy Cycle for the period 2018-2021. Most Member States identified Police and Customs Cooperation Centres (PCCCs) as a useful instrument to facilitate cross border cooperation.

The Assessment has also highlighted the expectations of stakeholders as regards the added value of recently adopted legislation to enhance security in the EU including the recent Directive on Combating Terrorism[16], the new legal framework applicable to Firearms[17] and the recent legislation on Money Laundering and Terrorism Financing.[18]

3.2 Areas where improvement and refinement are needed

While the Assessment found that the majority of areas covered by EU action are appropriate and relevant, for some areas there is scope for further improvement and refinement.

The Assessment confirmed the existence of certain gaps in the EU **information systems** that have been developed overtime (whether centralised such as the Schengen Information System, the Visa Information System and Eurodac, or decentralised such as the Prüm framework) and provide valuable information, in particular for law enforcement. These gaps have already been addressed by the Commission in recent legislative proposals (Entry/Exit System (EES) and a European travel information and authorisation system (ETIAS)).

In the area of **counter-terrorism**, although the work done to prevent radicalisation is viewed positively, it was felt by stakeholders that work within the EU framework needs to keep pace with new challenges requiring a comprehensive response combining an enhanced criminalisation framework with measures on prevention of radicalisation and more efficient exchange of information on terrorist offences. The various EU initiatives (such as the Radicalisation Awareness Network and initiatives under the EU Internet Forum) have laid a solid basis for more effective Prevent work and made valuable contributions to equipping the relevant stakeholders with the necessary skills to tackle radicalisation. At the same time, given the increased threat level and the scope and scale of radicalisation, the Assessment found that more could and must be done in terms of coordination, outreach and impact, building on the achievements so far.

The Assessment also found that **financial investigations procedures have** not yet been used to their full potential in the fight against terrorist financing. Work here was hampered by the complexity of financial investigations, the high level of expertise required for their implementation, the time-consuming procedures necessary to check the financial information

16 Directive (EU) 2017/541.

17 Directive (EU) 2017/853 of the European Parliament and of the Council of 17 May 2017 amending Council Directive 91/477/EEC on control of the acquisition and possession of weapons

18 The Fourth Anti-Money Laundering Directive to strengthen EU rules to tackle money laundering, tax avoidance and terrorism financing entered into force on 26 June 2017.

obtained, legal impediments that prevented the authorities from conducting parallel investigations, as well as limited coordination and cooperation on an internal level.

In the fight against terrorist financing, the Terrorist Finance Tracking Programme (TFTP) agreement with the US was positively assessed. The Commission is currently studying whether a European system, complementing the TFTP to cover single euro payments area (SEPA) payments, could close a gap that could otherwise potentially be exploited by terrorists.

On money laundering, asset recovery and financial crime, the assessment found the legal framework in this area to be well developed, but also identified scope for further improvements, as addressed by recent Commission proposals.

EU action in the area of **organised crime** was assessed as having focused on specific types of crime, rather than pursuing a horizontal, comprehensive approach to organised crime and organised crime groups. This should be taken into account when building up a more robust evidence base for future EU action in this area.

The need for further development of "information hubs" within the EU agencies was noted, in particular for the European Counter Terrorism Centre and the European Cybercrime Centre at Europol. The new legislative proposals to reinforce the Schengen Information System (SIS) have taken important steps in this direction by proposing the extension of Europol's access to SIS in order to allow it to access all the alert categories in the system. The links between terrorism and organised crime are well-known and the extended access will help to ensure that the analytical expertise of the agency will be fully exploited. Enhanced cooperation with priority third countries with the necessary data protection standards will further reinforce the role of Europol as "information hub".

Given the constantly evolving nature of cybersecurity threats, the objectives of the 2013 Cybersecurity Strategy were judged still to be relevant, but the measures proposed to implement them were no longer adequate in view of the changed threat landscape and the emergence of new threat actors and rapidly developing technology. The Commission (together with the High Representative) has decided to review the 2013 EU Cybersecurity Strategy, on the basis of an evaluation by September 2017. Overall, the Comprehensive Assessment pointed to the continued relevance of all instruments currently in place but highlighted the need for more measures at all levels – strategic, legislative and operational – and the full integration of the risks of cyberattacks made in the context of sophisticated hybrid campaigns.

It emerged from the Assessment that the legislative framework in place related to **cybercrime** is still relevant for the purposes for which it was designed – to harmonise substantive criminal law. Some of the instruments are still in the process of transposition and further support is needed to Member States to ensure that the potential of existing instruments is fully used. Major gaps were identified on the procedural side in terms of cross-border access to evidence and cooperation with private actors for access to evidence.

The Assessment also confirmed that the structures established for support of operational cooperation – notably the European Cyber-Crime Centre (EC3) at Europol – are seen by stakeholders as very successful. Eurojust contributes to this operational cooperation via a Eurojust representative seconded to EC3 in order to facilitate the judicial aspect of cooperation. It emerges from the assessment that demands for EC3 support have already

outpaced supply and are likely to increase in the future. During the consultation phase for the assessment, a wide range of stakeholders insisted on the need for establishing a joint centre of excellence for Cyber Forensics and Encryption which can provide support for analysis and operations to Member States and would allow to pool resources, thus supporting also Member States that do not dispose of own capabilities.

Finally, the Assessment found that the fight against cybercrime, including the coordinated response to large-scale attacks, requires a more complete threat intelligence picture and greater coordination among all relevant actors.

3.3 Areas requiring review of applicable legislation

The legislative stockpile developed at EU level in the area of internal security is relatively recent, and therefore, generally judged to be fit for purpose. There are areas where the security landscape (and sometimes also the legal framework) has rapidly evolved, resulting in the need to review whether legislation is still relevant in today's reality.

The Commission has already assessed and identified, in the light of the end of transitional provisions set out in the Protocol 36 to the Treaty of Lisbon, as from 1 December 2014, the legal acts related to the Area of Freedom, Security and Justice that had exhausted all their effects and/or were no longer relevant in order to repeal them. As a result, in November 2014, the Commission proposed to repeal 24 acts in the area of police cooperation and judicial cooperation in criminal matters[19]. In addition, every year as part of the preparation of its Annual Work Programme, the Commission identifies instruments that could be repealed because they are considered obsolete or redundant.

In this context, the findings of the assessment suggest the following acts which could be considered for further review:

- The Commission decision 2006/299/EC setting up a group of experts to provide policy advice to the Commission on fighting violent radicalisation: no longer applicable since 20 March 2007;
- Council Common Position of 27 December 2001 on combating terrorism (2001/930/CFSP), as this is subsumed by Framework Decision 2002/475/JHA (not to repeal), which is in its turn is replaced by Directive (EU) 2017/541;
- Joint Action 98/699/JHA on money laundering, the identification, tracing, freezing, seizing and confiscation of instrumentalities and the proceeds from crime: most of its provisions were already replaced by Framework Decision 2001/500/JHA, which applies also to UK and DK. This instrument was replaced in full by Directive 2014/42/EU for all MS participating in the Directive (all except DK and UK). The remaining provisions are general recommendations with no binding value which now apply only to UK and DK;
- Council Framework Decision of 28 May 2001 combating fraud and counterfeiting of non-cash means of payment (2001/413/JHA);
- Council Directive 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection.

[19] COM (2014) 713, COM (2014) 714 and COM (2014) 715. The co-legislators added some additional acts to the repeal package. In all 26 legal acts were finally repealed by the co-legislators (Regulation (EU) 2016/93, Regulation (EU) 2016/94 and Regulation (EU) 2016/95).

II. COUNTER-TERRORISM

Europe is facing a high and evolving terrorist threat, as demonstrated by an increase in recent years in terrorist attacks, fatalities and arrests.[20] This high threat, along with the understanding that an efficient response to terrorism requires collective action, highlights the need for a strong EU response to terrorism. This expectation is shared by more than 80% of EU citizens.[21]

Terrorism is not a new phenomenon in Europe, with several Member States facing decades of separatist or ethno-nationalist threat, right-wing and left-wing (violent) extremism as well as religiously inspired terrorism. The attacks on 11 September 2001 in the US, the 2004 Madrid bombings and the 2005 London attacks acted as a catalyst for the development of counterterrorism policies at EU level. Due to the increase and evolution of the terrorist threat in the last years, in particular linked to the crises in Syria, Iraq and Libya and the foreign terrorist fighter phenomenon, substantial progress has been made since 2015 in many areas.

While Member States have the primary responsibility in the field of security and counterterrorism (retaining also the sole responsibility for national security pursuant to Article 4 of the Treaty on European Union (TEU), the EU has supported Member States' efforts to collectively combat terrorism. This support has taken various forms, from harmonisation of counterterrorism legislation to the development of specific IT systems or tools facilitating information exchange and law enforcement and judicial cooperation[22], to more operational activities to advance the sharing of best practices, cooperation with civil society and private sector.

EU counterterrorism policy encompasses a wide range of non-counterterrorism measures and instruments, both to close down the space in which terrorists can operate (cutting access to financing, weapons and channels of propaganda and recruitment, as well as denying them freedom of operation) and to increase the resilience of Member States (enhancing their capacity to withstand attacks, protecting citizens and infrastructures). These measures include horizontal information sharing and law enforcement cooperation tools as well as other policy areas: border security, transport security or crisis response.

The overarching goal of EU policy in the field is to reinforce efforts to safeguard security while promoting the respect of our common values including the rule of law and respect for fundamental rights. To provide a comprehensive response to the evolving terrorist threat, an enhanced criminal law framework needs to be complemented by effective measures on prevention of radicalisation leading to terrorism and efficient exchange of information on terrorist offences.

In this area, the assessment shows that the overall conceptual framework of EU invention has remained valid while allowing for its adaptation in response to a rapidly changing environment. It results from the assessment that there is an overall need to ensure correct and consistent transposition and application of the EU acquis (especially the new Terrorism

---

[20] Europol, EU Terrorism Situation and Trend Report of 2015, 2016 and 2017.

[21] Autumn 2016 "Standard Eurobarometer": http://ec.europa.eu/COMMFrontOffice/publicopinion/index.cfm/Survey/getSurveyDetail/instruments/STANDARD/surveyKy/2137.

[22] The Eurojust National Coordination System (ENCS) includes the national correspondents for Eurojust for terrorism as its members.

Directive (EU) 2017/541, and all newly adopted instruments in the field of terrorism financing).

In various areas, the assessment points to the need of consolidation of the policy, the need for more structured exchanges among stakeholders, the need to develop common understanding of threats (building on the work of Europol and the EU Intelligence and Situation Centre (EU INTCEN), as the entry point for Member States intelligence and security services), expand the operational cooperation and use EU tools to support and leverage Member States actions (risk assessment methodology, CBRN and soft target protection, crisis management).

4. Counter-Terrorism Strategy and Horizontal Instruments

a. Main findings

The assessment suggests that the conceptual framework of the 2005 **Counter-Terrorism Strategy** remains valid overall (including the four strands of Prevent, Protect, Pursue, Respond). Within this strategic framework the EU has gradually refined and developed its approach by addressing a number of dimensions of the terrorist threat, from the legal framework to border security, countering radicalisation, disrupting terrorist financing as well as their access to firearms, explosives and CBRN materials, protecting citizens and critical infrastructures.

With the recent adoption of Directive (EU) 2017/541, the Union's definition of terrorist and terrorist-related offences is considered to be fit for purpose to address the evolution of terrorists' modus operandi. The Directive aims to prevent terrorist attacks by criminalising acts such as undertaking training or travelling for terrorist purposes, as well as organising or facilitating such travel. The assessment indicates the need to support Member States with the transposition and application of the Directive.

It results from the assessment that the EU would benefit from more extensive use of regular monitoring and **assessment of the threat and risks**. This work is carried out by the Commission services along with Member States' experts and EU agencies, and it builds on the strategic analysis produced by INTCEN on the basis of Member States' security and intelligence services contributions. Examples are risk assessments in areas such as aviation security, terrorism financing or border security. Stakeholders called for expanding this risk assessment based approach to other policy domains. At the more strategic level, a regular analysis of the threat and risk facing the Union by Commission services and the EEAS and with the support of the Counter Terrorism Coordinator and relevant agencies could inform European Council discussion and guidance, pursuant to Article 222(4) of the Treaty on the Functioning of the European Union (TFEU).

The assessment confirms that the **European Counter Terrorism Centre** is growing in its capacity as a hub for counterterrorism cooperation at EU level. In line with the commitment of European Police Chiefs, sustained efforts will focus on consolidating the progress made in the field of information sharing and operational support. Strengthened cooperation with priority third countries with the necessary data protection standards will further reinforce the role of the ECTC as "information hub".

b. Overview of EU action

The European Union aims to facilitate cooperation between national authorities competent to prevent, investigate and prosecute terrorist offences. This is done through several tools:

coordination of Member States' counterterrorism policies, harmonisation of national legislation and support for operational work conducted by national authorities.

Given that before 11 September 2001, only six (the UK, Italy, Spain, Greece, France and Portugal) of the (then) 15 Member States had dedicated terrorism legislation, and relevant international conventions only addressed specific terrorism-related offences, the achievements at Union level can be considered considerable.

The origins of the EU's counter-terrorism agenda can be traced back to the Conclusions of the extraordinary Justice and Home Affairs Council convened on 20 September 2001 which called for concerted action in thirty-three specific areas, with a further eight measures relating to cooperation with the US. Among the expedited measures were proposals for a Framework Decision on combating Terrorism and on Framework Decision on European Arrest Warrant (EAW), published on 25 September 2001. The positive impacts of a horizontal instrument such as the EAW particularly apply to terrorism (see below Chapter V. Information exchange and operational cooperation).

In light of the 2001 terrorist attacks in the US, the Council Decision of 28 November 2002 established a mechanism for evaluating the legal systems and their implementation at national level in the fight against terrorism (2002/996/JHA) and set up a **peer review mechanism** run by Member States in the Council with a limited support role for the Commission. In its March 2004 Declaration on combating terrorism, the European Council highlighted the importance of peer evaluation of national arrangements. This mechanism has not been activated.

External border control has also become an integral part of the EU's counterterrorism toolkit. While it had not originally been identified as a priority dimension of the EU counter-terrorism policy, the importance of effective border control has grown since then, especially following the Madrid terrorist attacks in March 2004. The Declaration on Combating Terrorism, which was subsequently adopted on 25 March 2004, was the first EU official counter-terrorism document to identify effective border control as a counter-terrorism priority.

In the revised Plan of Action on Combating Terrorism adopted in June 2004, the importance of ensuring effective systems of border control was once more presented as one of the seven EU strategic objectives to combat terrorism ('Objective 4: To protect the security of international transport and ensure effective systems of border control')[23].

In the field of legislative harmonisation, the adoption of the Framework Decision 2002/475/JHA[24] on combating terrorism constituted a milestone. It identified a number of offences that must be qualified as "terrorist" when committed with a specific terrorist aim, namely to seriously intimidate a population, to unduly compel a government or an international organisation to perform or abstain from performing any act, or to seriously destabilise or destroy the fundamental political, constitutional, economic or social structures of a country or an international organisation.

This instrument was amended by Framework Decision 2008/919/JHA introducing the offences of 'public provocation to commit a terrorist offence', 'training for terrorism' and 'recruitment for terrorism'. It answered the noted change in the terrorist threat, which sees an

[23] For details on the role of the Schengen Information System in this context, see Chapter V. Information exchange and operational cooperation, of this assessment.

[24] Council Framework Decision 2002/475/JHA of 13 June 2002 on combating terrorism (OJ L 164, 22.6.2002, p. 3).

increase in the use of the internet in the self-training and self-radicalisation of potential terrorists with the consequent development of the 'lone wolves' phenomenon.

EU-wide definitions of terrorist and terrorist-related offences remove legal gaps that may result from a fragmented approach. They are thus of clear added value for enhancing the security of the EU and the safety of EU citizens and people living in the EU. They facilitate a common understanding and benchmark for cross-border information exchange and cooperation in police and judicial matters.

The EU definitions provided in the Framework Decision also serve as a yardstick for other EU instruments that refer to terrorism. This includes the EU regime for freezing the assets of foreign terrorist organisations and individuals.

The attacks carried out on European soil in recent years tragically illustrate that the risk of terrorism can rapidly materialise and that the terrorist threat continues to evolve rapidly. No measures were in place for victims of terrorism that would respond to their specific needs. The existing horizontal rules on victims of crime[25] were therefore strengthened by new provisions of Directive (EU) 2017/541[26] on combating terrorism[27]. To minimise the impact of terrorist attacks on victims and their families, the new Directive sets up mechanisms that respond more to the needs of victims of terrorism. The Directive also strengthens the obligation to exchange information on terrorism between Member States under Decision 2005/671/JHA[28], and sets up an obligation for Member States to take down terrorist content online.

The new Directive on combating terrorism is a good example of the mainstreaming of fundamental rights. It includes an explicit fundamental rights clause whilst several fundamental rights aspects were taken into account in the drafting and negotiation process, including the necessity and proportionality of interferences with the rights to freedom of movement, data protection and freedom of expression (Articles 45, 8 and 11 of the Charter). Due account was also taken of the principles of legality and proportionality of criminal offences and penalties (Article 49 of the Charter) and the rights of victims, including the right to an effective remedy (Article 47 of the Charter). The *ex post* assessment of the Directive will also cover its impact on fundamental rights and freedoms.

The 2014 implementation report[29] of Framework Decision 2008/919/JHA was supported by an external evaluation of the legal framework adopted by the Member States to combat terrorism in practice. The evaluation concluded that the changes introduced in 2008 were seen as useful in helping to combat the changing nature of the terrorist threats faced by Member States. The added value of the Framework Decision was considered as high for Member

---

25 Directive (EU) 2012/29 of the European Parliament and of the Council of 25 October 2012 establishing minimum standards on the rights, support and protection of victims of crime, and replacing Council Framework Decision 2001/220/JHA; Council Directive 2004/80/EC of 29 April 2004 relating to compensation to crime victims, OJ L 315, 14.11.2012, p. 57–73.

26 Directive (EU) 2017/541 of the European Parliament and of the Council of 15 March 2017 on combating terrorism and replacing Council Framework Decision 2002/475/JHA and amending Council Decision 2005/671/JHA, OJ L 88, 31.3.2017, p. 6.

27 The Directive must be transposed by Member States by 8 September 2018.

28 Council Decision 2005/671/JHA of 20 September 2005 on the exchange of information and cooperation concerning terrorist offences, OJ L 253, 29.9.2005, p. 22.

29 Report from the Commission to the European Parliament and the Council on the implementation of Council Framework Decision 2008/919/JHA of 28 November 2008 amending Framework Decision 2002/475/JHA on combating terrorism (COM(2014) 554 final).

States that did not already have a specific legal framework to tackle terrorism. For those that did, added value lay in strengthening the framework for cooperation with other Member States in tackling the preparatory stages of a terrorist action thanks to a common understanding of terrorist-related crimes like public provocation, recruitment and training to terrorism.

Directive (EU) 2017/541 requires the Commission, by 8 September 2021, to submit a report to the European Parliament and to the Council, assessing the added value of the new provisions in the Directive with regard to combating terrorism, including those designed to protect and assist victims of terrorism.

To forge a strategic approach in the field, in December 2003, the European Council adopted a **European Security Strategy**, where terrorism heads the list of threats facing the Member States and which indicates that concerted European action against terrorism is 'indispensable'. Following the European Council Declaration on Combating Terrorism of 25 March 2004, the Council adopted a revised Plan of Action to Combat Terrorism.[30] The **EU Counter-Terrorism Strategy** was adopted by the European Council in December 2005, focusing on fours strands of work: Prevent, Protect, Pursue and Respond. The European Council committed to review progress on the Strategy every six months. Among the measures included in this declaration was the establishment of the position of a Counter-Terrorism Coordinator. The Counter-Terrorism Coordinator and the Commission were invited to update on the progress. Since then, terrorism has figured prominently in the 2010 Internal Security Strategy, the 2015 European Agenda on Security[31] and the 2016 Security Union Communication.

The 2016 Global Strategy for the European Union's Foreign and Security Policy recalls that security at home depends on peace and stability beyond our borders, and underlines that EU external action must reflect, complement and contribute to EU's internal security. The Foreign Affairs Council Conclusions of 9 February 2015 remain the cornerstone of the EU's external engagement on counterterrorism. Two years and a half after their adoption, Member States have called for the EU to take stock, to adapt to the changing nature of the terrorist threat and to strengthen its external efforts in full coordination with all EU services putting all instruments available to the task. In order to better prepare the adoption of this new set of Council Conclusions at the Foreign Affairs Council of 19 June 2017, EEAS and Commission services prepared and presented to Member States a joint paper on the external dimension of counter-terrorism that frames the ideas for new lines of priority and action, including a sharpening of the thematic and geographical focus.

In order to establish a robust approach that is not simply reactive or "crisis-driven", a security strategy needs to anticipate the threat and rely on a sound understanding of its evolution. The Commission has promoted **risk-based decision making** in the field of counterterrorism: in its 2010 Communication Internal Security Strategy in Action, the Commission proposed to develop EU risk assessment and suggested the establishment at EU level of a coherent risk management policy linking threat and risk assessment to decision making.

Risk assessment

[30] http://www.consilium.europa.eu/uedocs/cmsUpload/EU_PlanOfAction10586.pdf.

[31] The same year, at the informal meeting of the Heads of State or Government on 12 February 2015, the members of the European Council set out a number of orientations to guide the work in the fight against terrorism.

The Commission continues to develop risk assessment capabilities as a support instrument to inform policy formulation, seeking to ensure that counterterrorism measures are both effective and proportionate. Building on regular threat assessment inputs from the EU INTCEN and Europol, and in coordination with Member States experts and other relevant EU agencies, the Commission has developed risk assessment activities in areas such as aviation security (air cargo, passenger-related risks, risks from conflict zones), border checks (common risk indicators in respect of foreign terrorist fighters), CBRN risks (chemical, biological, radiological and nuclear) or terrorism financing (supranational risk assessment on money laundering and terrorism financing).

The successful experience developed in the field of risk assessment at EU level contributed to building the necessary confidence for close cooperation with Member States. The risk-based approach allows for the definition of effective and proportionate measures, adapted to the evolution of the threat and taking into account existing mitigation measures.

In addition, the Commission encouraged closer cooperation between Europol's European Counter Terrorism Centre (ECTC) and the EU INTCEN in the field of strategic assessment of the terrorist threat. Updated threat and trend analysis should support the formulation (and revision) of EU counterterrorism policy, ensuring that measures are tailored to the evolution of the threats and risks.

The methodologies developed at EU level have proven flexible and tailored to the needs, building on existing EU capabilities where available (EEAS including EU INTCEN and counter-terrorism/security experts in EU delegations, Europol, European Border and Coast Guard) and the specific expertise of Member States. These processes have also provided an incentive for Member States to develop their own risk assessment capabilities at national level where this was not yet the case.

Strong political commitment and requests as well as the increasing interests of stakeholders (Member States, EU INTCEN, agencies, private sectors as well as third countries) have compensated for the ad hoc provisions or political mandates. The use of the provisions of Article 222 TFEU (solidarity clause further analysed under point 4) could provide a solid basis for structured risk assessment at EU level.

While the necessary secure infrastructures (Secure Zone) and procedures allow within the EU institutions for the handling of classified information during meetings, insufficient secure IT communication channels constitute a technical challenge for the rapid exchange of such information within EU institutions and with Member States.

At the operational level, information sharing and operational cooperation constitute core pillars of EU action. The specific roles of Europol and Eurojust in the field of counterterrorism are analysed in Chapter V.

In 2005, the Council adopted legislation providing for the mandatory collection and sharing of information concerning criminal investigations and prosecutions/convictions on terrorist offences with Europol and Eurojust respectively, and other Member States.[32] This legislation

[32] Council Decision 2005/671/JHA of 20 September 2005 on the exchange of information and cooperation concerning terrorist offences, OJ L 253/22, 29.9.2005.

has however proved challenging to monitor and enforce, despite the significant progress made in particular in terms of contributions to Europol[33] and Eurojust.

European Counter Terrorism Centre (ECTC)

The establishment of the **European Counter Terrorism Centre (ECTC)** at Europol was a flagship initiative of the European Agenda on Security and a milestone in EU counterterrorism cooperation. Operational since January 2016, the ECTC aims primarily at optimising the use of existing instruments to support Member States' investigations. In the period from 2015 to 2017, the ECTC was granted 84 staff to build the EU law enforcement response to the terrorist threat. The support provided to French and Belgian investigators by the "Task Force Fraternité" after the November 2015 Paris and March 2016 Brussels attacks illustrated the added value of the ECTC. With the classification upgrade of Europol's system (CT SIENA[34]) and the steady increase in information sharing, the ECTC has supported an increasing number of CT investigations and operations.

The establishment of the ECTC at Europol illustrates a significant evolution in counterterrorism cooperation and information exchange at EU level. Despite the existence of CT capabilities at Europol and the legal provisions on mandatory exchange of information[35], the potential of cooperation through Europol remained largely untapped. Only a few dozens of suspected foreign terrorist fighters were reported in Europol's databases at the beginning of 2015.

The development of dedicated capabilities in the ECTC (including the upgrade of Europol's SIENA), the pooling of existing instruments (Europol Information System, specialised Focal Points, European Bomb Data System, the EU-US Terrorism Financing Tracking Programme, the Internet Referral Unit) and the high level political commitment from the European Council paved the way for a steady increase in contributions to Europol databases on terrorist suspects (over 9.000 suspects in the Europol Information System and 38.000 in Focal Point Travellers). In return, in response to the proactive engagement of Member States in the wake of the Paris and Brussels attacks and with the sharing of an unprecedented amount of data, the ECTC has proven flexible and capable of providing valuable support to Member States' investigators. Since then, the number of operations supported has continuously increased (87 in the first quarter of 2017 compared to 127 in total in 2016).

The European Police Chiefs meeting in Berlin in February 2017 confirmed this positive evolution. The establishment of a Programme Board, as proposed by the Commission in its Communication of September 2016[36], should improve the governance of the ECTC, ensuring that the Centre focuses on priorities set by Member States' counterterrorism experts.

Acting as an "information hub" and operational support provider for Member States, the ECTC can also facilitate exchange with third countries. With the entry into force of the new

---

33 https://www.europol.europa.eu/newsroom/news/information-sharing-counter-terrorism-in-eu-has-reached-all-time-high.

34 The Secure Information Exchange Network Application, SIENA, is Europol's platform allowing for secure communication among Europol's liaison officers, analysts and experts, Member States and third parties with which Europol has cooperation agreements. SIENA was updated in 2016 to handle restricted content on counter terrorism (CT SIENA). https://www.europol.europa.eu/activities-services/services-support/information-exchange/secure-information-exchange-network-application-siena

35 Council Decision 2005/671/JHA on the exchange of information on terrorist offences.

36 COM(2016) 602 final.

Europol Regulation[37], the Commission will work with the agency to further develop cooperation with priority countries. Eurojust will also consider ways to foster the operational cooperation with the ECTC and is currently preparing the secondment of a Eurojust representative to the ECTC.

The Commission has also supported actions through funding under direct management, from 2007 to 2016, in the area of counter-terrorism for an approximate amount of 158 million.[38] In addition, the EU has committed substantial financial resources to security research in areas relevant to the fight against terrorism through FP7 and Horizon 2020 Secure Societies Programme and Inclusive, Innovative and Reflective Societies Programme. Since 2007, approximately EUR 980 million have been invested in security research on issues such as CBRN protection (EUR 75 million), explosives (EUR 68 million), critical infrastructures protection (EUR 55 million), intelligence against terrorism (EUR 35 million), preparedness, prevention, mitigation and planning (EUR 150 million), recovery (EUR 17 million), energy, transport and communication grids (EUR 116 million).

5. Prevent

a. Main findings

It results from the assessment that the various EU initiatives (such as the RAN and initiatives under the EU Internet Forum) have laid a solid basis for more effective prevent work and made valuable contributions to equipping the relevant stakeholders with the necessary skills to tackle radicalisation. At the same time, given the increased threat level and scope and scale of radicalisation, more can and must be done in terms of coordination, outreach and impact by building on achievements so far.

Furthermore, stakeholders expressed a clear need for a more structured exchange on preventive work among the relevant stakeholders. The Commission has announced the setting up of a High Level Expert Group on Radicalisation (HLEG-R) including in particular representatives from Member States, the RAN Centre of Excellence and researchers[39].

The HLEG-R would provide advice and expertise to the Commission with the triple objective i) to improve cooperation and collaboration among the different stakeholders, ii) to support the further development of EU prevent policies, but especially iii) to help assess options for a more permanent structure for collaboration and coordination of prevent work at EU level within the shortest possible timeframe.

b. Overview of EU action

The prevention of radicalisation is a cornerstone of the EU's counterterrorism efforts. EU prevent policies find their origin in the 2005 EU Counter Terrorism Strategy[40] and were further developed and refined in several other policy documents.[41] The 2015 European

37 See for details, Chapter V. Information exchange and operational cooperation, of the present assessment.

38 Based on the amounts foreseen in the annual work programmes.

39 COM(2017) 354 final.

40 Council doc. 14469/4/05.

41 EU Strategy on radicalisation and recruitment (as revised in 2014) as well as the Internal Security Strategy 2010-2014, replaced in 2015 by the European Agenda on Security and its follow up communication and the Council's renewed Internal Security Strategy 2015-2020. See also, the Opinion of the Committee of the Regions (15/16 June 2016) and the Report of the European Parliament (3 November 2015) on radicalisation.

Agenda on Security highlighted the need for further action to prevent and counter radicalisation leading to violent extremism and terrorism. The often similar nature of the challenges faced by Member States but also the scale and interconnected nature of the phenomenon call increasingly for actions at EU level[42]. The Communication on radicalisation of June 2016[43] specified in more detail how the EU supports Member States in a number of key areas making use of instruments and initiatives in different policy areas.

The Commission's main policy objective is to **support stakeholders** in Member States to effectively prevent and counter radicalisation. The Commission actions are directed at creating the appropriate framework for enhanced exchanges of practices and expertise, capacity building, and financially supporting initiatives and projects. The policy approach is deeply grounded in the promotion of democratic values, a multi-sector/agency approach, the empowerment of civil society, the mobilisation of education and the youth sector, and the involvement of local actors. In addition to more targeted initiatives to prevent and counter radicalisation, the Commission also ensures coordination and synergies with EU action in adjacent fields drawing on instruments and policies that can make a relevant contribution to **tackling the root causes of radicalisation while strengthening resilience,** by fostering social inclusion, enhancing mutual understanding and tolerance, tackling inequalities and preventing marginalization and the stigmatisation of groups or communities. This includes measures in the area of education, youth, social inclusion, integration, non-discrimination and preventing and combating hate speech, in particular online, and hate crime. The implementation of these policies is supported by research into the different aspects of radicalisation.[44] Given the long-term nature of prevention policies, it is important to create a stable policy environment with systemic measures and sustained support to stakeholders on the ground, which have the potential to reach out to a critical mass of youngsters.

Through its different funding programmes[45], the Commission provided and earmarked financial support, amounting to about EUR 150 million[46], to a large number of projects tackling radicalisation within the EU (and in total more than EUR 300 million including projects outside Europe). Under the Erasmus+ programme, in 2016 more than €200 million were devoted to transnational cooperation projects aimed at promoting social inclusion, citizenship, critical thinking and media literacy, as well as intercultural dialogue in the field of education.

---

42 Cf. also Commission Communication delivering on the European Agenda on Security to fight against terrorism and pave the way towards an effective and genuine Security Union, COM(2016) 230 final of 20.4.2016.

43 COM(2016) 0379 final.

44 This includes a policy review on addressing terrorism: Addressing Terrorism - European research in social sciences and the humanities in support to policies for Inclusion and Security: A Policy Review (2016) - https://publications.europa.eu/en/publication-detail/-/publication/55a9f3db-7fe5-41e5-97cc-fc4a3d73325b

45 Programmes include security focussed funds such as ISEC, Union Actions of the Internal Security Fund, and Horizon 2020), other funds addressing different aspects, such as Erasmus +, the Justice Programme, the Rights, Equality and Citizenship Programme, but also the European Social Fund and several funds which cover also the external dimension including the European development Fund, European Neighbourhood Instrument and/or the Instrument contributing to Stability and Peace.

46 Due to the cross-sectorial and far-reaching nature of the challenge, it is difficult to clearly identify projects in the field of radicalisation. This estimate gives a magnitude of the projects directly related to radicalisation and which are mainly co-financed by the programmes mentioned in the previous footnote. It does not take into account the projects on radicalisation funded by national authorities under shared management of ISF-Police, which has a global budget of 662 Million EUR for the period 2014-2020.

Furthermore, **research** on radicalisation (funded primarily through FP7 and Horizon 2020)[47] produced valuable insights and results directly usable by practitioners. There is however scope for further streamlining research activities and feeding research results, in a timely manner, into the policy making cycle, e.g. through mapping, effective dissemination as well as synthesising of research projects and results. With this objective, a number of EU initiatives have already been complemented by research capabilities.[48][49]

Several Council Conclusions addressing different aspects of preventing and countering radicalisation have called upon Member States to adopt a series of measures to better tackle the phenomenon.[50] Several Member States have in the meantime adopted prevent strategies or prevention measures.[51] However, there is currently no reporting or check mechanism that would keep track of or assess the state of implementation at national level. The newly established network of prevent policy makers has helped ensure that new policy developments at Member State level are shared with their EU counterparts.

Most of the key actions identified in the Commission Communication on radicalisation of June 2016 have been implemented or initiated already. Key actions, initiatives and achievements include the creation of EU wide networks or platforms fostering exchanges of expertise and cooperation and contribution to the development of best practices and capacity building. These networks and platforms include the **RAN Centre of Excellence**, the Commission' main policy tool for countering radicalisation, the **EU Internet Forum** to address terrorist propaganda online, the **network of national prevent policy makers** and the European Strategic Communications Network (ESCN). These networks and platforms bring together the relevant stakeholders across the EU, including first line practitioners, civil society actors, law enforcement and government officials, Member State policy makers and the internet industry.

The achievements under these initiatives constitute a solid basis for further work in this field. The RAN has grown into a network connecting over 3000 practitioners across the EU with different professional backgrounds. It has offered training and advice. The exchanges among practitioners have resulted in a large number of RAN best practices, guidelines and handbooks, and recommendations on issues and themes such as polarisation, Foreign Terrorist Fighters (FTFs) and returnees, prison radicalisation and exit programmes, family support measures, youth work and education, community policing, communication and narratives, engagement and empowerment of young people (e.g. through the new platform

---

47 Cf. FP 7 Programme on Social Sciences and Humanities and Horizon 2020, Societal Challenge 6 on inclusive, innovative and reflective societies (e.g. MYPLACE, RELIGARE, EURISLAM, DARE) and Societal Challenge 7 on secure societies (e.g. PRIME; IMPACT EUROPE; VOX-PoL).

48 For instance, under the EU Internet Forum, Vox-pol has been tasked to provide relevant research findings, the EU Internet Referral Unit has given itself an advisory research body, the RAN established an editorial board with researchers from different areas providing input for the work in the different RAN working groups, European Strategic Communications Network is developing its complementary research activities.

49 In the frame of its Focus Area 'Boosting the effectiveness of the Security Union' Horizon 2020 will fund collaborative social sciences and humanities research projects about the drivers and contexts of violent extremism in the broader MENA region and the Balkans and about the linkages between extreme ideologies and social polarisation.

50 See in particular the Conclusions on the criminal Justice response to radicalisation leading to terrorism and violent extremism (20 November 2015), on the role of the youth sector (30 May 2016), on developing media literacy and critical thinking through education and training (30 May 2016), on the prevention of radicalisation leading to violent extremism (20 November 2016).

51 Cf. the repository of national prevent strategies: http://ec.europa.eu/dgs/home-affairs/what-we-do/networks/radicalisation_awareness_network/ran-and-member-states/repository/index_en.htm.

RAN YOUNG). RAN has looked into the root causes of radicalisation, the role of religion, setting up local multi agency approaches, identified research gaps and evaluation methods for prevent work and interventions. A manual on responses to the major problem posed by returning terrorist fighters and their families, offering guidance to practitioners and Member States and comprising advice on risk assessment tools as well as a checklist for Member States, was prepared by the RAN Centre of Excellence and presented at the RAN Conference on 19 June 2017.

Under the **EU Internet Forum**, cooperation with industry has helped address the problem of terrorist content online. The Forum has two key objectives: to reduce accessibility to terrorist content online and to empower civil society partners to increase the volume of effective alternative narratives online. Under the first objective, the EU Internet Referral Unit at Europol has referred over 30,000 items of terrorist material to internet companies. In 80-90% of cases, the material is swiftly removed. Furthermore, four of the largest companies have established a database of hashes preventing that material once taken down on from one platform is not simply re-uploaded onto another. Efforts continue to reach out to smaller/newer platforms in order to enhance their resilience against terrorists' exploitation of their platforms. Efforts are also focused on how automated detection tools could help companies identify terrorist material at the point at which it is uploaded. The Civil Society Empowerment Programme has also been launched, with €10m support, which will support civil society in producing effective, alternative narratives online. With the support of the industry, 170 civil society partners have already received training in this respect. While achievements are considerable, the implementation of different initiatives has also highlighted challenges such as returning Foreign Terrorist Fighters (FTFs), rise of right wing extremism and risks of further societal polarisation.

As called upon by the Council in its 2015 Conclusions on enhancing the criminal justice response to radicalisation leading to terrorism and violent extremism, Eurojust monitored terrorism convictions with a view to acknowledging whether alternatives to imprisonment and rehabilitation programmes are imposed by the courts. It fostered the exchange of national practice and lessons learned, particularly in relation to risk assessment tools used by judges and prosecutors for assessing the level of threat posed by foreign terrorist fighters as well as de-radicalisation programmes.
The input inter alia from Member States to the comprehensive assessment exercise revealed a recognised need for the EU to do more and better in terms of preventing radicalisation leading to violent extremism and terrorism. The critical appraisal of existing instruments equally shows scope for improvement in terms of coordination and cooperation, outreach and impact.

Coordination becomes increasingly important given that many of the challenges we face are multi-dimensional and inter-related. The assessment indicates that there is a need to use the full potential of existing instruments while seeking complementarity and synergies of existing initiatives and policy instruments[52] (education, criminal justice, security, social inclusion and integration, external engagement). Increased coordination must also target project funding, complementarity between different stakeholders and their initiatives as well as research.

[52] See in this regard also the results of the Eurobarometer published in July 2016 stressing the need to make better use of existing tools and improved coordination across policy fields.

In terms of **outreach**, all relevant stakeholders must be involved. For voluntary arrangements under the EU Internet Forum, this means reaching out to smaller/younger companies whose platforms are increasingly used by terrorist organisations for their purposes. For the implementation of the Civil Society Empowerment Programme, this means forging partnerships between civil society actors and the creative, communications industry. For the work within the RAN this means offering a platform for exchanges among the most experienced practitioners with a view to develop concrete recommendations and guidance while at the same time equipping less experienced practitioners with the necessary skills.

In order to focus even more on the **impact** of actions, the assessment shows a need to invest more into a better analysis of the base line scenario, targeted research supporting the development of evidence based actions and more systematic evaluation mechanisms. For instance, to inform discussions, stakeholders of the 2nd high level EU Internet Forum in December 2016, VOX-POL[53] presented research on how terrorists' use of the internet has evolved while looking also into future trends providing the basis for developing appropriate responses. In addition, the evaluation methodologies developed under the EU funded IMPACT project[54] were applied and tested with RAN practitioners through a series of trainings; there is scope to expand such trainings and develop and apply similar mechanisms where appropriate at policy level.

6. Protect

a. Main findings

As terrorist organisations are changing their modus operandi, Europe is facing new challenges. The assessment points to the need to be prepared for attacks on critical infrastructure, more attacks on soft targets, the use of explosives as well as CBRN agents and materials.

In terms of legislation, it results from the assessment that there is a need for a wider consideration on the protection of **critical infrastructure** in EU in general, and in particular a need for re-launching the discussion on the Directive of 2008/14 in order to identify the best way forward.

In the area of **CBRN (chemical, biological, radiological and nuclear),** taking into account the changing threat picture in Europe, the assessment points to a need for increased cooperation at the EU level, based on better understanding of the CBRN threat and pooling of resources with a view to achieve better preparedness for possible CBRN attacks.

[53] The VOX-Pol Network of Excellence is an academic research network focused on researching Violent Online Political Extremism. For details on their activities see: www.voxpol.eu.

[54] IMPACT Europe is a project funded by the European Union's Seventh Framework Programme, which aims to fill the gap in knowledge and understanding of what works in tackling violent radicalisation and to help practitioners engaged in counter radicalisation interventions to improve the impact of their activities. For details on the project see: http://impacteurope.eu/

In the area of **soft target protection**, the work on raising awareness and fostering cooperation should be continued and further developed. The assessment indicates that there is a need to develop a comprehensive approach to support soft target protection which could include aspects such as a risk assessment methodology, insider threats and vetting procedures, detection capacity, raising public awareness and training citizens, engaging with private stakeholders and harnessing new technology, in particular on detection and security by design.

Latest attacks and threats highlight the continuous interest of terrorist to target **transport** infrastructures to cause mass casualties, create public anxiety and generate economic disruption. The EU aviation security framework is being constantly revised and reinforced to stay ahead of the threat. The risk posed by explosive concealed in electronic devices illustrate the need for regular risk analysis to design the most effective and proportionate response to address terrorists' capacity to innovate, through a combination of measures including new technologies. The EU remains exposed to vulnerabilities in third countries, in particular those facing high terrorism threat and with lower aviation security standards. To address the risks posed by incoming flights and in line with UN Security Council resolution 2309 (2016), additional capacity-building efforts in third countries are needed, while ensuring better prioritisation of projects and closer cooperation with Member States and international partners. There is also a strong need to provide a high level of cybersecurity to transport as part of the EU's cybersecurity strategy, in particular to enable the safe use of innovative technologies such as automated driving and drones.

It results from the comprehensive assessment that it is important to make available information on existing projects and programs as regards CBRN-E security. It is important to centralise any information on existing projects and programs, and identify and map all relevant CBRN-E actors in the EU, and their objectives and capabilities. This information should then be disseminated to the relevant community, with a view to develop further cooperation and pooling of knowledge and expertise for law enforcement/CBRNE Experts at EU level in both preparedness and response. The cooperation between military and law enforcement in CBRN-E domains should also be enhanced (technical innovation; joint training activities; information exchange; mutual operational support; etc.).

b. Overview of EU action

One of the four pillars of the EU counter-terrorism strategy is the protection of citizens, critical infrastructures and other assets. The aim is to strengthen their protection and resilience, by reducing their vulnerability to attacks and the impact of an attack. Within this wide scope, a specific focus is placed on reducing the vulnerability of critical infrastructures and developing an effective approach to the mitigation of chemical, biological, radiological, nuclear and explosives (CBRN-E) risks.

The **critical infrastructures** in the EU are becoming increasingly interconnected and the interdependencies in and between systems of infrastructures makes them even more vulnerable and complex. The policies in this area require the involvement of a large number of both public and private actors. The 2004 Commission Communication 'Critical Infrastructure Protection in the Fight against Terrorism' laid the foundation for the EU efforts in this field. However, since 2009, when the Stockholm Programme included as one of its objectives the need to reduce EU critical infrastructure vulnerabilities, the EU, its Member States and other key partners have undertaken numerous activities in this field, such as the

adoption and implementation of the Directive 2008/114/EC on the identification and designation of European critical infrastructures (ECI), the setting up of the European Programme for Critical Infrastructure Protection (EPCIP), and the Critical Infrastructure Warning Information Network (CIWIN).

Council Directive 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures (ECI) and the assessment of the need to improve their protection is the main element of European Programme on Critical Infrastructure Protection (EPCIP). The scope of the Directive is however limited to the energy and transport sectors. The Member State on whose territory a potential ECI is located designates it as an ECI following an agreement between that Member State and those Member States that may be significantly affected. There are currently 89 ECIs declared and registered by Member States.

Any designated ECI has to be properly protected, and needs to:

a) establish an Operator Security Plan (OSP) or an equivalent measure identifying important assets, a risk assessment plus identification, selection and prioritization of counter-measures and other appropriate procedures;

b) design a Security Liaison Officer or equivalent, in order to facilitate cooperation and communication with relevant national critical infrastructure protection authorities. The SLOs function as points of contact for security related issues between the owner/operator of the ECI and the relevant Member State authority;

c) inform the EU Commission about the designation of each ECI[55] .

Following the 2012 review of the EPCIP and of the Directive 2008/114 in particular, the Commission devised a new, more practical approach to the implementation of the EPCIP[56]. A pilot phase involving four critical infrastructures (CIs) of a European dimension (Eurocontrol, Galileo, the electricity transmission grid and the gas transmission network) was started, aiming to develop tools for improving the protection and resilience of CIs at EU level. This complex and pioneering pilot phase should conclude during 2017 and result in a comprehensive set of tools, such as for better risk assessment, contingency planning, training.

The Directive 2008/114 has proved to be a useful, but not fully sufficient tool. Some weaknesses were identified such as its limited scope, which minimised its impact.[57] Many ECI have been designated in the last years and Member States have set up their own national laws inspired by the Directive. During the review phase different policy options were explored. In the current context of increasing terrorist threat, the discussion with Member States and stakeholders on the relevance and suitability of the Directive needs to be re-launched. Further consideration is needed whether this Directive could be repealed or replaced by a new legislative instrument, and complemented with additional enhanced voluntary measures.[58]

---

55 The information concerns only numbers of ECIs, not their identities or technical details

56 SWD (2013) 318 final.

57 Study to support the preparation of the review of the Council Directive 2008/114/EC on the "identification and designation of European critical infrastructures (ECI) and the assessment of the need to improve their protection, https://ec.europa.eu/home-affairs/financing/tenders/2011/2011_03_en.

58 Another element under the EPCIP is the Critical Infrastructure Warning Information Network CIWIN, which was set up following a Council Decision in 2008 (COM(2008)676 final, This decision was withdrawn in 2012 and CIWIN was transformed into a simple eCommunity, managed by the Commission, and where the CI

The need for a strategic approach in the areas of **CBRN-E** was underlined in the EU CBRN Action Plan[59], the EU Action Plan on Enhancing the Security of Explosives,[60] the Commission's Communication on a new EU approach to the detection and mitigation of CBRN-E risks[61] and the EU action plan against illicit trafficking in and use of firearms and explosives[62]. With a view to ensuring effectiveness, EU measures in this field have to be based on risk and threat assessments and focus on the enhancement of knowledge, research, the exchange of best practices and joint training and exercises for all relevant stakeholders (public authorities, first responders, researchers, the general public, security managers and staff).

Since the launch of the Action Plans, there have been numerous achievements in the CBRN-E area at the EU level. A key achievement was the adoption of the **Regulation 98/2013 on Explosives Precursors.** To prepare and implement this Regulation, the Standing Committee on Precursors was established with a view to examine the threat posed by chemical substances that can be used to manufacture homemade explosives[63].

Regulation (EU) No 98/2013 aims to restrict access by the members of the general public to chemical substances that can be misused for the illicit manufacturing of home-made explosives and to ensure the reporting of suspicious transactions, disappearances and thefts along the supply chain. As put forth in a 2017 Commission report,[64] the Regulation has contributed to reducing the threat posed by explosives precursors in Europe, by reducing the amount of such substances on the market and by increasing the capacity of competent and law enforcement authorities to investigate suspicious incidents. Recent attacks show, however, that regulated substances continue to be accessed by individuals and groups that aim to carry out terrorist attacks.

The Regulation's main strength is that it disrupts the sourcing of chemicals at an early stage in the planning of a terrorist attack. The main limitations of Regulation EU 98/2013 are related to awareness in the supply chain and on sharing information across borders, the large size of the supply chain, especially at retail level, which requires a proactive engagement by Member States to reach out to economic operators, and the multiplicity of different regimes across the EU, which creates challenges for the supply chain actors which conduct business across the EU. The assessment indicates that there is a need to step up efforts in order to make full use of the restrictions and controls in place, and to collect quantitative and qualitative data which helps evaluate more accurately the Regulation's effectiveness and efficiency in reducing the threat posed by home-made explosives. In 2016 the Commission initiated infringement procedures against six Member States for failure to implement certain obligations under this regulation. Since then, three infringement procedures have been closed, while the procedures against Spain, France and Romania are at the stage of Reasoned Opinion[65].

---

stakeholders can share documents of interest. See http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.C_.2012.156.01.0010.01.ENG

59 Council doc. 15505/1/09 REV 1.

60 Council doc. 8109/08.

61 COM(2014) 247 final.

62 COM(2015) 624 final.

63 It supports also the work on the implementation of the regulation on explosives precursors.

64 COM(2017) 103 final.

65 For details, see Commission's public database of infringement decisions: http://ec.europa.eu/atwork/applying-eu-law/infringements proceedings/infringement_decisions/?lang_code=en.

The improved exchange of information and best practices were priorities in the 2008 EU Action Plan for the Enhancement of the Security of Explosives. This resulted in the establishment of different database tools such as the European Bomb Data System (EBDS) and the system for the control of intra-EU transfers of explosives SCEPYLT, as well as creation of the European Explosive Ordinance Disposal Network (EEODN), gathering not only explosives but also CBRN experts.

Similarly, the comprehensive (more than 120 individual actions) **2009 EU CBRN Action Plan** aimed to prevent and limit the impact of CBRN risks by restricting access to these materials, improving their detection and enhancing the response to incidents involving CBRN substances. Its adoption stimulated work in the CBRN area both at national and EU level. One of the most significant achievements has been the creation – at the Commission premises in Karlsruhe and Ispra – of a training centre focused on radiological and nuclear threats. A few hundreds law enforcement and customs officials from Member States and third countries as well as inspectors from the European Commission and other international organisations are being trained every year.

The **EU CBRN Action Plan** aimed to address the fragmentation of efforts and initiatives both at the EU and at national level. Its comprehensive nature and all-hazard approach stimulated cooperation between various actors involved in the CBRN area. Member States reported that coordination of various actors – even at national level – was one of the main obstacles to effectively implement at least some of the actions. In the final progress report, the impact of the Action Plan was assessed as very positive, but certain gaps and areas where work needs to be continued or stepped up at EU level were identified. These include the need to further deepen knowledge of CBRN risks through regular risk assessment, to conduct research on lower risk alternatives for CBRN materials, to promote cross-sector cooperation and conduct training and exercises, etc. On this basis, and given the changing threat picture in Europe a new initiative looking at enhancing our knowledge regarding the CBRN threat, bringing actors together and enhancing operational preparedness, needs to be explored.

Building on the experience gathered, the EU has also shared its expertise with **international partners**, and has established regional networks of experts and expertise. Since 2008, the EU and the United States have established cooperation on threats posed by terrorist and criminal use of explosives. The EU CBRN Centres of Excellence have been set up with the aim to contribute to increase CBRN security in different parts of Africa, the Middle East, Central and South East Asia, and South East Europe These regional networks and cooperation with strategic partners, such as the US, are valuable tools for increased security cooperation.

There is no EU legal instrument dealing with the **soft target protection**. Soft targets have increasingly been targeted by terrorists. Their protection remains high on the agenda of the EU. It is an area with great complexity and many challenges and there is a consensus that establishing an EU platform for Member States to learn from each other will help on enhancing EU's resilience and protection against future soft target attacks.

Health security is best achieved by improving prevention, preparedness, and risk management, while also enabling swift responses to emergencies, including terrorist attacks, border security, soft target protection, and innovative research. The deliberate release of anthrax in the US in 2001 has changed the international perception of the risk of terrorism. Bioterrorism has emerged in its own right as a key challenge for health security, leading to more concerted global action to strengthen preparedness planning and response.

At EU level, Decision 1082/2013/EU[66] provides the key framework to improve preparedness and strengthen our capacity to coordinate responses to health emergencies caused by biological, chemical and environmental agents, as well as threats of unknown origin. The Decision lays down rules on epidemiological surveillance, monitoring, early warning, and combating serious cross-border threats to health in order to coordinate and complement national policies. Frameworks contributing to health security exist also in the areas of food safety, animal health, and pharmaceutical products. The Commission closely cooperates with Member States, EU agencies[67] and international partners[68] to prevent and control serious cross-border health threats by using strategic structures and mechanisms. These include the Health Security Committee (HSC) for information exchange, consultation and coordination between Member States; the Early Warning and Response System (EWRS) for notifying alerts on health threats and measures undertaken by Member States; and the EU Health Programme for supporting Member States through training and exercises, and by facilitating the sharing of experiences, guidelines and procedures.

In 2015, the first report on the implementation of Decision 1082/2013/EU stressed that established structures and mechanisms had operated effectively in specific real-life cases of serious cross-border health threats.[69] A 2016 Special Report of the European Court of Auditors recognized the complexity of implementing Decision No 1082/2013/EU in light of the competences of the EU and the Member States, the multitude of actors and complex structures in place both within Member States and internationally, and the fact that serious threats keep emerging. The Court called for a more rapid development and implementation of new elements introduced by the Decision; requested that a strategic roadmap for the HSC be developed towards a more effective coordination of preparedness and response; and that EWRS be modernized to ensure that it and other rapid alert and information systems at Union level are linked up and complement each other.

EU efforts in infrastructure protection and other protection areas such as CBRN-E have been underpinned by a significant increase in funding for **security research** by the Commission. The development of the ESRP (European Security Research Programme) within the 7th Framework Programme of Community Research (2007–13) (FP7) has been supported with an allocation of EUR 1.4 billion.

Many actions and projects have been undertaken to help combatting the threat of terrorism by developing technology capable of analysing and quickly processing threats, such as CBRN and explosives threats. One example in the area of critical infrastructure protection is engaging scientists, architects and planners to design future buildings and public places that are safer and better protected. Together with industry improved materials have been designed, ranging from tougher glass that stops broken pieces from flying in an explosion, which can cause injury and deaths, to bollards and barriers that can withstand the impact of a speeding truck.

Due to the private ownership of major elements of critical infrastructure and CBRN facilities

66 Decision 1082/2013/EU on serious cross-border threats to health.

67 In particular the European Centre for Disease Prevention and Control (ECDC), the European Food Safety Authority (EFSA), the European Medicines Agency (EMA).

68 Including through the World Health Organisation (WHO).

69 Including the Ebola outbreak, the Middle East Respiratory Syndrome (MERS CoV) crisis, and the poliomyelitis threat in 2015.

such as chemical factories or nuclear plants, greater **partnership** is required in the future **with the private sector**. Security and control measures require the involvement of both private and public interests. The private sector must be offered support to develop its own responses to terrorist events.

Together with Member States, the Commission explores what exact types of EU support could be mobilised to help build resilience and strengthen security around potential soft targets. The Commission is offering funding for projects in this field. For instance, a pilot project by Belgium, the Netherlands and Luxembourg is financed under the Internal Security Fund to establish a regional Centre of Excellence for law enforcement special interventions, which will offer training for Police officers who are often the First Responders in case of an attack.

Delivering security to transport services and confidence to transport passengers and businesses to use transport is essential for the multiplier effects that this sector generates for economic and social prosperity. Terrorists often target **public transport**, and in particular air transport. Building on efforts in the framework of the United Nations (such as the 1970 Convention for the Suppression of Unlawful Seizure of Aircraft and the 1971 Convention for the Suppression of Unlawful Acts against the Safety of Civil Aviation) and the International Civil Aviation Organization (in particular Annex 17 to the Chicago Convention), the EU has developed a robust aviation security framework. Regulation (EC) n°300/2008 lays down common rules and standards on aviation security and procedures to monitor their implementation. This legislation replaced the initial framework Regulation n°2320/2002 adopted in the wake of the September 2001 attacks, to meet evolving risks and allow new technologies. The EU legislation on **aviation security** is constantly monitored and adapted under a risk based approach, in full consultation with the industry, the Member States, international partners and international organisations. Since 2009, several regulations have supplemented Regulation 300/2008 as regards liquids, aerosols and gels, the use of security scanners, the adoption of alternative security measures, controls of air cargo internally as well as internationally and the specifications of national quality control programmes. Cooperation through the Committee for Civil Aviation Security (AVSEC) and the commitment of Member States to the aviation security inspection regime with its continuous reviewing effect work well and provide indication on possible improvement of security measures.

EU security policy is less developed in other transport domain. The overall objective of the EU's **maritime transport security policy** is to protect citizens and economies from the consequences of unlawful intentional acts against shipping and port operations.[70] The basis of the EU legislation was the International Ship and Port Security (ISPS) Code on security in ports and on ships laid down by the International Maritime Organization (IMO). The ISPS

[70] The stated objective refers to EU Maritime transport security policy and not EU Maritime security policy at large. The main objectives of EU's Maritime security policy are also defined in the EU Maritime Security Strategy (EUMSS), adopted on 24 June 2014. While not strictly falling within the scope of this assessment, the EU Maritime Security Strategy (EUMSS), is very relevant in that regard, with one of its aims being to improve the way in which the EU pre-empts and responds to the maritime security challenges. Another important actor in the maritime domain is the Maritime Safety Agency (EMSA), which is an important information hub and provider of integrated services and awareness pictures to other EU Agencies. The agency's main objectives are to assist the Commission in monitoring the implementation of EU legislation in the maritime field, operate, maintain and develop maritime information capabilities at EU level, establish marine pollution preparedness, detection and response capability, and provide technical and scientific advice to the Commission in the field of maritime safety and prevention of pollution by ships.

Code was introduced in the EU legislation in 2004 with the Maritime Security Regulation 725/2004. It was complemented by Directive 2005/65/EC that addressed elements of port security not covered by the Regulation. The EU **maritime security** legislation transposing and enhancing the ISPS Code, provides an harmonised interpretation, implementation and monitoring of the international rules. It is applicable to ships engaged in international and domestic voyages and the ports and port facilities serving them. The Member States ensure that security assessments are periodically reviewed taking into account changing threats. The Commission undertakes inspections to monitor the application of this legislation. An option would be to consider some security issues for ferries and cruise ships based on a dialogue with the Member States and the stakeholders.[71]

In the area of **land transport** (including rail), there is no EU legislation. Yet, as illustrated by the Madrid and London bombings, and most recently the Thalys and Brussels metro attacks, terrorists have shown an interest in targeting rail transport, exploiting specific vulnerabilities to cause mass casualties. Most experts of land transport security consulted via the Expert Group on Land Transport Security (LANDSEC) established by the European Commission are supportive of greater action at EU level. Based on the Commission Staff Working Paper of 2012 and discussions with stakeholders after the recent security incidents, a better framework is considered needed to improve rail security: e.g. encouraging railway companies to have contingency plans and recovery plans, based on risk analyses carried out by the Member States. Consideration could be given to the deployment of better security technology and security training of rail transport staff. The recent attacks in Brussels have also shown the need to address, in a consistent manner, the issue of protection of public areas of transport infrastructures such as airport terminals or train stations. The EU has engaged in developing guidance together with law enforcement practitioners on how to better protect different transportation hubs, such as airports and train stations. Transport security policy is a matter of shared competence between the EU and its Member States. Although Member States are responsible for taking measures to manage their security, the EU dimension has to be factored in as a large proportion of transport operations occur between Member States and there is clear added value for certain actions to be envisaged at the EU level.

7. Crisis Management

a. Main findings

In a context of high level terrorist threat, where more attacks are assessed as likely, the EU and its Member States need to be prepared to respond in a coherent and effective manner. The EU has developed a range of coordination tools, at both political and operational levels, to assist its Member States facing major crises or disasters.

The assessment suggests that specific exercises and tests could further contribute to enhance preparedness and raise awareness of the benefits of the IPCR and the solidarity clause in the event of major terrorist attacks.

At operational level, EU tools can offer added value by supporting cooperation or leveraging Member States' action, notably to face complex threat scenarios requiring specific expertise or

[71] The above paragraph refers mainly to the EU Maritime transport security policy and not the EU Maritime security policy at large. The main objectives of EU's Maritime security policy are defined in the EU Maritime Security Strategy, adopted on 24 June 2014.

capabilities not available to each individual Member State. The EU can also help the coordination of the different first responders in such scenarios, e.g. the cooperation between police special intervention units and civil protection in the event of complex attacks (e.g. the Arete 2014 field exercise scenario of hostage-taking situation with CBRN threat).

Supporting the response to attacks, particularly on soft targets, should continue to be a key component of the work to reduce vulnerabilities in the immediate aftermath of terrorist attacks. These actions need to target joint trainings and exercises so as to ensure a sustained dialogue via existing focal points and expert groups. Possible areas for further work could include the exchange of good practices, support for the development of specialised modules for responding to terrorist attacks, including within the framework of the Union Civil Protection Mechanism, and initiatives to share lessons learnt and raise public awareness. Dedicated funding opportunities need to be exploited. Member States could also apply for financing from the European Investment Bank (EIB) (including the European Fund for Strategic Investments) in line with EU and EIB Group policies.

b. Overview of EU action

Recognising that the risk of terrorist attacks cannot be reduced to zero, the fourth pillar of the 2005 EU Counter-Terrorism Strategy, "Respond" implies the immediate mobilisation of EU resources and capabilities to deal with the consequences of such man-made disasters by having in place crisis management arrangements.

Member States are responsible for managing emergencies on their territories and for deciding whether they need external assistance. Since disasters (both man-made and natural) are often of a cross-border nature, they might require multilateral and coordinated responses. When requested, the EU should activate all relevant instruments at its disposal to support affected Member States in responding to emerging or on-going crises.

In 2006, the Council adopted the EU emergency and crisis co-ordination arrangements (EU-CCA).[72] While the proposal was already mentioned in the Hague Programme, the December 2004 tsunami, Hurricane Katrina, the earthquake in Pakistan and the 2005 London bombings highlighted the need for integrated EU crisis management arrangements to ensure information sharing, coordination and collective decision-making.

In 2010 in its Communication "The EU Internal Security Strategy in Action", the Commission committed to **increase Europe's resilience to crises and disasters**, in particular making full use of the solidarity clause, linking up the different situation awareness centres and developing the Emergency Response Coordination Centre (ERCC).

The 2015 European Agenda on Security highlighted the role of coordination hubs to facilitate a coherent European response during crises and emergencies, avoiding unnecessary and expensive duplication of efforts. It stressed the need to reinforce crisis management preparedness (including through field exercises and training) to ensure a more efficient and coherent EU response to crises sparked by criminal acts, impacting on borders, public security and critical systems.

As regards public awareness to the terrorism threat, the Commission proposed to support efforts to improve the various definitions of **national "threat levels"**. The Council adopted in

[72] https://www.consilium.europa.eu/uedocs/cmsUpload/WEB15106.pdf.

December 2010 conclusions establishing an information sharing mechanism allowing Member States to exchange on changes in their national threat level. Yet not all Member States possess a threat level or terror alert system, the existing systems rely on different definitions and scales and linguistic issues constitute a significant obstacle in terms of public information. Proposals for the development of a European system of threat level were not supported. The assessment suggests that alternative options could be explored to improve the access of the public to such information (e.g. online repository or dashboard) and common understanding of threat levels and the associated flanking measures.

The EU has adopted crisis response arrangements at the EU political level to ensure information sharing and support to political coordination.

First, the Lisbon Treaty introduced a specific **solidarity clause**, building on the solidarity commitment expressed by the European Council in its Declaration on combating terrorism adopted on 25 March 2004 in the wake of the Madrid bombings. Enshrined in Article 222 TFEU, the clause introduces a legal obligation[73] 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. The clause is meant to be used on request in case of "large-scale crises, which are often trans-border and trans-sectoral and thus exceed the response capacity of one individual Member State.", The Council Decision of 24 June 2014[74] lays down the arrangements for the implementation by the Union of the solidarity clause, including the identification and mobilisation of "all relevant Union instruments. The solidarity clause has not been activated so far.

Second, the **EU Integrated Political Crisis Response (IPCR)** arrangements were adopted in 2013, replacing the 2006 Crisis Coordination Arrangements after a two-year review process of the EU-CCA. The IPCR follows the key principles of flexibility, scalability and subsidiarity to tailor the response to major crisis requiring political coordination. Upon activation by the Presidency of the Council, the IPCR allows a timely policy coordination and response at EU political level and contributes to establish a common picture of the situation (improving data collection and analysis) with the support of the Commission, the EEAS and EU agencies.

The IPCR builds on three key support instruments:

- a central 24/7 contact point (the Emergency Response Coordination Centre);
- the IPCR web platform (a virtual crisis room facilitating information sharing); and
- the Integrated Situational Awareness and Analysis (ISAA).

The ISAA is developed by Commission services and the EEAS as a capability to support the decision-making and to develop a common and regularly updated situation picture of the crisis (including its possible evolution and consequences) to inform the political response. ISAA relies on relevant information and analysis provided by the Member States, EU agencies and other sources.

---

[73] According to the text of the implementing decision, a Member State can choose the most appropriate means to comply with its own solidarity obligation towards another Member State. In addition, Article 42 (7) TEU provides that "if a Member State is the victim of armed aggression on its territory, the other Member States shall have towards it an obligation of aid and assistance by all the means in their power, in accordance with Article 51 of the United Nations Charter.

[74] Council doc. 2014/415/EU.

The first activation of the EU IPCR in 2015 in response to the migration crisis confirmed the added value of EU crisis coordination arrangements, in particular the establishment of a common picture of the situation through the development of ISAA with "the crucial support of the Commission, the EEAS and EU agencies."[75]

While IPCR and ISAA were initially described as a "promising tool", the lack of practical resources and issues of interaction between the different institutions have also been flagged. The current experience has proven that the strong buy-in of all key stakeholders, and the constructive cooperation between all crisis structures in the Commission services, the EEAS, the Council General Secretariat, EU agencies and Member States allowed for information sharing and discussions to design and coordinate effective policy responses.

The dedicated support tools (the IPCR web platform, the 24/7 contact point and the ISAA) have proved solid assets. The IPCR can rely on well-established Council procedures but with the necessary flexibility and scalability to adapt to the needs. Yet, the IPCR has not been tested yet to handle other crisis scenarios (and in particular acute security crisis requiring the exchange of classified information and immediate response, such as a terrorist attack). The ongoing work under the Joint framework on countering hybrid threats[76] and the specific Operational protocol provide an opportunity to consolidate the IPCR for security crises.

Third, at Commission level, a **rapid alert system - ARGUS** was created to better coordinate the Commission's response capacity, including its contribution to the preparation of the Integrated Situational Awareness and Analysis (ISAA). ISAA is a capability developed to support decision making in IPCR. ARGUS brings together all relevant Commission services to coordinate efforts, evaluate the best options for action and decide on the appropriate response measures during an emergency. It facilitates the coordination of existing sectorial crisis response capacities, including the network of specialised crisis centres in the Commission and agencies (e.g. in the field of civil protection/humanitarian aid, security and migration, public health).

Fourth, the EEAS has developed its **Crisis Response System** (Crisis Platform, EU Situation Room, Crisis Management Board, EU Hybrid Fusion Cell) covering crises occurring outside the EU, which may affect EU security and interests, including those affecting the EU delegations or any other EU asset or person in a third country. It equally covers crisis occurring inside the EU if those have an external dimension.

The EU has also developed instruments to support Member States' response at the **operational level**:

- **law enforcement and judicial response** to terrorist attacks: for instance through the ATLAS network of 37 special intervention units, as well as Europol's "First Response Network" and the analytical support for investigations provided by its European Counter Terrorism Centre.[77] As regards the ATLAS network, a decade of cooperation and

[75] Netherlands Presidency of the Council of the EU, *Presidency report: A comprehensive and systematic approach to migration – State of play & way forward*, February 2016: https://english.eu2016.nl/binaries/eu2016-en/documents/reports/2016/02/13/presidency-report-migration/presidency-report-final-130216.pdf.

[76] JOIN (2016) 18 final.

[77] Council Decision 2008/617/JHA of 23 June 2008 on the improvement of cooperation between the special intervention units of the Member States of the European Union in crisis situations (ATLAS decision), OJ L 210, 6.8.2008, p. 73–75.

confidence building has contributed to establishing a true knowledge hub and platform for the exchange of best practices for practitioners on special tactics, tools and equipment and the development of common standards. Through the pooling of resources and expertise and the facilitation of cooperation, the network has demonstrated a clear added value for the development of highly specialised knowledge and techniques that is not widely available to each Member State. The network relies heavily on the commitment of its participants and the lead countries. More structured EU support, including cooperation with relevant Agencies (Europol and CEPOL) and specialised networks (e.g. Airpol, Railpol, Air Marshals) as well as research efforts to develop innovative techniques could help create further synergies. Although the Atlas decision has provided a common legal basis for cross-border cooperation, significant obstacles stem from the various national legislative frameworks.

- **management of the consequences of emergencies, including terrorist attacks**, notably through the Union Civil Protection Mechanism. The EU Civil Protection Mechanism ("**UCPM")** is currently undergoing an interim evaluation and will assess how current capacities of the UCPM match current and emerging risks, including those triggered by security threats.

The new provisions on victims of terrorism under Directive 2017/541/EU on combating terrorism are also relevant from the perspective of crisis management. In particular, the Directive requires that Member States ensure that mechanisms or protocols are in place allowing for activation of support services for **victims of terrorism** within the framework of their national emergency-response infrastructures. Such mechanisms or protocols shall envisage the coordination of relevant authorities, agencies and bodies to be able to provide a comprehensive response to the needs of victims and their family members immediately after a terrorist attack and for as long as necessary, including adequate means facilitating the identification of and communication to victims and their families.

8. Terrorist Financing

a. Main findings

In its 2016 Action Plan, the Commission identified the areas where work was needed to further enhance the fight against terrorist financing. The Action Plan included all ongoing and upcoming measures and initiatives, centred around preventing the misuse of the financial system for money laundering and terrorism financing, increasing the cooperation and access to and exchange of information of competent authorities, such as customs, FIUs and LEAs, tracing the financial movements of terrorists, improving the effectiveness of asset freezing systems and reinforcing the criminal justice response to terrorist financing and money laundering.

With the majority of the measures proposed in the 2016 Action Plan now complete, the EU has responded swiftly to the evolving challenges of terrorist financing. However, final adoption and full implementation of the legislative and non-legislative instruments developed must be achieved. Overall, it is considered that efforts must be continued in this field to limit the capacity of terrorists to operate and finance their activities and to ensure that financial information can be used to detect terrorists and their supporters, in full respect of fundamental rights, in particular the protection of privacy and personal data.

b. Overview of EU action

Countering the financing of terrorism is a core component of the EU's strategy in the fight against terrorism. Efforts to disrupt, deter and dismantle terrorist financing networks aim to limit the resources available to terrorists and terrorist organisations and can help to track operatives, chart relationships and deter individuals from supporting terrorist organisations both directly and indirectly.

In 2004, the European Union designed a specific **Strategy on Terrorist Financing**[78], which was revised in 2008 and 2011. This highlighted that reducing the financial flows to terrorists and disrupting their activities can provide vital information on terrorists and their networks, which in turn improves law enforcement agencies' ability to undertake successful investigations.

The Union has developed a number of dedicated instruments specifically designed to implement and/or enhance the two key frameworks to counter terrorist financing ("CTF") that have shaped CTF efforts worldwide – the so-called 'smart' sanctions model advanced by the United Nations (UN) Security Council and the anti-money laundering (AML) model advanced by the Financial Action Task Force ("FATF"). These two internationally agreed approaches for combating terrorism financing (**freezing financial assets** on the one hand and **identifying and tracking transactions** on the other) are not mutually exclusive. Depending on the specific situation, governments may consider it more useful to track the financial transactions of a terrorist (group) than to designate them publicly. After an initial wave of designations in the wake of 9/11, the emphasis of European efforts against terrorism financing has increasingly shifted to detecting and tracking terrorists' transactions.

The UN resolutions required the **blacklisting** of individuals and groups suspected of terrorism, in particular Osama Bin Laden, the Al Qaeda network and the Taliban. Moreover, the listing procedures send an important political signal and have a deterrent psychological impact. However, the practices of blacklisting have also raised controversy, as they raised issues as regards the lack of democratic oversight, in particular by the European Parliament[79] and the respect of certain fundamental rights, in particular the presumption of innocence and the right to an effective remedy and to a fair trial, as reflected in the consistent case-law of the Court of Justice f the European Union. [80]

The EU legislation concerning procedures for listing persons and entities related to terrorism with a view to freezing their assets was reviewed to strengthen its fundamental rights components (such as the rights of the defence). The listing procedures relating to the freezing of funds are currently based on Common Position 931/2001, Regulation 2580/2001, Council Decision 2580/2001 and Regulation 881/2002, Council Decision 1693/2016 and Council Regulation 1686/2016.

Common Position 2001/931/CFSP on the application of specific measures to combat terrorism is designed to address terrorist threats in general, pursuant to UNSC Resolution 1373(2001) and draws a comprehensive list of persons, groups, and entities considered

78 http://www.consilium.europa.eu/uedocs/cmsUpload/DECL-25.3.pdf.

79 See, for instance, http://www.europarl.europa.eu/sides/getDoc.do?type=IM-PRESS&reference=20080218IPR21527&format=XML&language=EN.

80 See the landmark judgment of the Court (Grand Chamber) of 3 September 2008 in Joined cases C-402/05 P and C-415/05 P, Yassin Abdullah Kadi and Al Barakaat International Foundation v Council of the European Union and Commission of the European Communities, and the significant related jurisprudence.

terrorist. Council Decision 1693/2016 and Council Regulation 881/2002 created for the implementation of UNSC Resolution 1267 (1999) transposes the UN ISIL/Al-Qaida designations on behalf of the Member States, which are bound by UN Resolutions. This has recently been complemented by the **EU-autonomous ISIL (Da'esh)/Al-Qaida regime**, constituted by Council Decision 1693/2016 and Council Regulation 1686/2016. This regime enables the EU to adopt autonomously restrictive measures against persons and entities linked to ISIL/Al-Qaida, independently from the UN.

The existing EU asset freezing regimes concerning terrorism, which apply to third-country nationals as well as to EU citizens, are adopted under the Common Foreign and Security Policy (CFSP). In addition, **Article 75 TFEU** enables the EU to adopt administrative measures against individuals, legal persons, groups and non-state entities where necessary to achieve the objectives of the area of freedom, security and justice. On 21 December 2016, the Commission presented an appraisal on the possible need for additional measures for freezing terrorist assets under Article 75 TFEU. With the main current threat from jihadi-inspired terrorism covered by existing regimes, a low overall threat from other terrorist groups, together with existing possibilities to use measures such as criminal law asset freezing against other groups, the Commission considered that it is not necessary to take further steps under Article 75 TFEU at this time.

Under the second strand, current Union CTF measures are mainly based on the **forty recommendations of the FATF**[81], the global standard setter in this field. These recommendations require states worldwide to regulate financial transactions in order 'to detect, prevent and suppress the financing of terrorism and terrorist acts'. The EU has transposed the FATF's recommendations by adopting the four successive anti-money laundering Directives[82] and the two successive funds transfers Regulations[83]. In addition, the Cash Control Regulation[84] requires the disclosure of cash or equivalent in excess of EUR 10 000 when entering or leaving the EU.

It is important to note the international dimension of EU CTF efforts. In addition to supporting the CTF efforts of the UN and FATF and other international organisations such as the IMF, Council of Europe or the Gulf Council, the EU has also sought cooperation with several key external partners, in particular the United States. The 2010 EU-US Agreement on the **Terrorist Finance Tracking Programme (TFTP)** allows Member States to request a search of financial data when there is reasonable suspicion of terrorist activity.

The 2010 TFTP Agreement provides the legal framework under which data from the EU is transferred to the US, as well as the conditions for access, providing a comprehensive set of safeguards and controls, the implementation of which is assessed through joint reviews with the US.

---

81 http://www.fatf-gafi.org/media/fatf/documents/FATF%20Standards%20-%2040%20Recommendations%20rc.pdf.

82 Council Directive 91/308/EEC of 10 June 1991, Directive 2001/97/EC of 4 December 2001, Directive 2005/60/EC of 26 October 2005 and Directive (EU) 2015/849 of 20 May 2015, OJ L 166, 28.6.1991, p. 77–82.

83 Regulation (EC) No 1781/2006 of 15 November 2006, repealed and replaced by Regulation (EU) 2015/847 of 20 May 2015, OJ L 345, 8.12.2006, p. 1–9.

84 Regulation (EC) No 1889/2005 of the European Parliament and of the Council of 26 October 2005 on controls of cash entering or leaving the Community, OJ L 309, 25.11.2005, p. 9.

All four existing review reports[85] concluded that the TFTP helps to identify terrorist organisations and financial facilitators operating internationally, and has provided leads relating to numerous terrorist suspects and their supporters which have been crucial for counter-terrorism investigations, including those relating to attacks on EU soil.

The TFTP is a key tool for tracking terrorist financing. The regular review reports point both to its value to the EU and US authorities as well as the effectiveness of the safeguards and governance arrangements in place. While its value has been demonstrated, it is worth exploring whether there is additional potential for EU authorities to make better use of the TFTP for the purposes of counter-terrorism investigations, as well as to identify possible ways to facilitate and optimise its use. In parallel, following a first appraisal presented in December 2016 the Commission is studying the possible need for additional complementary measures to track terrorist financing in the EU, notably to cover transactions not covered by the TFTP, such as intra-EU payments in euro.

In terms of potential for further improvement, the Commission has recommended that Member States consider providing regular feedback on the TFTP data received from the US Treasury which could further improve the quality and the quantity of information exchanged under Articles 9 and 10. The Commission also encouraged Europol to continue its efforts to actively promote awareness of the TFTP and to support Member States seeking its advice and experience. It is important that Europol continues fulfilling its verification role as thoroughly and independently as at present.

Fighting against the illicit trade of cultural goods coming from conflict zones and endangered cultural heritage sites is also an important measure to block potential sources of funding for terrorists.[86][87]

[85] The latest report can be found at https://ec.europa.eu/home-affairs/sites/homeaffairs/files/e-library/documents/policies/crisis-and-terrorism/19012017_tftp_report_en.pdf.

[86] As stressed in the Action Plan for strengthening the fight against terrorist financing, COM(2016) 50 final, 02.02.2016.

[87] In the frame of the Horizon 2020 Focus Area 'Boosting the effectiveness of the Security Union', a stakeholder platform on endangered cultural heritage and on illicit trafficking of cultural goods will be launched in 2018, addressing, inter alia, the destruction of archaeological sites by terrorist groups as well as the funding of terrorist activities via illicit excavations of archaeological sites and the illicit removal from conflict zones of cultural goods.

III. ORGANISED CRIME

Organised crime is an important threat to security and combatting it is one of the priorities of the European Agenda on Security. 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. More than 5000 international organised crime groups with more than 180 nationalities are currently under investigation in the EU. Criminal activities were considered being "worth" two trillion euros worldwide in 2009[88]. Organised crime is also one of the enabling factors to terrorism.

In this area, the assessment shows that the EU intervention has been framed with regard to specific crime types, each with their own strategies, legislation and action plans, rather than being based on a comprehensive approach, something which is increasingly called for in order to effectively address the today's crime challenges. Such a comprehensive approach needs to be based on a solid intelligence picture regarding organised crime across the Union. In some specific areas, a need has been identified to ensure better application of the EU acquis, updating existing instruments, improving information access and exchange and operational cooperation.

1. Organised crime – General

a. Main findings

With regard to the overall EU action in the area of organised crime, it emerges from the assessment that the approach focused on specific types of crime, rather than pursuing a horizontal, comprehensive approach to organised crime and organised crime groups. However, many of the criminal groups are increasingly involved in more than one type of criminal activity. A more horizontal approach is therefore needed. Such an approach also needs to be based on a comprehensive intelligence picture of markets and actors involved.

In terms of specific horizontal instruments, and apart from those further covered in Chapter V. below, the assessment reveals that the legal standard of the Framework Decision 2008/841/JHA (e.g. penalty thresholds) appear quite low; the Framework Decision had little impact on Member States' legislation due to pre-existing instruments, notably Joint Action 98/733/JHA (which it replaced) and the UN Convention Against Transnational Organised Crime (UNTOC). [89]One possibility would be for the EU to focus in the future on various soft law measures to assist Member States in the way they apply the Framework Decision in practice, in order to increase the impact of this legal instrument.

b. Overview of EU action

The European Union and the Commission have a key role to play in enhancing cross-border cooperation between the Member States, against serious and organised crime activities, risks and threats. The single market and the suppression of internal border controls entailed a need for stronger police and judicial cooperation to address trans-border activities.

---

[88] UNODC, *Estimating illicit financial flows resulting from drug trafficking and other transnational organized crime*, 2011.

[89] See for details, Annex III.1 of SWD (2017) 278 final (26.07.2017).

In this regard, the European Anti-Fraud Office (OLAF) is involved in the exchange of operational information and operational co-operation with Member State authorities in its investigations. The co-operation needs to be stepped up to keep up with increased sophistication of transnational organised crime groups.

The first 20 years of EU action in the Justice and Home Affairs (JHA) area essentially focused on building up necessary tools and legal instruments so as to enhance law enforcement and judicial cooperation (customs cooperation included). The EU has developed a range of initiatives in order to support and help Member States to better fight organised crime, such as legislative measures harmonising rules concerning offences in relation to criminal organisations or specific crimes, the gathering of crime statistics and the funding of European projects or specialist networks.

EU policy initiatives were developed in a number of areas, including drugs, illicit trade in tobacco products[90], money laundering, financial investigations, firearms, trafficking in human beings (THB) and environmental crime. Another related area of action at EU level is the fight against corruption. In this area, the implementation of EU core anti-corruption acquis[91] introduced common definitions of the offence and the obligation for Member States to apply effective, proportionate and dissuasive criminal law penalties, as well as criminal liability of legal persons.

The European Anti-Fraud Office (OLAF) targets fraud, corruption and any other illegal activity negatively affecting the financial interests of the EU. It performs inter alia financial investigations in the area of protection of the financial interests of the EU, which may have real and potential security and organised crime implications. The European Public Prosecutor Office (EPPO), which is expected to be launched as an enhanced co-operation initiative (with 20 Member States at the moment) is a ground-breaking initiative in the area of EU-level criminal law investigations (potentially with security/organised crime implications).

Legal and policy framework

The Framework Decision 2008/841/JHA on the fight against organised crime aims at approximating definitions and sanctions for offences of organised crime in the Member States through encompassing offences typically committed by a criminal organisation. The aim of this instrument is to target the criminal association through which criminal activities are carried out (as opposed to directly targeting individual criminal acts).

This Framework Decision was adopted with the objective of improving the common capability of the Union and the Member States for the purpose, among others, of combating transnational organised crime. This objective was to be pursued by, in particular, the approximation of legislation. In 2016, the Commission reported on the implementation of the Framework Decision[92]. It results from the analysis that while the Framework Decision has

90 In 2013, the EU also developed a comprehensive strategy to address the illicit tobacco trade, see COM (2013) 324 final of 6 June 2013 to which a progress report was issued in May 2017(COM (2017) 235 final of 12 May 2017). Key policy tools in the EU include tracking and tracing under the 2014 Tobacco Products Directive as well as, at the global level, the FCTC Protocol.

91 Council Framework Decision 2003/568/JHA of 22 July 2003 on combating corruption in the private sector and the 1997 Convention drawn up on the basis of Article K.3(2)(c) of the Treaty on European Union on the fight against corruption involving officials of the European communities or officials of Member States of the European Union.

92 COM(2016) 448 final.

been largely transposed, national approaches differ substantially. Those differences stem from the Member States' legal traditions and systems. Whilst most Member States have adopted self-standing offences in relation to participation in a criminal organisation, two Member States have not done so. All Member States that provide for a self-standing offence also cover participation in a criminal organisation, while a few of them cover additionally the offence of conspiracy in organised crime.

It stems from contacts with stakeholders (the law enforcement and judiciary authorities) and from the research that the offence of organised crime is being effectively applied to less serious types of organised crime, e.g. property crime, while it is less applied in practice in relation to serious criminality for which it was initially designed. Instead, the Member States continue often addressing serious organised crime cases through predicate offences. As a result the cases of convictions for the offence of organised crime, if any, are mostly carried out in parallel to those on predicate offences. The latter are usually more attractive due to higher penalty thresholds and they are easier to prove before the court (the *chapeau* organised crime offence composed of numerous elements is more challenging).

EU agencies and frameworks for cooperation

The JHA agencies (in particular Europol, Eurojust, European Border and Coast Guard) 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.

Cross-border operational police cooperation to tackle organised crime remains to date essentially conducted by Member States under the framework of bilateral or multilateral agreements, which they have signed with their EU counterparts. A number of instruments exist at EU level to facilitate operational cross-border police cooperation between the police forces of different Member States[93] (e.g. Joint Police (and customs) operations, Joint Investigation Teams (JITs), the Prüm Decision, the Convention Implementing the Schengen Agreement). These provisions give flexibility to Member States in terms of implementation. Some of these provisions have been replaced or complemented by other legislative acts such as the Swedish Framework Decision. To further structure their cooperation in the fight against organised crime at the operational level, Member States have developed a specific cooperation framework: the EU Policy Cycle.[94] Its aim is to fight the most important serious and organised crime threats to the EU by encouraging co-operation between the Member States, the EU institutions, the agencies and where relevant third countries and organisations.

Judicial cooperation in criminal matters also relies on Eurojust as the EU's judicial Cooperation Unit to stimulate and improve the coordination of investigation and prosecutions between the competent authorities in the Member States and on effective cross-border instruments (e.g. mutual recognition of judgments and the European Arrest Warrant are key elements of the judicial framework). National judges can rely on the European Judicial Network (EJN) for the execution of European Arrest Warrants and freezing and confiscation orders.

---

93 For the assessment of the main instruments in this regard, see Chapter V Information exchange and operational cooperation '2. Law enforcement and judicial cooperation: the role of the EU agencies (Europol, the EU Policy cycle, CEPOL)' below.

94 See further information see Chapter V Information exchange and operational cooperation '2. Law enforcement and judicial cooperation: the role of the EU agencies (Europol, the EU Policy cycle, CEPOL)' below.

Other authorities are also key actors in the fight against organised crime. Customs authorities are the leading authorities for control of goods, and therefore contribute to tackle illegal activities at the external border. Tax administrations are the main responsible authorities for fighting VAT fraud. At EU level Eurofisc, a network of tax officials, provides a quick and multilateral exchange of targeted information to tackle serious cross-border VAT fraud. It handles crucial intelligence on fraudsters and new fraud trends. Under the current Policy Cycle, the platform brings together Eurofisc and other law enforcement agencies officials, which resulted in successful actions against criminal organisations behind VAT fraud.

At EU level, a number of European networks or cooperation structures complement the work of EU agencies and foster operational cooperation. Among these networks are those involving police officers[95] and prosecutors[96] specialised in environmental crime, drug trafficking (MAOC (N))[97], anti-corruption authorities[98] or crime prevention[99]. These allow knowledge and experience to be shared across the EU and good links maintained with third countries.

In order to improve national standards and performances in the implementation of EU instruments for the fight against organised crime, and to share best practices, mutual evaluation procedures have been established by Joint Action 97/827/JHA of 5 December 1997. Regular evaluations are carried out by experts from the Member States who undertake visits and examine the national system and practices of the Member State in question. The mechanism consists of a "peer" evaluation, aimed mainly at improving national standards and performances in the implementation of cooperation instruments for the fight of organised crime and at sharing best practices in this respect. Therefore, the aim of the evaluation is not necessarily assessing the implementation of the EU legislation but mainly the existing practices and arrangements stemming of the various acts and instruments. Consequently, the experts of the evaluation team, who have both the substantial specific experience on the topic of the evaluation, and also the concrete possibility to closely examine the national systems and practices in the evaluated Member State during the on-the-spot visits, have an essential role in this context. Currently the seventh round of mutual evaluations (cybercrime) is being finalised and the topic of the eight round (environmental crime) was agreed upon in the second semester of 2016. The previous rounds focused on: 1) mutual legal assistance, 2) drug trafficking, 3) exchange of information between Europol and the Member States and between the Member States, 4) European Arrest Warrant 5) financial crime and financial investigations, 6) the implementation of the legal framework of Eurojust and EJN in the Member States.

Specific EU funding programmes and instruments

---

95 European Network for Environmental Crime (EnviCrimeNet). For more details, see: www.envicrimenet.eu/

96 European Network of Prosecutors for the Environment (ENPE). For more details, see: https://www.environmentalprosecutors.eu.

97 http://maoc.eu/. The Maritime Analysis and Operations Centre – Narcotics (MAOC (N)), based in Lisbon, is an initiative by 7 EU Member Countries: France, Ireland, Italy, Spain, Netherlands, Portugal and the UK and is co-funded by the Internal Security Fund of the European Union. The Centre provides a forum for multi-lateral cooperation to suppress illicit drug trafficking by sea and air. From 2007 to July 2016, MAOC (N) supported the coordination and seizure of over 116 tons of cocaine and over 300 tons of cannabis. As such, the MAOC (N) is probably one of the most cost effective initiatives ever financed by the Commission.

98 European Partners against Corruption/European contact-point Network against Corruption (EPAC/EACN).

99 http://eucpn.org/. The European Crime Prevention Network (EUCPN) was set up on 28 May 2001 and then re-established on 30 November 2009 by a Council Decision. The EUCPN is supported by the EU through a grant.

Apart from sector-specific legislation, the EU contributes to the fight against organised crime through specific EU funding programmes and instruments. In particular, Council Decision 2007/125/JHA of 12 February 2007 established, for the period 2007 to 2013, as part of General Programme on Security and Safeguarding Liberties[100], the Specific Programme Prevention of and Fight against Crime. The subsequent 7 year period were covered by the Internal Security Fund-Police (ISF-P) established with the general objective of contributing to ensuring a high level of security in the Union, and with a global budget for the period 2014-2020 is EUR 1.1 billion.

Support to the policy implementation has also been provided by the security research programme and the Social Sciences and Humanities research programme, in Framework Programme 7 Societal Challenge 6 (Inclusive, Innovative and Reflective societies) and Societal Challenge 7 (Secure societies) in and Horizon 2020.[101]

2. Money laundering, asset recovery and financial crime

a. Main findings

The assessment suggests that the legal framework in this area is well developed, but could still be improved further. The review has shown that in some instances, more efforts are needed to ensure that instruments achieve their goals. This is the case for asset recovery offices for which recent developments, most notably the increases in requests for information, suggest a need to enhance their capabilities. Better clarity on the provisions on the exchange of information both between asset recovery offices and other national authorities, could also provide added value.

With a legal framework that was recently modernised, it results from the assessment that consideration could be given to revoking Joint Action 98/699/JHA of 3 December 1998 on money laundering, the identification, tracing, freezing, seizing and confiscation of instrumentalities and the proceeds from crime. Most of the provisions of the Joint action have been replaced, and only some of the general recommendations remain relevant. Such provision must respect fundamental rights.

b. Overview of EU action

The major 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. The confiscation and recovery of criminal assets was identified by stakeholders as a very effective measure to disrupt the activities of organised crime groups, as it takes away the motivation (financial gain) and resources that could be used for further criminal activities. International criminal networks use legal business structures to conceal the source of their profits. This leads to the infiltration of the licit economy by organised crime, which distorts competition between businesses and

[100] http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2007:058:0007:0012:EN:PDF.

[101] Specific examples of relevant projects funded include the FP7 projects CAPER ("Collaborative information, Acquisition, Processing, Exploitation and Reporting for the prevention of organised crime"). HEMOLIA ("Hybrid Enhanced Money Laundering Intelligence, Investigation, Incrimination and Alerts") which delivered sets of guidelines for those fighting organised crime. FIDUCIA ("New European Crimes and Trust-based Policy") and ANTICORRP ("Anticorruption Policies Revisited. Global Trends and European Responses") that investigated the relationship between corruption and organised crime and its impact on vulnerable groups (http://anticorrp.eu/).

substantially affects the internal market. This phenomenon can be countered by a comprehensive framework for the prevention of money laundering, backed up by effective law enforcement action and by a robust confiscation policy, based on effective national systems and on international cooperation.

Countering money laundering

Over the past 25 years, the Union has developed a comprehensive legal regime aimed at **countering money laundering**. The evolution of this regime has been closely linked with the parallel development of global standards in the field. The Union has been active in a number of international fora producing international treaties in the field, most notably in the United Nations (the Vienna Convention of 1988 and the Palermo Convention, of 2000, focusing on the laundering of the proceeds of drug trafficking), in the Council of Europe and in the Financial Action Task Force on Money Laundering (FATF). The main output of the FATF was the 40 FATF Recommendations produced in 1990 and revised in 1996, 2003 and 2012.

The main elements of the EU approach include the criminalisation of money laundering (and terrorist financing); the prevention of money laundering by ensuring an effective detection and reporting of suspicious activities by the private sector; provisions enabling the freezing and confiscation of assets; and the focus on financial intelligence, by establishing Financial Intelligence Units and asset recovery offices responsible for receiving and analysing reports received from the private sector, and for recovering criminal assets.[102]

As a key component of the EU's anti-money laundering strategy and in line with global developments, the creation of a series of new money laundering offences was achieved through the first AML Directive in 1991, which introduced a definition of money laundering that remained virtually unchanged. By contrast, the list of associated predicate offences (the crimes which are deemed to generate proceeds) evolved over time, by being extended to cover many more crimes, including tax crimes and offences established in EU instruments adopted in various fields. In 2015, the EU adopted a new (fourth) directive to address the threat of money laundering, following the previous directives of 1991, 2001, 2005 and 2006 (Commission). The adoption of the 4th Anti-Money Laundering Directive was a major step forward in improving the effectiveness of the EU's efforts to combat the laundering of money from criminal activities and to counter the financing of terrorist activities.

The Anti-Money Laundering Directive aims at fighting against money laundering and terrorist financing while ensuring proportionality and minimising the burden on legitimate business. The key measures include: identification of customers, proxies, and beneficial owners; ongoing monitoring of the business relationship; obligation to report suspicious transactions; record keeping; supervision and cooperation; staff protection; sanctions. Designated obliged entities need to carry out customer due diligence, report suspicions of money laundering and terrorist financing and take supporting measures. Underpinning the entire system, the risk based approach means that obliged entities have to apply customer due diligence procedures taking into account the risk of money laundering. The risk based

[102] Apart from money laundering, legislative instruments in the area of financial crime developed at EU level covered issues such as the control of cash entering or leaving the Community (2005), the protection of the Euro and other currencies against counterfeiting by criminal law (framework decision of 2000, and then Directive of 2014 laying down EU-wide minimum rules on the definition of offences and the level of sanctions, and ensured that effective investigative tools) and fund transfers (2006 then 2015).

approach requires a serious assessment from those who have to comply with the legal obligations, as misjudgement can lead to excessive procedures or serious danger to society.

In July 2016, the Commission proposed a number of amendments to the Directive on selected issues. They include provisions strengthening the powers of the Financial Intelligence Units, improving access to beneficial ownership information and establishing centralised bank account registers at the Member States level, as well as provisions on high risk third countries, pre-paid cards and virtual currencies.

Preventive action needs to be complemented by effective law enforcement to detect and investigate money laundering activities and bring perpetrators to court. While all Member States have criminalised money laundering, there remain differences both on the definition of money laundering and on the sanctions applied to such a crime. These differences create obstacles that hinder cross-border judicial and police cooperation to effectively tackle money laundering. For this reason, on 21 December 2016, the Commission adopted a proposal for a Directive on countering money laundering by criminal law[103]. The proposal aims to establish minimum rules concerning the definition of criminal offences and sanctions in the area of money laundering, as well as common provisions to improve the investigation of those offences. To complement this initiative, on the same date, the Commission also adopted legislative initiative replacing Regulation (EC) No 1889/2005 in order to establishing tighter controls on people entering or leaving the EU with at least €10,000 in cash. The proposal extends customs checks to cash sent in postal parcels or freight shipments, to precious commodities such as gold and to prepaid payment cards which are currently not covered by the standard customs declaration.

While the outlined measures are ultimately geared to protecting the financial system, they aim to offer all guarantees to balance the need for increased security with the need to protect fundamental rights, including the right to private life and the protection of personal data.[104]

Confiscation of the proceeds of organised crime

Even where crime proceeds have been successfully laundered, the assets of organised criminals can be identified through financial intelligence and investigation, seized and recovered. The confiscation and recovery of criminal assets is seen as an effective way to fight organised crime, which is essentially profit-driven. Confiscation prevents that criminal wealth may be used to finance other criminal activities, jeopardise the confidence in the financial systems and corrupt legitimate society. Confiscation also has a deterrent effect by strengthening the notion that "crime does not pay".

Substantial efforts have been made at EU level to better trace and confiscate the proceeds of organised crime. In 2001, Framework Decision 2001/500/JHA[105] led to a limited level of harmonisation of national provisions regarding confiscation and criminal sanctions for money laundering. In 2003, Framework Decision 2003/577/JHA[106] applied the principle of mutual recognition to orders freezing property or evidence. *In 2005, Framework Decision*

[103] COM(2016) 826 final.

[104] 2016 Report on the Application of the EU Charter of Fundamental Rights, COM(2017) 239 final.

[105] Council Framework Decision 2001/500/JHA of 26 June 2001 on money laundering, the identification, tracing, freezing, seizing and confiscation of instrumentalities and the proceeds of crime, OJ L 182 of 5.7.2001, p. 1.

[106] Council Framework Decision 2003/577/JHA of 22 July 2003 on the execution in the European Union of orders freezing property or evidence, OJ L 196 of 2.8.2003, p. 45.

2005/212/JHA[107] had the objective to ensure that Member States introduced effective rules on confiscation, including rules on proof with regard to the source of the assets concerned. However, an implementation report from the Commission of December 2007[108] showed that the text's provisions were considered unclear and lead to piecemeal transposition. In 2006, Framework Decision 2006/783/JHA[109] applied the principle of mutual recognition to confiscation orders.

In a Communication of 2008[110], the Commission noted that the overall number of confiscation cases in the EU was relatively limited and the amounts recovered from organised crime were modest, especially if compared to the estimated revenues of organised criminal groups. An increased use of confiscation procedures was felt desirable. The Commission took a critical view of the legal framework applicable at the time, noting the partial transposition and some limitation on the effectiveness of the legal instruments.

The Directive 2014/42/EU of 3 April 2014 on the **freezing and confiscation of instrumentalities and proceeds of crime**, aims to act against the financial incentive which drives most serious and organised crime, to protect the EU economy against infiltration and corruption by criminal groups, and to return such assets to the rightful owners. It enables extended confiscation (of assets not directly linked to a specific crime, but which clearly result from criminal activities by a convicted person), third-party confiscation and the confiscation of assets in cases where the suspect is permanently ill or has fled. The Directive includes provisions enabling the temporary freezing of assets in urgent cases and on the management of frozen assets, as well as strong safeguards to preserve fundamental rights.

The Directive is a relatively recent instrument (with a transposition deadline of 4 October 2016) and it is too early to assess its concrete impact. By the transposition deadline, only 8 Member States had notified the Commission that they had fully transposed its provisions into their national legislation. The Commission therefore launched infringement procedures for the failure to communicate national implementing measures in full transposition of the Directive against 18 Member States in November 2016. By the end of May 2017, 18 Member States had notified full transposition[111].

On 21 December 2016 the European Commission has adopted a package of measures to strengthen the EU's capacity to fight the financing of terrorism and organised crime, delivering on the commitments made in the Action Plan against terrorist financing from February 2016.[112] A proposed Regulation on the **mutual recognition of freezing and confiscation orders** is part of this package.[113] The proposal is aimed at enabling a swift recognition and execution of such orders in other Member States without cumbersome formalities, thereby simplifying existing rules. It widens the scope of freezing and confiscation orders covered compared to the current legal framework and includes classic,

---

107 Council Framework Decision 2005/212/JHA of 24 February 2005 on Confiscation of Crime-related Proceeds, Instrumentalities and Property, OJ L 68 of 15.3.2005, p. 49.

108 Report from the Commission pursuant to Article 6 of the Council Framework Decision of 24 February 2005 on Confiscation of Crime-related Proceeds, Instrumentalities and Property (2005/212/JHA), COM (2007) 805.

109 Council Framework Decision 2006/783/JHA of 6 October 2006 on the application of the principle of mutual recognition to confiscation orders, OJ L 328 of 24.11.2006, p. 59.

110 COM(2008) 766 final.

111 For details, see Commission's public database of infringement decisions: http://ec.europa.eu/atwork/applying-eu-law/infringements proceedings/infringement_decisions/?lang_code=en

112 COM(2016) 50 final.

113 COM(2016) 819 final.

extended and third party confiscation as well as non-conviction based confiscation decided by a criminal court. The proposed Regulation also aims at improving the protection of victims of crime in cross-border cases.

Under the 2014 Directive, the freezing and confiscation of the proceeds of crime is generally based on a criminal conviction. However, most Member States have in place procedures (under their criminal law) allowing the confiscation of the proceeds of crime even in circumstances where a criminal conviction cannot be obtained (e.g. death of the suspect or accused person), or procedures held in civil or administrative courts which allow the confiscation of the proceeds of crime in the absence of a criminal conviction (UK, Ireland, Italy, Bulgaria, Slovenia, Slovakia). When adopting the 2014 Directive on confiscation, the European Parliament and the Council issued a joint declaration calling on the Commission to analyse the feasibility, opportunity and possible benefits of introducing common rules on non-conviction based confiscation in the EU.

With regard to tracing and **recovery of proceeds from crime**, the Council Decision 2007/845/JHA required Member States to set up or designate a national Asset Recovery Office (ARO) in order to facilitate the tracing and identification of proceeds from crime, in view of their possible freezing and confiscation. However, in an implementation report issued by the Commission in 2011[114], it appeared that two years after the expiry of the transposition deadline, five Member States still had not designated their ARO. The 2011 report also identified a number of specific challenges. With regard to the cooperation between EU countries' Asset Recovery Offices, the 2007 Council Decision provided a legal basis for the exchange of information between those national agencies of the Member States that were already cooperating informally under the Camden Asset Recovery Inter-Agency Network (CARIN)[115].

Since then, substantial progress was made. All Member States have today designated their AROs. The Europol SIENA system has become the preferred secure information exchange system of the AROs (21 AROs connected) and the operational exchanges between AROs have drastically increased (from 539 exchanges in SIENA in 2012 to over 4217 in 2016).

With an increasing focus on asset recovery, and increased cooperation between AROs, the latter are faced with an increasing number of asset tracing requests, which they need to be able to handle. In the context of the comprehensive assessment, stakeholders[116] have stressed the need to enhance the AROs capabilities and powers (e.g precautionary freezing powers in order to avoid the dissipation of the assets identified; granting of access to additional databases such as centralised bank account registers). It results from the assessment that other areas for improvement in this regard could be the provisions applicable to (and related funding for) the exchange of information between AROs as well as between AROs and other national authorities; specialised training for ARO investigators, and further IT solutions. Overall, it appears that experts in this area suggest that further improvement is necessary to speed up response times to AROs and ensure information of better quality. One example on how to achieve this is looking at high risk sectors and mapping out investments made by organised crime groups – in order to better detect the infiltration of organised crime in the

114 COM(2011) 176 final.

115 For details, see: http://carin-network.org/

116 See in particular Annex VI Workshops, 2. Europol workshop on "EU Security Policy" of the comprehensive assessment.

economy. Finally, the need for increased cooperation between AROs, customs and Financial Intelligence Units (FIUs) was also recognised during the consultation process.

At the international level, the Commission also supports the efforts aimed at strengthening the effectiveness of asset recovery. The CARIN network of asset recovery practitioners, through its network of operational law enforcement and judicial contact points, covers 122 countries and jurisdictions and has the ultimate objective of achieving a global reach. The informal exchanges between the CARIN contact points allow exchanging intelligence information on financial flows or the location assets without cumbersome procedures.

Reference should also be made to financial support under the Hercule III Regulation (250/2014) to national and regional authorities in the Member States tasked with activities for the protection of the financial interests of the Union. The Programme provides funds for the purchase of equipment deployed in operations in support of investigations into transgressions by organised crime groups perpetrated against the financial interests of the Union. These operations often generate information on transgressions in relation to money laundering, THB, smuggling of drugs. The beneficiaries of this financial support often report that this information is shared with other law enforcement agencies located in the same Member State or other countries. In addition, the programme provides a modest funding for digital forensic training sessions for law enforcement staff from the Member States and third countries. These training sessions provide a strengthening of the operational and technical capacity of law enforcement agencies whose tasks are not limited to the protection of the financial interests of the Union, but that cover other areas as well, including the fight against money laundering, THB, drugs or terrorism.

3. Trafficking of firearms

a. Main findings

Feedback from Member States experts highlighted the importance of keeping the firearms issue as a major priority. Any inconsistencies in implementation of the current legislation should be effectively resolved. It was felt that further capacity building and even better cooperation between bodies, not just public authorities such as customs services, but with the private sector and their networks as well, would be needed, and that cooperation should be developed further with third countries.

The EU Action Plan has been a key driver for better cooperation and information sharing. However, much more still needs to be done in relation to this aspect. For instance, developing systematic harmonised data collection on firearms seizures for all Member States could improve the intelligence picture. In addition, setting up an EU-wide information system to exchange information on authorisations (or refusals) to possess, acquire, transfer or export firearms could greatly improve the legal arsenal in this area.

The initiatives under the Action Plan with the Balkan countries require regular assessment and some aspects can be sharpened, for example, by organising regular joint meetings between the European Union and the South Eastern Europe Firearms experts. Efforts on international cooperation with other third countries, following the model of the cooperation with the Western Balkans should also continue.

b. Overview of EU action

Organised crime groups are heavily involved in the illicit trafficking of firearms. It is a lucrative source of revenue and facilitates the ability to commit other forms of violent crime. Furthermore counteracting the illegal access to both firearms and explosives is crucial in the fight against terrorism. 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. Differences in national legislation can hinder controls and police cooperation.

General

Initiatives at EU level began in 1991 with the adoption of the Council Directive 91/477/EEC (the "firearms Directive")[117]. This was at the time when intra-EU barriers were being removed leading to the internal market. It was thus a measure related to the internal market by setting minimum rules across Member States on the acquisition and possession of firearms and on the transfers between Member States. The firearms directive was subsequently amended in 2008[118] to ensure the conclusion of the UN Firearms Protocol. A full revision of the Directive was achieved in May 2017[119]. In 2005 the European Council adopted the EU strategy to combat the illicit accumulation and trafficking of small arms and light weapons (SALW) and their ammunition. This Strategy focussed on the illicit trade in small arms and light weapons because of their role in the worsening of terrorism and organised crime, triggering of conflicts and the collapse of state structures. The main goal of the Strategy was to engage the whole EU in supporting the implementation of the 2001 UN Programme of Action to prevent, combat and eradicate the illicit Trade in SALW in all its aspects. The EU SALW Strategy is currently under revision taking into account the Lisbon Treaty, the guiding principles of the 2016 EU Global Strategy for Foreign and Security Policy and the new challenges and opportunities with regards to conventional arms control that presented themselves since 2005.

In 2012, Regulation 258/2012 concerning export, import and transit licensing or authorization systems of firearms, their parts and components, was adopted to implement the United Nations' Protocol against the illicit manufacturing of and trafficking in firearms, their parts and components and ammunition. This regulation is part of an overall legal and operational framework aiming at preventing, detecting, investigating and prosecuting firearms trafficking. While the 1991 firearms directive deals with intra-EU transfers of firearms, the Regulation governs imports to and exports from the EU.

The European Agenda on Security equally identified the fight against the trafficking in firearms as one of its priority actions. In October 2015 the Council called on the Member States, the Commission, Europol and INTERPOL to deliver a series of actions. In November 2015, the Commission adopted a package of measures to strengthen control over access to firearms across the EU[120]. These included a proposal for a revision of the firearms Directive to strengthen the legal framework, rendering the controls on acquisition and possession more vigorous, and an Implementing Regulation on deactivation of firearms.

---

117 Council Directive 91/477/EEC on control of the acquisition and possession of weapons, OJ L 256, 13.9.1991, p. 51–58.

118 Directive 2008/51/EC of the European Parliament and of the Council of 21 May 2008 amending Council Directive 91/477/EEC on control of the acquisition and possession of weapons, OJ L 179, 8.7.2008, p. 5–11.

119 Directive (EU) 2017/853 of the European Parliament and of the Council of 17 May 2017 amending Council Directive 91/477/EEC on control of the acquisition and possession of weapons, OJ L 137, 24.5.2017, p. 22–39.

120 http://europa.eu/rapid/press-release_IP-15-6110_en.htm.

An evaluation of the firearms Directive highlighted several obstacles that could undermine its effectiveness. One of these issues related to the need for common and stringent guidelines for the deactivation of firearms. It appeared that deactivated firearms could be reactivated and used for criminal purposes in several instances. As a result, an implementing regulation on deactivation of firearms was agreed in December 2015.[121] It became applicable as from April 2016. This Regulation sets out rules on the way Member States must deactivate such arms so as to make them inoperable. This Regulation is based on the criteria for deactivation developed by the Permanent International Commission for the Proof of Small Arms (the CIP).

Other relevant EU measures currently in force also include the 2013 Regulation[122] on the marketing and use of explosives precursors. The instrument aims to cut access to dangerous chemicals and to allow early police investigations on suspicious transactions and similar incidents. The full implementation of this measure is considered an urgent priority to enhance the security of explosives. Strong cooperation with Member States and the engagement with the supply chain of precursors is needed.

In the area of research, several projects, financed by the EU, such as "EFFECT" and "FIRE" improve knowledge on the illicit trafficking of firearms covering inter alia online trafficking and the diversion from the legitimate activity. Europol too has organised training on how to tackle the illicit trade of firearms (including online trade).

EU Action Plan - Operational cooperation between Member States

In addition to the measures adopted by the Commission at the end of 2015, the need to improve operational cooperation at EU level among Member States led the Commission to develop an Action Plan against the illegal trafficking of firearms and explosives in December 2015 (the "EU Action Plan").[123] The EU Action Plan aims to promote better operational cooperation between police, customs and other law enforcement bodies and between Member States through Europol. The initiative also aims to extend cooperation with key third countries (see below) and international organisations such as INTERPOL. The focus is to better prevent, detect, investigate and seize firearms, explosives and explosives precursors as part of a security package.

The clear cross-border dimension of arms trafficking means that the legal dimension had to be complemented by stronger police and intelligence service coordination between the authorities in the EU and beyond. The EU Action Plan seeks to enhance this cooperation. Many of measures in the EU Action Plan have been completed or are in the process of being completed, and preliminary conclusions can be drawn.

The EU Action Plan has contributed to better intelligence (including better statistical and analytical measures at both Member State and EU level) on the trafficking of firearms and the use of explosives.

---

121 Commission Implementing Regulation (EU) 2015/2403 of 15 December 2015 establishing common guidelines on deactivation standards and techniques for ensuring that deactivated firearms are rendered irreversibly inoperable, OJ L 333, 19.12.2015, p. 62–72.

122 Regulation (EU) No 98/2013 of the European Parliament and of the Council of 15 January 2013 on the marketing and use of explosives precursors, OJ L 39, 9.2.2013, p. 1–11.

123 Implementing the European Agenda on Security: EU action plan against illicit trafficking in and use of firearms and explosives. COM(2015) 624 final.

Operational Actions have been a key focus under the EU Action Plan. One such example, "MARS", a coordinated transnational investigation based on a modus operandi of converted/reactivated firearms and joint actions in Western Balkans has proven successful in both seizing firearms and arresting the perpetrators.

Action beyond EU borders

An Action Plan on firearms trafficking between the EU and South East European countries for 2015-2019 was formally adopted by both the Council[124] and the EU-Western Balkans Ministerial Forum on Justice and Home Affairs. It foresees actions including enhancing the exchange of information at regional level and with Member States, enhancing operational law enforcement co-operation at regional level and harmonising national legislation on firearms in line with EU and international standards. In early 2016, the EU and Western Balkans experts agreed to enlarge the scope of the Joint Action Plan to illicit explosives. In December 2016, the EU-Western Balkans Ministerial Forum on Justice and Home Affairs reaffirmed the commitment to implement a number of specific actions under the Action Plan[125].

Beyond the Action Plan on the illicit trafficking of firearms between the EU and the South East Europe Region, the EU has a well advanced dialogue with Middle East North Africa ("MENA") countries to enhance cooperation among relevant law enforcement agencies, ensure capacity-building assistance in relevant regional and/or bilateral programmes and develop operational actions under a commonly agreed framework.

The EU supports financially measures to combat trafficking on small arms and light weapons (SALW) in various regions in the world[126]. The EU reported on the implementation of the Action Plan of the 2005 EU SALW Strategy by means of bi-annual and later annual progress reports[127] that give an overview of all actions the EU has undertaken abroad and at home. Cooperation and assistance projects in third countries were supported by means of the CFSP-, Instrument contributing to Stability and Peace (IcSP)/Instrument for Stability (IfS)- and DEVCO-funds in South-East. The EU also undertook diplomatic initiatives in the context of the CFSP and outreach by specialised services of the European Commission. Most projects served the implementation of the UN PoA and focussed on collection and destruction of surplus SALW, physical security and stockpile management, capacity building for marking, record keeping and tracing, including the provision of equipment. In the framework of the Common Foreign and Security Policy, financial assistance is currently provided under a number of Council Decisions to support SALW-control actions.[128]

---

124 Council doc. 6130/16.

125 See for full list of actions, the Statement on Enhancing the Fight Against Illicit Trafficking of Firearms and Ammunition in the Western Balkans, Brussels, 16 December 2016, available here: http://europa.eu/rapid/press-release_STATEMENT-16-4445_en.htm.

126 Latest report: https://eeas.europa.eu/sites/eeas/files/celex-52017xg041101-en-txt.pdf.

127 https://eeas.europa.eu/topics/disarmament-non-proliferation-and-arms-export-control/14721_en.

128 Council Decision 2014/912/CFSP in support of physical security and stockpile management (PSSM) activities to reduce the risk of illicit trade in small arms and light weapons (SALW) and their ammunition in the Sahel region; Council Decision (CFSP) 2015/1908 in support of a global reporting mechanism on illicit small arms and light weapons and other illicit conventional weapons and ammunition to reduce the risk of their illicit trade ('iTrace II'); Council Decision (CFSP) 2016/2356 Reducing the Threat of the Illicit Accumulation and Trafficking of Small Arms and Light Weapons (SALW) in South East Europe (SEESAC); Council Decision (CSFP) 2017/633 In support of the United Nations Programme of Action to Prevent, Combat and Eradicate the Illicit Trade in Small Arms and Light Weapons in All Its Aspects (UN PoA).

The EU also supported the implementation of the UN Firearms protocol in cooperation with the United Nations Office on Drugs and Crime (UNODC). The EU has also systematically negotiated the inclusion of SALW-related clauses in trade agreements with third countries.

The EU provides funding in support of activities to counteract arms trafficking. In 2016, under the Internal Security Funds the Commission has granted about €3 million to fund projects by national stakeholders in this field and provided €1.5 million financial support over two years to the United Nations Office on Drugs and Crime (UNODC) project, instrumental in developing internationally harmonised data collection, to regularly map out global firearms trafficking routes to the EU and make it available to all Member States law enforcement authorities. EU funding is also envisaged in certain other cases (such as for the destruction/neutralisation of confiscated/decommissioned firearms), e.g. under the Instrument contributing to Stability and Peace, other EU assistance programmes or the CFSP budget.

4. Trafficking in Human Beings

a. Main findings

The analysis conducted in the context of this review indicates that both the 2011 Directive and the THB Strategy have contributed towards addressing the key challenges in the area of trafficking in human beings.

More specifically, the EU THB Strategy has provided a coherent basis and direction for the EU policy in this area, and has put together a number of processes which have resulted in a coordinated and more coherent approach at the EU level to tackle the crime and protect the victims, which has been clearly recognised by the Council and EP resolutions.

Following the radical changes of the socio-political environment in which the 2012 Strategy was adopted, the Commission is considering options for the post-2016 follow-up in order to ensure the continuation of efforts at EU level. The Council, the European Parliament and the civil society have requested a new policy framework for the post-2016.

The Directive is a relatively recent instrument. In addition, and bearing in mind the changing socio-political context, challenges remain predominantly in the areas of prosecution, protection and prevention. In this context, ensuring full implementation of the Directive is crucial.

b. Overview of EU action

Trafficking in human beings ("THB") is an extremely pernicious and highly lucrative form of crime[129]. It is a violation of fundamental rights, explicitly prohibited under Article 5 of the EU Charter of Fundamental Rights, and a serious form of organised crime explicitly enshrined in Article 83 and linked to illegal migration, Article 79 TFEU. The legal and policy framework consists predominantly of Directive 2011/36/EU on preventing and combating trafficking in human beings and protecting its victims and the EU Strategy towards the eradication of trafficking in human beings 2012-2016.

[129] Europol's Report on Trafficking in Human Beings Financial Business Model of 2015: the estimated profit globally on all forms of THB is 29.4 billion euro annually. A trafficker's average annual income is about 70 000 euro. The estimated annual global profit of THB related sexual exploitation is 25.8 billion euro. The estimated profits of THB for the purpose of sexual exploitation in the EU and developed countries amount to 23.5 billion euro.

Trafficking in human beings is a transnational threat fuelled by high profits in the legal and illegal economy as well as demand that fuels all forms of exploitation. The political commitment at EU level to address the problem of trafficking in human beings is reflected in the large number of initiatives, measures and funding programmes established in the area both within the EU and third countries as early as in the 1990s[130].

The Directive 2011/36/EU[131] adopts a comprehensive approach anchored in human rights and is victim's centred, gender-specific and child sensitive which was considered by stakeholders as forward thinking and innovative. It equally focuses on law enforcement, criminal law, victim protection and support, as well as prevention and coordination. Based on Article 20 of the Directive, the EU Anti-trafficking Coordinator ensures coherence and coordination in the area of trafficking in human beings and oversees the implementation of the EU legal and policy framework addressing trafficking in human beings.

The 2012-2016 EU Strategy complements the THB Directive. With the 2012-2016 EU Strategy, the European Commission focused on concrete measures that support the transposition and implementation of Directive 2011/36/EU, bringing added value and complementing the work done by governments, international organisations and civil society in the EU and third countries. The 2012-2016 EU Strategy identified **five priorities** for the EU to focus on in order to address the issue of trafficking in human beings and outlined a number of actions which the European Commission proposed to implement over the five year period in concert with other actors, including Member States, European External Action Service, EU institutions, EU agencies, international organisations, third countries, civil society and the private sector. The five priorities concerned are: identifying, protecting and assisting victims of trafficking; stepping up prevention of THB; increased prosecution of traffickers; enhanced coordination and cooperation among key actors and policy coherence; and increased knowledge of and effective response to emerging concerns related to all forms of trafficking in human beings.

The 2012-2016 EU Strategy has provided a coherent basis and direction for the EU policy in the area of trafficking in human beings and coming to its end has completed nearly all actions envisaged. Member States have mirrored the implementation of the Strategy in their National

[130] The THB Directive is part of global action against trafficking in human beings, which includes action involving third countries as stated in the '*Action-oriented Paper on strengthening the Union external dimension on action against trafficking in human beings; towards global EU action against trafficking in human beings'* approved by the Council on 30 November 2009. In this context, action should be pursued in third countries of origin and transfer of victims, with a view to raising awareness, reducing vulnerability, supporting and assisting victims, fighting the root causes of trafficking and supporting those third countries in developing appropriate anti-trafficking legislation. The Union is committed to the prevention of and fight against trafficking in human beings, and to the protection of the rights of trafficked persons. For this purpose, Council Framework Decision 2002/629/JHA of 19 July 2002 on combating trafficking in human beings and an EU Plan on best practices, standards and procedures for combating and preventing trafficking in human beings were adopted. Moreover, the Stockholm Programme — "An open and secure Europe serving and protecting citizens", adopted by the European Council, gives a clear priority to the fight against trafficking in human beings. Other relevant earlier instruments: EU plan on best practices, standards and procedures for combating and preventing trafficking in human beings [Official Journal C 311 of 9.12.2005]; Commission Decision 2011/502/EU of 10 August 2011 on setting up the Group of Experts on Trafficking in Human Beings and repealing Decision 2007/675/EC [OJ L 207 of 12.8.2011]; Council Decisions 2006/618/EC and 2006/619/EC of 24 July 2006 on the conclusion, on behalf of the European Community, of the Protocol to Prevent, Suppress and Punish Trafficking in Persons, Especially Women and Children, supplementing the United Nations Convention against Transnational Organised Crime.

[131] Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions 'The EU Strategy towards the Eradication of Trafficking in Human Beings 2012–2016 - COM/2012/0286 final.

Action plans. To date, it appears that nearly all of the actions of the Strategy have been delivered. The Strategy has fostered coordination across policy areas and stakeholders, including with networks (regular meeting twice a year of the Civil Society Platform against THB and National Rapporteurs and Equivalent Mechanisms), Commission services (including the Inter-service group on THB consisting of Commission services), regular coordination meetings with the Justice and Home Affaires (JHA) Agencies as well as other EU institutions and international organisations.

Over the past five years a lot has been achieved in delivering key actions as laid down in the 2012-2016 EU Strategy and as required by the THB Directive, such as the publication of guidelines, manuals[132], studies[133] and reports[134].

Member States had to bring into force the laws, regulations and administrative provisions to comply with the Directive by 6 April 2013. Commission monitored the transposition of the Directive 2011/36/EU and issued its reports under Article 20, the so-called 'Transposition report'[135] and "Users report". It continues ensuring full compliance and implementation of this milestone piece of EU legislation in the area of THB.

Trafficking in human beings is a serious and organised crime with links to many other forms of crime (documents fraud, drug trafficking, cybercrime, child pornography, migrant smuggling, benefit fraud). THB was identified as priority crime in the 2013-2017 EU Policy Cycle (EMPACT on THB) and it was identified as such under the EU Serious and Organised Crime Threat Assessment (Europol, EU SOCTA 2017) and it will continue being a priority crime area of the 2018-2021 EU Policy Cycle for organised and serious international crime, with a focus on all forms of exploitation.

The external dimension of trafficking in human beings further constitutes an integral part of the policy framework and is one of its pillars. THB has a strong external dimension and many EU external policies address THB in relation to non-EU countries[136], both as a human rights issue as well as a cross-border illegal activity, involving countries of origin and transit outside the EU. The 2012-2016 EU Strategy addressed the importance of increasing cooperation

---

132 Guidelines on the identification of victims of trafficking in human beings in particular for consular services and border guards (2013); Guidelines on child protection systems published as reflection paper on 9th RC Forum; Handbook "Guardianship for children deprived of parental care" Joint COM-FRA deliverable available in 23 EU languages, June 2014; EU Rights of trafficking in human beings (available in 23 EU languages, 2013); Eurofound Handbook on temporary work agencies and intermediary agencies.

133 Study on comprehensive policy review of anti-trafficking projects funded by the European Commission (2016); Study on high-risk groups for trafficking in human beings (2015); Study on case-law on trafficking for the purpose of labour exploitation (2015); Study on prevention initiatives on trafficking in human beings (2015); Study on the gender dimension of trafficking in human beings (2016).

134 Commission Report assessing the extent to which Member States have taken the necessary measures in order to comply with Directive 2011/36/EU on preventing and combating trafficking in human beings and protecting its victims in accordance with Article 23 (1) and the Commission Report assessing the impact of existing national law, establishing as a criminal offence the use of services which are the objects of exploitation of trafficking in human beings, on the prevention of trafficking in human beings, in accordance with Article 23 (2) of the Directive 2011/36/EU - both published on 2 December 2016, as well as the Report on the progress made in the fight against trafficking in human beings as required under Article 20 of the Directive and the Accompanying Commission Staff Working Document published on 19 May 2016.

135 Commission Report assessing the extent to which Member States have taken the necessary measures in order to comply with Directive 2011/36/EU on preventing and combating trafficking in human beings and protecting its victims in accordance with Article 23 (1) COM(2016) 722.

136 The European Agenda on Security, the European Agenda on Migration, the EU Action Plan against migrant smuggling (2015 – 2020), the Global Strategy on the European Union's Foreign and Security Policy.

beyond borders, as initiatives against organised crime and trafficking in human beings contribute to coherence between the internal and external aspects of EU security policies.

The EU provides extensive funding under a number of thematic and geographical instruments and projects. As a measure of transparency and accountability on Commission funding, the Study on Comprehensive Policy Review of anti-trafficking projects (October 2016) - a deliverable of the EU Strategy - provides a series of conclusions and analysis on areas of intervention in relation to the objectives of the 2012-2016 EU Strategy during the period of 2004-2015 building upon concrete results of the set of the 321 projects with a total funding of €158.5 million per five Commission DGs (not including datasets on the migration crisis).

5. Drugs Trafficking

a. Main findings

The 2004 Council Framework Decision, setting out criminal offences and penalties in the field of illicit drug trafficking, has provided a common legal framework, which has also more generally supported the EU Policy Cycle and crime priorities as regards drugs trafficking. However, since the adoption of the Framework Decision, new developments, notably linked to the proliferation of online markets for drugs, have changed the context in which this legal instrument is applied and added new challenges.

The assessment has stressed the importance of action on the international stage, and to ensure appropriate follow-up, in particular through the implementation of the UNGASS outcome and on the preparation of the 2019 review process of the 2009 Political Declaration and Action Plan on International Cooperation towards an integrated and balanced strategy to counter the world drug problem.

b. Overview of EU action

The illicit drug market remains the largest criminal market in the EU. According to recent data from Europol, more than one third of the organised crime groups in the EU are involved in the illicit drugs activity[137] (other key criminal activities being property crime, migrant smuggling, THB and excise fraud). This lucrative business has spill-over effects into other illegal activity such as corruption. Drugs are also used as a form of payment between criminal groups. Each year in the EU alone, at least 24 billion euros are spent on illicit drugs according to the joint EMCDDA / Europol Drugs Market Report[138]. More than one third of the criminal groups active in the EU are involved in the production, trafficking or distribution of various types of drugs. Drug trafficking also supports the informal economy and spills over into violence and other illegal activities and causes major social problems. The 22nd EMCDDA report on the state of the drug problem in Europe published on 6 June 2017[139], provides a yearly overview of the drug situation: deaths due to overdose are on the rise for the third year in a row. There was a 6% increase in 2015 compared to the previous year, in almost all age groups. The availability of cocaine is rising in parts of Europe again. New potent synthetic substances like fentanyl are appearing on the market.

137 Europol SOCTA, 2017.
138 EMCDDA, *EU Drug Markets report*, 2016.
139 EMCDDA, European Drug Report, 2017, http://www.emcdda.europa.eu/publications/edr/trends-developments/2017.

General

The early 1990s saw the first steps being taken in the fight against drug trafficking at EU level, with adoption in 1990 of the first European plan to combat this problem. This first programme of coherent action against drugs made recommendations which included combatting illicit trafficking and increasing co-ordination at Member State level. The Maastricht Treaty on European Union which entered into force in 1993 then took this a step further by recognising the problem of drugs for the first time in an EU treaty. This led to the setting up of a Europol Drugs Unit with the focus of organising the exchange of information on narcotic drugs. It was also agreed to set up a European drug monitoring centre. The European Monitoring Centre for Drugs and Drug Addiction (EMCDDA) became fully operational in 1995[140]. The EMCDDA Regulation was substantially amended several times and finally recast by a Regulation in 2006[141]. The EMCDDA Regulation will be further amended to deal with the new trend of the growing numbers of new psychoactive substances.[142]

In 2001, a Council Decision of 28 May 2001[143] was adopted with the objective to set out procedures for the lawful transmission between Member States of samples of seized illicit drugs. Such exchanges help to combat the illicit production and trafficking of drugs.

In 2004, a Council Framework Decision[144] 2004/757/JHA of 25 October 2004 laid down minimum provisions on the constituent elements of criminal acts and penalties in the field of illicit drug trafficking. The need for legislative action for minimum rules at EU level to tackle illicit drug trafficking had by the time of the adoption of the Framework Decision long been acknowledged. Still today, illicit drugs remain the most dynamic of criminal markets, with a recent trend being the proliferation of new psychoactive substances (NPS). There therefore seems to be a continuing need for an EU common approach to tackle such illicit activity. While the main feature of the Framework Decision was to establish a common approach on EU level to fight against trafficking in drugs and precursors, it appears that its implementation by Member States is not satisfactory with only five Member States having been found to be in full compliance in 2013.

The Framework Decision is part of the new legislative package on new psychoactive substances and will, following political agreement on the package on 29 May 2017, be amended to take account of the growing numbers of NPS.

It appears from the assessment that there are several other issues pointing at a possible need for further modernisation. First, the Framework Decision dates from 2004 and has a legal basis that has since been superseded by the Lisbon Treaty. Second, it does not provide for any prevention measures, which are an important part of drug supply reduction and, third, it does

140 Regulation (EC) No 1920/2006 of the European Parliament and of the Council of 12 December 2006 on the) European Monitoring Centre for Drugs and Drug Addiction (recast), JO L 346, 27.12.2006, p.1.

141 Regulation (EC) No 1920/2006 of the European Parliament and of the Council of 12 December 2006 on the European Monitoring Centre for Drugs and Drug Addiction (recast) OJ L 376, 27.12.2006, p. 1–13..

142 This amendment is part of the legislative package on new psychoactive substances on which political agreement was reached on 29 May 2017.

143 Council Decision 2001/419/JHA of 28 May 2001 on the transmission of samples of controlled substances, OJ L 150, 6.6.2001, p. 1–3.

144 Council Framework Decision 2004/757/JHA of 25 October 2004 laying down minimum provisions on the constituent elements of criminal acts and penalties in the field of illicit drug trafficking, OJ L 335, 11.11.2004, p. 8–11.

not address new developments such as the online markets for drugs. As all Member States had already implemented the relevant UN Drug Control Conventions, the perception of stakeholders is that the Framework Decision had no significant impact on the practice of prosecutions, convictions and sentencing.

A Regulation in 2005[145] laid down rules for the monitoring of trade between the Union and third countries in drug precursors so as to ensure that licit substances are not diverted to the illicit manufacture of drugs. A Council Decision of 2005[146] established a mechanism for exchange of information on NPS, to provide for an assessment of the risks associated with these new substances to be carried out by the EMCDDA, and to set out a procedure on EU level for bringing specific NPS under control. This instrument will be repealed and replaced by a package on new psychoactive substances on which political agreement was found on 29 May 2017 (see below).

Illicit drugs trafficking are listed as one of the serious crimes under Article 83 TFEU. The main EU instruments in the fight against drugs trafficking are set out below.

The EU Drugs Strategy and Action Plan

The EU has adopted a number of successive strategies in this area. The EU Drugs Strategy for the period 2005–2012 was endorsed by the European Council of 16–17 December 2004. It built on the final evaluation of the 2000–2004 EU Drugs Strategy and Action Plan on Drugs[147] and on Europol and EMCDDA contributions in this context (Snapshots 1999-2004 and thematic papers). The Strategy aimed to provide added value to national drugs strategies in the EU while respecting the principles of subsidiarity and proportionality set out in the Treaties.

Confirming the EU's integrated, multidisciplinary and balanced approach to drugs combining demand and supply reduction, the 2005-2012 Strategy focused on these two policy fields as well as on two cross-cutting themes: 'International cooperation' and ' Information, Research and evaluation'. It also emphasised the importance of making optimal use of existing legal and information instruments and the need to ensure adequate consultation with a broad group of partners (e.g. scientific centres, drug professionals, representative NGOs, civil society and local communities). This eight-year Strategy formed the umbrella for two consecutive four-year EU Action Plans on Drugs. In terms of evaluation, the Strategy foresaw:

- annual progress reviews by the European Commission on the state of implementation of activities set out in the Action Plans;
- an impact assessment in 2008 (with a view to proposing a second action plan for the period 2009–2012);
- a final overall evaluation of the EU Drugs Strategy and Action Plans in 2012.

A final external evaluation of the previous EU Drug Strategy (2005–12) found that it provided a forum for consensus building and decision-making and a platform for information sharing and mutual learning. It also enhanced the 'voice' of the EU in international fora and promoted a culture of harmonised data collection and best practices identification. The review

145 Council Regulation (EC) No 111/2005 of 22 December 2004 (as amended by Regulation 1259/2013).

146 Council Decision 2005/387/JHA of 10 May 2005 on the information exchange, risk-assessment and control of new psychoactive substances.

147 COM (2004) 707 final.

recommended, among others, to further promote the development and use of evidence for drug policy, as there remain instances of insufficient evidence about the effectiveness of specific measures

The EU Drugs Strategy 2013-2020 set out the overarching political framework and priorities for EU drugs policy, for the period covered. The framework, aim and objectives of the Strategy serve as a basis for two consecutive four-year EU Drugs Action Plans, the first one covering the period 2013-16, and the second one covering 2017-2020[148]. The Strategy and Action Plan also framed the EU external policy in this field. They support the "voice" of the EU in international fora, provide guidance for candidate and neighbouring countries and a framework for regional bilateral cooperation with third countries.

In early 2017, the Commission assessed the progress made in implementing the EU Drugs Strategy 2013-2020 and the EU Action Plan on Drugs 2013-2016[149]. The Action Plan set out a political framework and priorities for the EU's drugs policy. The Strategy provides a single, evidence-based framework for tackling drugs inside and outside the EU, and is based on a five pillar structure including the reduction of drug supply. In this particular area, the evaluation found that whilst the efforts to enhance effective law enforcement coordination and cooperation (including enhancing judicial cooperation) were found to be behind schedule, those relating to responding effectively to current and emerging trends in illicit drug activity was assessed as being on target.

In line with the conclusions of this study, the Commission proposed on 15 March 2017 a new EU Action Plan for the period 2017-2020[150]. The new Action Plan on Drugs provides a strengthened response to the newly-emerging health and security challenges in the area of illicit drug use and trafficking. While maintaining and updating the core policy areas and cross-cutting themes of the overall EU Drugs Strategy, the new Action Plan identifies new priority areas for action, including the monitoring of new psychoactive substances as well as the use of new communication technologies for prevention of drug abuse and evidence gathering on the potential connection between drug trafficking and financing of terrorist groups and activities, migrant smuggling and trafficking in human beings.

New psychoactive substances

The proliferation of new psychoactive substances is a recent trend. The EU Early Warning System has facilitated the exchange of information between Member States and allowed the EMCDDA and Europol to identify emerging threats in relation to new substances. In 2016, 66 NPS were detected by the European Early Warning System. This number points to a decrease of the pace at which new substances appear on the market. However the availability of these substances remains high. By the end of last year, more than 620 NPS were monitored – they doubled since 2013. This requires a clear, strong and coherent answer at European level, thus pointing to the urgency of adopting a new legislative framework.[151]

148 Adopted by the 3552nd Meeting of the General Affairs Council on 20 June 2017.

149 Evaluation of the implementation of the EU Drugs Strategy 2013-2020 and of the EU Action Plan on Drugs 2013-2016: a continuous need - COM(2017) 195 final.

150 COM(2017) 195 final.

151 In November 2016, Eurojust and the EMCDDA issued a report on "New psychoactive substances in Europe" legislation and prosecution – current challenges and solutions".

On 29 May 2017, the Council and the Parliament reached a political agreement on a package reforming the legislation on NPS used as alternatives to illicit drugs. The new mechanism aims to allow more effective and efficient EU response to new psychoactive substances, which are appearing on the EU market at an unprecedented pace, posing a risk to public health and safety. The package is composed of an amendment to the founding Regulation 1920/2006 of the European Monitoring Centre for Drugs and Drug Addiction (EMCDDA) regarding information exchange, early warning system and risk assessment procedure on psychoactive substances and a Directive amending the Council Framework Decision 2004/757/JHA on the minimum provision on the constituent elements of criminal acts and penalties in the field of illicit drug trafficking.

External dimension

As far as international action is concerned, there is wide consensus that one key area in which the EU Strategy and Action Plan add value is enabling the EU to "speak with one voice" in international fora, as demonstrated in the run-up to UN General Assembly Special Session on Drugs (UNGASS) 2016. The drugs phenomenon is a global challenge and as such it requires global and comprehensive engagement: the EU is working with all Member States and its international partners to ensure that all commitments taken at the UN General Assembly Special Session on Drugs (UNGASS) 2016 are implemented.

Finally, the Maritime Analysis and Operations Centre (Narcotics) – MAOC (N) is a treaty-based organisation outside EU law: seven Member States, established the Centre by an international treaty. It provides a forum for multi-lateral cooperation to suppress illicit drug trafficking by sea and air. MAOC (N) is overwhelmingly funded by the Internal Security Fund of the European Union, currently of € 2.8 million over a period of 36 months, which represents 95% of the relevant costs of MAOC (N).

6. Environmental crime

a. Main findings

The attention of Member States' law enforcement authorities on organised environmental crime is increasing, as evidenced by the fact that environmental crime has become a political priority under the new Policy Cycle to fight serious and organised crime for the period 2018-2021[152]. Among the most recent activities, wildlife trafficking was the subject of a dedicated action plan (Communication on an EU 2016 Action Plan against Wildlife Trafficking[153]) which remains to be fully implemented.

A report on the contribution of criminal law to the fight against environmental crime is being prepared. The report would focus on (i) the main trends concerning environmental crime at national level; (ii) Member States' practice in investigating and prosecuting environmental crime as well as the main obstacles they face in this context and (ii) the added-value of the existing EU criminal legal framework as well as possible loopholes or additional elements that may need to be analysed further in view of any update or revision.

[152] For details on the Policy Cycle, see Chapter V.2 of the present assessment

[153] COM(2016) 87 final.

In addition to this, the Commission is supporting and collaborating with EU networks of police officers[154], prosecutors[155,] inspectors[156] and judges[157] specialised on combating environmental crime. The preparation for the Commission initiative on Environmental Compliance Assurance[158] announced in the Commission Work Programme for 2017[159] includes exchanges with these networks with a view to developing concrete actions and tools to tackle some key challenges concerning environmental crime.

b. Overview of EU action

Environmental crime in the European context concerns serious breaches of obligations stemming from EU environmental legislation, with one central instrument, namely the Environmental Crime Directive. Some legal instruments contain inspection requirements which, in practice, can help in the detection of environmental crime. Organised environmental crime covers most importantly wildlife trafficking and waste trafficking.[160]

Environmental crime covers activities and omissions that are connected with the unlawful exploitation of wild fauna and flora, pollution, illegal waste treatment and shipment, but can include other harmful acts of different degrees of seriousness as diverse as trafficking in animals and animal products, fly-tipping, unauthorised discharges into waters or the atmosphere, large-scale unlicensed fishing, damaging protected areas and buildings, destroying habitats and removing protected plants, illegal soil and sand mining, trade in ozone depleting substances, dumping and shipment of radioactive waste and potentially radioactive material, illegal logging and trade in wood. Depending on the specific criminal market the EU is the origin (e.g. illegal waste trafficking) or the destination market (e.g. protected species, illegal timber), and/or a hub for trafficking in transit to other regions (e.g. wildlife products)[161].

The low detection risk linked to its highly profitable nature makes environmental crime especially attractive for organised crime groups.[162] These groups use methods, such as falsification of transport documents and certification required under EU environmental legislation so as to facilitate phenomena such as illegal waste disposal. Due to the poly-crime nature of organised crime groups there are links with other criminal activities, such as trafficking in drugs and firearms, as well as with corruption, tax evasion and money laundering. Environmental crime not only has a devastating impact on biodiversity but it also undermines fair competition between economic operators, notably in the area of waste services. It also undermines the rule of law.

154 EnviCrimeNet.
155 European Network of Prosecutors for the Environment (ENPE).
156 IMPEL.
157 EU Forum of Judges for the Environment (EUFJE).
158 Environmental compliance assurance covers the broad range of methods to address problems of compliance with rules under the EU environmental *acquis*, including methods targeting at environmental crime.
159 The relevant roadmap is available at: http://ec.europa.eu/smart-regulation/roadmaps/docs/2015_env_066_environmental_compliance_assurance_en.pdf.
160 See also the report on the strategic project on Environmental Crime by Eurojust from 2013.
161 https://www.unodc.org/documents/data-and-analysis/wildlife/World_Wildlife_Crime_Report_2016_final.pdf.
162 http://www.rona.unep.org/news/2016/environmental-crime-threatening-peace-and-security-finds-new-interpol-un-environment.

The Court of Justice has played a crucial role in the development of an environmental criminal policy at EU level. In particular, in two landmark cases[163], the Court ruled that the fact that criminal law generally falls within the competence of Member States does not prevent the Community legislature from taking those essential measures for combating serious environmental offences which are necessary to ensure that environmental protection rules are fully effective. Since the adoption of the Lisbon Treaty, the legal basis for the adoption of criminal law provisions in the field of environment is clarified.

These judicial developments have paved the way for the adoption of Directive 2008/99/EC on the Protection of the Environment through Criminal Law. The Environmental Crime Directive pre-dates the Lisbon Treaty which enlarged the EU competence in this area.

The Environmental Liability Directive (Directive 2004/35/CE) is another important piece of EU legislation of relevance for combating environmental crime. It was adopted in 2004, after almost twenty years of deliberation by the EU. Its aim is to prevent and remedy environmentally harmful behaviour that affects protected species and natural habitats, waters and soil. Operators are required to take preventive action and bear the costs of remedial measures. While not an instrument of criminal law, provisions on environmental liability can help prevent environmental crime by making perpetrators liable for the consequences of their action and clean-up measures.

The Environmental Crime Directive (ECD)[164] requires Member States to criminalise under certain conditions violations of obligations stemming from more than 60 legal instruments at Union level. The ECD obliges Member States to criminalise unlawful conducts committed intentionally or with at least serious negligence by natural and legal persons. It imposes on Member States to provide for "effective, proportionate and dissuasive penalties". Those penalties must be of a criminal nature for natural persons while the choice is left to Member States for legal persons.

As far as the implementation of the ECD is concerned, Member States generally amended their national legislation. Among the main problems detected in the context of the transposition process were the coverage of offenses committed by serious negligence, as well as the liability of legal persons and the sanctions imposed on them under national law. The assessment of Member States's sanctioning systems was challenging in light of the very broad concept of "effective, proportionate and dissuasive penalties" contained in the ECD. Nevertheless, a number of Member States increased their level of sanctions as a consequence of the monitoring exercise.

At this stage, information is being gathered on the practical implementation of the ECD and the effectiveness of criminal enforcement in this area, and a review is currently undertaken on how national rules transposing the ECD are applied in practice and in particular whether and to which extent they contribute to the fight against organised environmental crime.

---

163 Judgment of the Court (Grand Chamber) of 13 September 2005. Commission of the European Communities v Council of the European Union, ECLI identifier: ECLI:EU:C:2005:542; Judgment of the Court (Grand Chamber) of 23 October 2007. Commission of the European Communities v Council of the European Union. Case C-440/05, ECLI identifier: ECLI:EU:C:2007:625.

164 Directive 2008/99/EC on the protection of the environment through criminal law, OJ L 328, 6.12.2008, p. 28–37.

As environmental crime grew, the threat it posed needed to be addressed by criminal justice. That is why the 2015 European Agenda on Security also environmental crimes, with a view to consider the need to strengthen compliance monitoring and enforcement.

Apart from legislation, the Union also uses softer approaches such as priority-setting on serious and organised crime and strategies. Besides providing a legislative framework, various bodies of the Union are also involved in monitoring and ensuring compliance with the legislative framework and providing support to Member States in combating environmental crime. The Commission, for instance, also provides judicial training, develops instruments for mutual cooperation on criminal matters and issues studies on environmental crime. Moreover, it works on improving inspections in Member States, can initiate infringement proceedings in case Member States do not properly implement EU environmental legislation.

On 26 February 2016, the Commission adopted an Action Plan on Wildlife Trafficking setting out a comprehensive blueprint for joined-up efforts to fight wildlife trafficking inside the EU, and for strengthening the EU's role in the global fight against these illegal activities[165]. The Action Plan focusses on prevention, stronger enforcement and global partnership. The Action Plan comes in support to the already strong EU rules on wildlife trade, notably to ensure their full implementation and enforcement. This requires better cooperation between enforcement agencies, adequate training, and support from Europol and cross-border operations between Member States and with partner countries.

Several of the EU's legal instruments in the area of environmental law, serve to implement international environmental agreements. The EU is party of Conventions, such as the Bern Convention on the Conservation of European Wildlife and Natural Habitats and the Convention on International Trade in Endangered Species of Wild Fauna and Flora (CITES Convention) which require an important dimension of criminal law application. The Ship-Source-Pollution[166] directive implements the MARPOL Convention 1973/1978. The Convention was adopted after severe ship accidents, which led to the release of oil and other substances into the environment. The Union is also part to the Aarhus Convention, under which members of the public must have access to courts to challenge the substantive and procedural legality of any decision, act or omission by private persons and public authorities which contravenes environmental law provisions.

Financial support to the policy implementation in this has been provided by the security research programme in both Framework Programme 7 and Horizon 2020. LIFE and the Internal Security Fund are also mentioned as sources of funding in the EU Action plan against wildlife trafficking.

[165] EU Action Plan against Wildlife Trafficking COM(2016) 87 final.

[166] Directive 2005/35/EC on ship-source pollution and on the introduction of penalties for infringements, OJ L 255, 30.9.2005, p. 11–21.

IV. CYBERSECURITY

European societies are increasingly dependent on electronic networks and information systems. Within the last 15 years, the evolution of information and communications technology has been very significant and has unsurprisingly also been accompanied by the development of a number of related criminal activities, often referred to in general as 'cybercrime', which may target citizens, businesses, governments and critical infrastructures.

In 2013, the Commission, together with the High Representative, put forward a Cybersecurity Strategy – "An Open, Safe and Secure Cyberspace" – which represented the EU's comprehensive vision on how to best support Member States and other stakeholders in preventing and responding to cyber disruptions and attacks.

The strategy outlines the principles guiding EU action in this domain - for example the importance of access to the internet and of the protection of fundamental rights online. It sets five priorities: (1) increasing cyber resilience; (2) drastically reducing cybercrime; (3) developing EU cyber defence policy and capabilities related to the Common Security and Defence Policy (CSDP); (4) developing the industrial and technological resources for cybersecurity; and (5) establishing a coherent international cyberspace policy for the EU and promote core EU values.

This assessment focusses mainly on the internal aspects of the Strategy, i.e. policies related to (1) increasing cyber resilience, (2) drastically reducing cybercrime and (4) developing the industrial and technological resources for cybersecurity[167]. It covers external activities only where they are directly related to these internal policies. The CSDP-related pillar (3) of the Cybersecurity Strategy is thus not part of this assessment. It also does not detail all initiatives and dialogues carried out as part of the EU's action to establish a coherent international cyberspace policy (5).

The Commission has further strengthened its approach in the past years by including cybersecurity at the heart of its political priorities: trust and security are at the core of the Digital Single Market Strategy presented in May 2015, while the fight against cybercrime is one of the three pillars of the European Agenda on Security of April 2015.

As announced in the mid-term review of the Digital Single Market Strategy[168], by September 2017 the Commission will, together with the High Representative/Vice-President, review the 2013 EU Cybersecurity Strategy to address the risks faced today, help improve the security in the Union and Member States and increase the confidence and trust of businesses and people in the digital economy and society. This will build on an assessment of the achievements of the 2013 EU Cybersecurity Strategy.

At operational level, the EU has specialised agencies and capabilities at its disposal to support its action on cybersecurity, including the European Union Agency for Network and Information Security Agency (ENISA), the European Cyber Crime Centre (EC3) at Europol and the Computer Emergency Response Team (CERT-EU).

---

[167] On the external side, a number of policy documents have also been adopted since 2013, such as the Cyber Defence policy Framework in 2014 and the Council Conclusions on Cyber diplomacy in 2015.

[168] Communication on the Mid-Term Review on the implementation of the Digital Single Market Strategy- A Connected Digital Single Market for All, COM(2017) 228 final.

1. Cybercrime policies

The **2013 EU Cybersecurity Strategy**[169] identifies the fight against cybercrime[170] as one pillar of a comprehensive approach to ensure cybersecurity. The Strategy advocates for ensuring full implementation of existing EU legislation as the first step in confronting cybercrime. The Commission is working with the Member States to ensure correct implementation of provisions in place and is preparing for further measures, for instance in the area of non-cash payment fraud. Cooperation among law enforcement authorities (for instance through the creation of the European Cybercrime Centre at Europol) and with the private sector is also of critical importance, with public-private partnerships to structure a common effort to fight online crime. Cybercrime demands a new approach to law enforcement in the digital age. In this area, the assessment shows that the EU intervention is perceived as successful but insufficient in view of the dynamically changing threat landscape. Given the constantly evolving nature of cybersecurity threats, measures that were appropriate in the 2013 context, while still relevant, are no longer proportionate in view of this changed threat landscape and the emergence of new threat actors and rapidly developing technology.

Overall, the comprehensive assessment points to continued relevance of all instruments currently in place but highlights the need for more measures at all levels – strategic, legislative and operational.

a. Main findings

The EU action on cybercrime encompasses legislative action, support for operational cooperation amongst Member States, international cooperation with public and private actors and funding.

In terms of legislative action, it emerges from the assessment that the current measures which focus mostly on the substantive legal framework, by setting common definitions and establishing standards for the minimum level of maximum penalties, is perceived positively by stakeholders. Stakeholders confirm that harmonised substantive law has facilitated cooperation across Member States, as reflected in the increased number of cases supported by Europol. In order to ensure that the adopted legislative framework is used to its full potential, however, stakeholders referred to the need to provide Member States with further support for the transposition and implementation of the cybercrime related directives, in particular the Directive on Child Sexual Abuse and the Directive on Attacks against Information Systems. In addition, the investigations are encountering new procedural challenges that are inadequately addressed in current legislation, in particular the need for swift investigation measures across borders and the challenges to effective judicial cooperation resulting from the current absence of a harmonised legal framework on data retention.

169 JOIN(2013) 1 final of 7 February 2013.

170 Cybercrime commonly refers to a broad range of different criminal activities where computers and information systems are involved either as a primary tool or as a primary target. Cybercrime comprises: (1) traditional offences (e.g. fraud, forgery, and identity theft) committed through the Interne; (2) offences unique to computers and information systems (e.g. attacks against information systems, denial of service and malware); (3) content-related offences related to child sexual abuse material, incitement to racial hatred, incitement to terrorist acts and glorification of violence, terrorism, and racism and xenophobia.

In terms of operational cooperation, it emerges from the assessment that Europol EC3 Centre is considered as a success and stakeholders are largely satisfied with the support it provides. The Joint Cybercrime Action Task force (J-CAT)[171] set up by Europol is also considered positively but too few Member States can afford to invest in it. The effective and efficient fight against cybercrime, including the coordinated response to large-scale attacks, requires a more complete threat intelligence picture and greater coordination among all relevant actors. It emerges from the assessment that demands for EC3 support have already outpaced supply and are likely to increase in the future. A wide range of stakeholders referred to the need to establish a joint centre of excellence for cyber forensics and encryption to provide support on analysis and operations to Member States, as this would allow to pool resources and support Member States that do not dispose of own capabilities.

The number of instances where Eurojust is requested to support, coordinate and contribute with its expertise is also rapidly growing.

b. Overview of EU action

Context

While cyber security was not officially part of the EU security priorities until 2005, the Commission actively contributed to the negotiation of the Council of Europe Budapest Convention on Cybercrime adopted in 2001. The Council of Europe's Convention on Cybercrime provides a common approach to tackle cybercrime and a valuable framework for international cooperation, with 55 parties from Europe and beyond. In an interconnected cyber-world, where every nation needs assistance from other countries to fight cybercrime, the Budapest Convention, being open to the accession of countries that are not parties to the Council of Europe, provides a flexible instrument of choice for doing so. It takes a broad approach, covering substantive and procedural criminal law, and thus provides a comprehensive framework for cooperation. The European Union supports and promotes the Budapest Convention internationally and urges Member States to ratify and implement it.

From the mid-2000s to 2014, the EU has significantly enhanced its focus on cybercrime, by giving it political consideration but also by creating institutions and policies to help tackle cyber risks.

Prior to the entry into force of the Lisbon Treaty, several EU instruments were adopted which covered substantive and procedural criminal law, cooperation and mutual assistance. Those included the Council Framework Decision on combating the sexual exploitation of children and child pornography[172], the Council Framework Decision on Attacks against information systems[173], the Council Framework Decision on fraud and counterfeit of non-cash means of payments[174], and the Council Framework Decision on combating racism and xenophobia[175].

---

171 J-CAT hosts national police officers temporarily seconded by national authorities on a temporary basis to EC3 (for a period of up to 6 months). The main added value of this group lies in its ability to pool national intelligence related to a single cybercrime case- which is typically scattered across several Member States- in order to build an accurate picture of its scale and relevance for EU coordinated action.

172 Council Framework Decision 2004/68/JHA of 22 December 2003, replaced by Directive 2011/92/EU of the European Parliament and of the Council of 13 December 2011 on combating the sexual abuse and sexual exploitation of children and child pornography.

173 Council Framework Decision 2005/222/JHA of 24 February 2005 on attacks against information systems

174 2001/413/JHA: Council Framework Decision of 28 May 2001 combating fraud and counterfeiting of non-cash means of payment.

In the field of criminal procedural law, the Mutual Legal Assistance Convention of 2000[176] is a key instrument.

At strategic level, the fight against cybercrime is guided by two strategies. Drastically reducing cybercrime is one of the priorities of the 2013 EU Cybersecurity Strategy. Fighting cybercrime more effectively is one of the three priorities under the 2015 European Agenda on Security 2015-2020. Cybercrime requires a coordinated response at European level, and the Security Agenda sets out the following actions:

- giving renewed emphasis to implementation of existing policies on cybersecurity, attacks against information systems, and combating 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;
- reviewing obstacles to criminal investigations on cybercrime, notably on issues of competent jurisdiction and rules on access to evidence and information; and
- enhancing cyber capacity building action under external assistance instruments.

The EU intervention consists of legislation and covers also support for operational cooperation and funding.

Legislation

Three main EU legislative actions contribute to the fight against cybercrime:

- Council Framework Decision 2001/413/JHA on combating fraud and counterfeiting of non-cash means of payment.
- Directive 2011/93/EU on combating the sexual abuse and sexual exploitation of children and child pornography
- Directive 2013/40/EU on attacks against information systems.

The 2001 Framework Decision on combating fraud and counterfeiting of non-cash means of payments was the first EU instrument in the field. It aims to ensure that fraud and counterfeiting involving all forms of non-cash means of payment are recognised as criminal offences and are subject to effective, proportionate and dissuasive sanctions in all Member States. The transposition reports show that Member States have used the margins of discretion left by the Framework Decision, resulting in very different levels of penalties for the same offence.

EU-wide law enforcement coordination and action has been conducive to more effectively tackling these forms of crime: in the framework of the EU Policy Cycle, a dedicated sub-priority within "Cybercrime" has targeted payment card fraud, resulting in several operational successes and tackling fraud in areas where private stakeholders seemed to have lost hope (e.g. fraud against airlines and e-commerce related fraud). The Policy Cycle has also contributed to identifying gaps and challenges (e.g. on "carding websites" selling bundles of compromised credit card credentials online).

---

[175] Council Framework Decision 2008/913/JHA of 28 November 2008 on combating certain forms and expressions of racism and xenophobia by means of criminal law, OJ L 328, 6.12.2008, p. 55–58.

[176] Council Act of 29 May 2000 establishing in accordance with Article 34 of the Treaty on European Union the Convention on Mutual Assistance in Criminal Matters between the Member States of the European Union.

EU-funded projects have created synergies and stimulated public-private cooperation, with the aims of improving law enforcement capacity (for instance through the RAMSES project, funded under the Secure Societies strand of Horizon 2020), assisting victims (for example through the PROTEUS project) and enhancing reporting of fraudulent transactions by financial institutions (as in the case of the OF2CEN project, funded under the ISEC programme and its successor, EU OF2CEN, funded under ISF-Police). Again, this allowed identifying shortcomings in the current framework (e.g. sharing information across borders).

As announced, the Commission is currently preparing a legislative proposal on non-cash means of payment based on an Inception Impact Assessment published in May 2016[177], which identifies areas that may benefit from further action at EU level:

- Shared definitions and minimal levels of maximum penalties;
- Scope of the legislation, to possibly cover conducts that are preparatory to fraud and counterfeiting of non-cash means of payment (e.g. phishing, collecting data), identity theft and the sale of stolen credentials (for instance on carding websites), and to cover non-corporeal payment instruments such as online wallets or mobile payment systems;
- Enhancing public-private cooperation and reporting of crimes;
- Enhancing operational cooperation.

A major step in the EU action to address sexual abuse and sexual exploitation of children was the adoption of **Directive 2011/93/EU on combating the sexual abuse and sexual exploitation of children and child pornography**[178], which replaced the 2003 Council Framework Decision.

Sexual abuse and sexual exploitation of children are particularly serious forms of crime with a cross border dimension, as listed in Article 83 of the Treaty on the Functioning of the European Union. They produce long-term physical, psychological and social harm to vulnerable victims, children, who have the need and the right to special protection and care, as explicitly provided for in Article 24 of the Charter of Fundamental Rights of the European Union. A common European level of understanding on issues including age of consent, victim identification and further methods of the illicit use of the internet in the light of dramatic advancements in electronic communication technologies were considered necessary to effectively combat the sexual abuse of children.[179]

The Directive is a comprehensive legal instrument that sets out minimum standards to be applied throughout the European Union. It follows a holistic approach, incorporating provisions covering investigation and prosecution of offences, assistance and protection of victims, and prevention.

The Commission is currently monitoring implementation and has found that there is still considerable scope for the Directive to reach its full potential. The Commission focuses on

177 http://ec.europa.eu/smart-regulation/roadmaps/docs/2016_home_077_non_cash_payment_en.pdf.

178 Directive 2011/92/EU of the European Parliament and of the Council of 13 December 2011 on combating the sexual abuse and sexual exploitation of children and child pornography, and replacing Council Framework Decision 2004/68/JHA, OJ L 26, 28.1.2012, p. 1–21.

179 Report from the Commission based on Article 12 of the Council Framework Decision of 22 December 2003 on combating the sexual exploitation of children and child pornography, COM (2007) 716 final.

ensuring that children benefit from the full added value of the Directive through its complete and correct implementation by Member States.[180]

Part of the planned support is the exchange of best practices, to be carried out in a series of meetings starting in the autumn 2017.

There are, however, a number of issues not covered in the Directive but frequently highlighted as problematic.[181] For example:

- Lack of mandatory background checks for employment and volunteering relating to children;
- Lack of mandatory reporting by industry of child sex abuse material detected in their infrastructure and conservation of evidence – the embryo of an equivalent of the US' NCMEC (National Centre for Missing and Exploited Children);
- Management of travel by convicted child sex offenders and exchange of information on individuals posing a risk for children;
- Possibility for hotlines to proactively search child sexual abuse material (like IWF in the UK);
- Need for additional investigation tools in view of new challenges, such as anonymization, darknet, P2P networks and live streaming.

Particularly challenging global issues include the exchange of information of travel by convicted child sex offenders and individuals posing a risk for children.

To facilitate the implementation of the Directive and the achievement of its objectives, the Commission has funded several initiatives ranging from the INHOPE network of hotlines, raising awareness among parents and educators (Better Internet for Kids initiative under Connecting Europe Facility) to supporting INTERPOL in enhancing global law enforcement cooperation in this area and allowing for the creation and maintenance of the central global victim identification database (ICSE).[182]

With regard to international cooperation in this field, to raise standards worldwide, the Commission co-launched the Global Alliance Against Child Sexual Abuse Online rallying 54 countries to better identify child victims, improve investigations, enhance public awareness and reduce the availability of child pornography. This initiative is gaining further strength through the merger with the UK-led WePROTECT initiative, to be formalized this year. The merged entity[183] will include more than 70 countries, along with major international organisations, technology companies, and leading civil society organisations.

The ongoing work at the Commission with regard to cross-border access to digital evidence as well as on the role of encryption in criminal investigations is directly related to the goals of the Directive. For example, Article 15 requires Member States to ensure that effective investigate tools are available to the units investigating child sexual abuse, in particular with regard to victim identification. Other provisions cover issues on jurisdiction, offences concerning child pornography and solicitation of children for sexual purposes.

---

180 http://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1486726102713&uri=CELEX:52016DC0871.

181 As also highlighted by the European Parliament in its 2015 resolution on this issue, 2015/2564(RSP).

182 https://www.interpol.int/Crime-areas/Crimes-against-children/Victim-identification.

183 http://www.weprotect.org/.

The most recent EU instrument in the field of cybercrime is **Directive 2013/40/EU on attacks against information systems.**[184] The objectives of the Directive are to subject attacks against information systems in all Member States to effective, proportionate and dissuasive criminal penalties and to improve and encourage cooperation between judicial and other competent authorities.

For that purpose, the Directive establishes minimum rules concerning the definition of criminal offences and the relevant sanctions, and obliges Member States to establish a network of national operational points of contact. This obligation strengthens the importance of the networks set up before, e.g. following the Council Recommendation of 25 June 2001 on contact points maintaining a 24-hour service for combating high-tech crime.

The Commission is currently assessing the transposition of the Directive by Member States.

In general, the development of technology and practices of cybercriminals over the recent years has posed new challenges for criminal investigations and has increased the need for cross-border cooperation between authorities. In that regard the scope of the existing instrument appears to be rather limited and lacks rules relating to cross-border access to electronic evidence and the role of encryption in criminal investigations[185].

While the assessment is still ongoing, it appears that the use of approximated definitions of criminal offences and the relevant sanctions has improved operational cooperation between Member States' authorities on specific investigations.

To support implementation, the Commission addressed reasoned opinions to Bulgaria, Belgium and Ireland in December 2016 for non-communication of complete transposition of Directive 2013/40/EU on attacks against information systems in their national legislation.[186]
In parallel, the Commission is reviewing how to remove obstacles to the investigation of cyber-enabled crime and terrorism. In 2016, Eurojust and Europol presented a joint paper, listing the most prominent common challenges faced in criminal investigations and prosecutions of cybercrime. This document was updated in 2017.[187]

In particular, the Commission is currently reviewing mechanisms available for obtaining cross-border access to **electronic evidence**[188]. The Commission reported to the 8 June 2017 Council on the results of a comprehensive expert consultation process that identified possible options to improve cross-border access to electronic evidence for criminal investigations.[189]

Also in the area of electronic evidence, Europol has indicated[190] that technologies[191] used by Internet Service Providers to allocate one IP address to multiple users are an increasing

[184] Replacing Council Framework Decision 2005/222/JHA.
[185] The Commission is exploring various options with a view to presenting conclusions in October 2017.
[186] Ireland recently notified the Commission of its transposition of the Directive.
[187] Updated version in Council doc. 14812/15: http://data.consilium.europa.eu/doc/document/ST-7021-2017-INIT/en/pdf.
[188] The work stems from the Commission's commitment in the April 2015 European Agenda on Security to address obstacles to access to evidence, the April 2016 communication on implementing the European Agenda on Security, which included a commitment to deliver solutions by June 2017, and the June 2016 Council conclusions on improving criminal justice in cyberspace, which call on the Commission to present solutions by June 2017.
[189] https://ec.europa.eu/home-affairs/what-we-do/policies/organized-crime-and-human-trafficking/e-evidence_en
[190] iOCTA 2016, page 57.
[191] These technologies are referred to as Carrier Grade Network Address Translation (CGN).

problem for investigators, because it greatly complicates the identification of criminals to the point that some investigations must be abandoned.

The Commission has also begun a review of the role of **encryption** in criminal investigations. This stems from the Commission's commitment in the April 2015 European Agenda on Security to explore with service providers concerns law enforcement authorities have on encryption technologies followed by the discussion launched by the Slovak Presidency of the Council on the role of encryption in criminal investigations, which was concluded at the 8-9 December 2016 JHA Council meeting. Moreover, in its Internet Organised Crime Threat Assessment 2016, Europol highlights that "*The growing misuse of legitimate anonymity and encryption services and tools for illegal purposes poses a serious impediment to detection, investigation and prosecution, thereby creating a high level of threat cutting across all crime areas*."

As announced, the Commission intends to report on its conclusions on encryption to the Council in the fourth quarter of 2017.

Operational cooperation

To support **operational cooperation** among Member States, Europol's Cybercrime Centre (EC3) was set up in 2013 as an integral part of Europol and has become a focal point in combatting and preventing cross-border cybercrime. The Centre serves as the central hub for criminal information and intelligence and:

- supports Member States' operations and investigations by means of operational analysis, coordination and expertise;
- provides strategic analysis products;
- reaches out to cybercrime related law enforcement services, private sector, academia and other non-law enforcement partners (such as internet security companies, the financial sector, computer emergency response teams) to enhance cooperation;
- supports prevention, awareness raising, training and capacity building in the Member States;
- provides highly specialised technical and digital forensic support capabilities to investigations and operations; and
- serves as a common voice for the EU law enforcement community (R&D requirements, internet governance, policy development).

The EC3 focuses on providing operational support of the Member States at the EU level for cross-border cybercrime, as well as specialised strategic and threat assessments. EC3 supports Member States and links investigations in different Member States, either via direct contacts or the Joint Cybercrime Action Task Force (J-CAT) set up by Europol. J-CAT hosts of police officers temporarily seconded by national authorities on a temporary basis to EC3 (for a period of up to 6 months). The main added value of this group lies in its ability to pool national intelligence related to a single cybercrime case - which is typically scattered across several Member States - in order to build an accurate picture of its scale and relevance for EU coordinated action.

A regular production of strategic reports on emerging threats and trends was established to identify priorities.

The EC3 also created advisory groups in order to develop strategic cooperation with the private sector. Four dedicated advisory groups have been created in the areas of internet

security, financial services, communication services and e-commerce in order to foster closer cooperation with its leading non-law enforcement partners.

In the area of awareness-raising, prevention and mitigation, Europol participates in the recently launched project "No More Ransom!". Founded by the Dutch National Police, Europol, Intel Security/McAfee and Kaspersky Lab, this projects aims to combat ransomware, by helping victims and raising awareness, in particular by making available to the public a wide range of decryption tools.

In providing support to Member States' law enforcement and judicial authorities, Europol and Eurojust have increased their operational cooperation. Many cases now involve operational and judicial coordination from an early stage, leading to more effective and more efficient investigations and prosecutions. A Eurojust representative is seconded to the EC3 to build the bridge between Eurojust and Europol, facilitating the exchange of information, and supporting and coordinating cooperation with the EC3.

Eurojust has also intensified its focus on the support it provides to Member States in cases of cybercrime, leading to a steep rise in the number of cases supported by Eurojust.

To further improve judicial cooperation within the EU, in 2016 the Council has established the European Judicial Cybercrime Network. The task of this network of specialised prosecutors and judges is to facilitate and enhance cooperation between the competent judicial authorities dealing with cybercrime, cyber-enabled crime and investigations in cyberspace, by facilitating exchange of information and best practices, as well as fostering dialogue among the different actors and stakeholders that have a role in ensuring the rule of law in cyberspace. In line with Council expectations, Eurojust provides support to the network in accomplishing its tasks.

International cooperation

In view of the cross-border nature of the internet, the Commission is also engaged in policy development activities at international level. With the United States as a key partner in the fight against cybercrime, the Commission engages in regular dialogues at working level in the context of the EU-US working group on cybercrime. The EU-US working group on cybercrime provides for an opportunity for collaboration on relevant issues, including on cross-border access to electronic evidence, the role of encryption in criminal investigations and the fight against child sexual abuse and exploitation online. The EU-US working group reports back periodically at senior official and ministerial level.

The Commission engages in policy development processes under the Internet Corporation for Assigned Names and Numbers (ICANN) with a focus on public safety consequences of the organisation of the Internet. In view of ICANN's responsibility for the coordinating of the maintenance and procedures of the Internet's Domain Name System (DNS)[192], the Commission continuously assesses at policy level potential risks of abuse by cybercriminals, and ways to ensure accountability online by law enforcement authorities on the basis of the functioning of the DNS. The Commission co-chairs the Public Safety Working Group

[192] The Domain Name System (DNS) associates domain names with relevant information, e.g. it allows for the translation of readable domain names (www.europa.eu) to numerical Internet Protocol (IP) addresses that are used for identifying and localising services and devices at technical level, and is therefore an essential component of the functioning of the Internet.

(PSWG) of ICANN's Governmental Advisory Committee (GAC), which meets several times a year.

Funding

As far as **EU funding** is concerned, in addition to financing Europol's EC3 (staff and operational costs), the Commission supports the fight against cybercrime by funding cybercrime projects through tools such as:

- the Prevention and Fight against Crime Programme (ISEC 2007-2013) which has contributed around EUR 15 million to the fight against cybercrime since 2007;
- the Internal Security Fund (ISF) as the successor to ISEC for the period 2014-2020, with a total budget slightly over EUR 1 billion available for funding actions under the ISF Police instrument, including the fight against cybercrime. Concrete actions to be funded through this instrument can include a wide range of initiatives, such as setting up and running IT systems, acquisition of operational equipment, promoting and developing training schemes and ensuring administrative and operational coordination and cooperation;
- Under the 7th Framework Programme for Research and Technological Development (FP7, 2007-2013), the EU invested 80 million euros in cybercrime-related projects, addressing topics like legal, criminological and sociological aspects of cyber-crime as a new European-scale emergency[193], the economy of cybercrime, risk analysis for infrastructure protection, money laundering, identity theft, European informatics data exchange framework for court and evidence, or dedicated road mapping actions;
- In the first two years of Horizon 2020 (2014-2015), six cybercrime-related projects were selected within the Fight against Crime and Terrorism (FCT) call, with the total of 33 million euros;
- Beyond the EU, the Commission funds cybercrime capacity building through
    - the Instrument contributing to stability and peace, including 9 million for the GLACY+ project run by the Council of Europe (in partnership with INTERPOL) between 1 March 2016 and 27 February 2020, which aims to strengthen the capacities of States worldwide to apply legislation on cybercrime and electronic evidence and enhance their abilities for effective international cooperation in this area;
    - the Instrument for Pre-Accession Assistance (IPA), including 5 million for the CyberProceeds@IPA project run by the Council of Europe between 15 December 2015 and 14 June 2019, which aims to strengthen the capacity of authorities in Western Balkans and Turkey to search, seize and confiscate cybercrime proceeds and prevent money laundering on the Internet.

2. Policies aimed at achieving cyber resilience and developing the industrial and technological resources for cybersecurity

a. Main findings

The protection of network and information security is the first line of defence against cybercrime. Every day, cyber security incidents cause major economic damage to the European economy and businesses. Cyber-attacks are a key component of hybrid threats;

[193] http://fiduciaproject.eu/wps.

timed precisely in conjunction with physical threats, such as terrorism, they can have a devastating impact, destabilising a country or challenging its political institutions. As they increasingly rely on online technologies, critical infrastructure such as energy grids, satellite communications and healthcare systems become ever-more vulnerable. This is a key challenge facing the Union and one where action at EU level can make a real difference to our collective resilience. Ensuring the security of the Union requires the mainstreaming of cybersecurity across both our internal and external security work and a broad range of EU policies.

Since 2013, the cybersecurity context has evolved significantly, in terms of threats landscape technology, market and policy developments. Given the constantly evolving nature of cybersecurity threats, and the dynamic policy development in this field, this part of the assessment presents the main elements of EU action on achieving cyber resilience.

In terms of legislation, considering that the main act – the Directive on security of network and information systems (NIS Directive) was adopted in 2016, it appears from the assessment that its objectives are still consistent with the current needs and the Directive clearly brings EU added value. For the time being, the Member States have very different levels of capabilities and preparedness leading to fragmented approaches across the EU. Once transposed and implemented, the new directive will ensure that all Member States have in place a minimum level of national capabilities.

With regard to the European Union Agency for Network and Information Security (ENISA)[194], the 2013 Regulation gave ENISA a very broad mandate in the cybersecurity area that allowed the agency to be flexible in terms of responding to new challenges not specifically mentioned in the legal text. The Commission is currently performing a full evaluation of ENISA, with a view to review its mandate. The evaluation aims to assess the relevance, impact, effectiveness, efficiency, coherence and EU added value of the agency. In light of the significant changes that occurred in the cybersecurity landscape since 2013, in the dialogue process of the assessment, stakeholders noted the need for focussing on the support to Member States cooperation to strengthen Europe's cyber resilience and on the cooperation with other agencies, such as Europol and Eurojust.

As regards industrial policy, the objectives of the recently created contractual Public-Private Partnership[195] in this area are still consistent with the current needs. However, stakeholders pointed to the need of expanding the EU investment in the field of cybersecurity which still remains substantially lower if compared to other key global players such as e.g. the US or China. As a positive development resulting from the establishment of the contractual Public-Private Partnership (cPPP) was considered the fact that it stimulated private cybersecurity actors to organise themselves at European level and overcome the fragmentation which existed earlier.

---

194 Regulation (EU) No 526/2013 of the European Parliament and of the Council concerning the European Union Agency for Network and Information Security (ENISA) and repealing Regulation (EC) No 460/2004, OJ L 165, 18.6.2013, p. 41–58.

195 Commission Decision on the signing of a contractual arrangement on a public-private partnership for cybersecurity industrial research and innovation between the European Union, represented by the Commission, and the stakeholder organisation, C(2016) 4400 final (5.7.2016). For further details, see: https://ec.europa.eu/digital-single-market/en/news/commission-decision-establish-contractual-public-private-partnership-cybersecurity-cppp.

Overall, the assessment points to continued relevance of all instruments currently in place but highlights the need for more measures at all levels – strategic, legislative and operational.

b. Overview of EU action

Since the adoption of the first EU Cybersecurity Strategy in 2013, the European Commission has stepped up its efforts to better protect Europeans online.

EU action to develop cyber resilience and industrial capabilities pursues **three main objectives**:

- Increasing cybersecurity capabilities and cooperation. The aim is to bring cybersecurity capabilities at the same level of development in all the EU Member States and ensure that exchanges of information and cooperation are efficient, including at cross-border level;
- Making the EU a strong player in cybersecurity. Europe needs to be more ambitious in nurturing its competitive advantage in the field of cybersecurity to ensure that European citizens, enterprises (including SMEs), public administrations have access to the latest digital security technology, which is interoperable, competitive, trustworthy and respects fundamental rights including the right to privacy and data protection. This should also help take advantage of the booming global cybersecurity market. To achieve this Europe needs to overcome the current cybersecurity market fragmentation and foster European cybersecurity industry; and
- Mainstreaming cybersecurity in EU policies by embedding cybersecurity in the future EU policy initiatives from the start, in particular with regard to new technologies and emerging sectors such as connected cars, smart grids and the Internet of Things (loT).

Since 2013, the Commission has adopted a set of legislative proposals; in particular the Directive on Security of Network and Information Systems (NIS Directive), earmarked more than EUR 600 million of EU investment for research and innovation in cybersecurity projects during the 2014-2020 period, and fostered cooperation within the EU and with partners on the global stage.

In July 2016, the Commission presented additional measures to boost the cybersecurity industry and to tackle cyber-threats.[196] The **Digital Single Market Strategy** presented in May 2015 called for the creation of a public-private partnership on cybersecurity. The partnership was signed on 5 July 2016 by the Commission and the European Cyber Security Organization (ECSO) – an industry-led association, which includes a wide variety of stakeholders such as large companies, SMEs and start-ups, research centers, universities, end-users, operators, clusters and association as well as public authorities.

Legislation

Over the past few years, the European Commission has adopted a series of measures to raise Europe's preparedness to ward off cyber incidents. The approach adopted previously in the area of NIS[197], starting in 2001, mainly consisted in the adoption of a series of action plans

[196] See: http://europa.eu/rapid/press-release_IP-16-2321_en.htm.

[197] Security of network and information systems (NIS) means the ability of network and information systems to resist, at a given level of confidence, any action that compromises the availability, authenticity, integrity or confidentiality of stored or transmitted or processed data or the related services offered by, or accessible via, those network and information systems.

and strategies urging the Member States to increase their NIS capabilities and to cooperate to counter cross border NIS problems[198].

The adoption of the NIS Directive[199] was a key step towards building European level cybersecurity resilience. The Directive was adopted in July 2016 and Member States have until May 2018 to transpose the Directive into their national laws and 6 months more to identify operators of essential services. Its objective is to achieve a high common level of security of network and information systems within the EU. The four cornerstones of the NIS Directive are:

- Improving national cybersecurity capabilities - Member States will be required to adopt a national NIS strategy defining the strategic objectives and appropriate policy and regulatory measures in relation to cybersecurity. Member States will also be required to designate a national competent authority for the implementation and enforcement of the Directive, as well as Computer Security Incident Response Teams (CSIRTs) responsible for handling incidents and risks.
- Improving cooperation - The Directive creates 'Cooperation Group' between Member States, in order to support and facilitate strategic cooperation and the exchange of information among Member States and to develop trust and confidence amongst them. The Commission provides the secretariat for the Cooperation Group. The Directive also creates a network of Computer Security Incident Response Teams, known as the CSIRTs Network, in order to promote swift and effective operational cooperation on specific cybersecurity incidents and sharing information about risks. The EU Agency for Network and Information Security (ENISA) provides the secretariat for the CSIRTs Network.
- Security and notification requirements for operators of essential services - Businesses with an important role for society and economy, referred in the Directive as "operators of essential services", will have to take appropriate security measures and to notify serious incidents to the relevant national authority[200].
- Security and notification requirements for digital service providers - Important digital businesses, referred to in the Directive as "digital service providers" (DSPs), will also be required to take appropriate security measures and to notify serious incidents to the competent authority. The Directive will cover the providers of the following services: online marketplaces; cloud computing services and search engines.

As the Directive was recently negotiated and adopted, its objectives are still consistent with the current needs. At the same time, the Directive clearly brings EU added value. For the time being, the Member States have very different levels of capabilities and preparedness leading

198 For a detailed overview see Annex II "Action plans and strategies adopted so far in the field of Network and Information Security in the EU" of the Impact Assessment of the NIS Directive, SWD (2013) 31 final (7.2.2013).

199 Directive (EU) 2016/1148 on Security of Network and Information Systems (NIS Directive)

200 The Directive covers such operators in the following sectors: energy (electricity, oil and gas); transport (air, rail, water and road); banking (credit institutions); financial market infrastructure (trading venues, central counterparties); health (healthcare providers); water (drinking water and distribution) and digital infrastructure (internet exchange points which enable interconnection between the internet's individual networks, domain name system service provides, top level domain name registries). Member States need to carry out a so-called identification process in which they have to define which entities concretely referred to in Annex II will fall under the scope of the NIS Directive. This identification process will be based on criteria laid down in the directive, such as whether the service provided by the entity is essential for the maintenance of critical societal or economic activities.

to fragmented approaches across the EU. Therefore, cooperation and information sharing is happening mainly among a minority of Member States with a high-level of capabilities. The establishment of the strategic and operational cooperation mechanisms which are entrusted with concrete tasks under the Directive should be a major improvement in this regard. However, since the cooperation is voluntary, the success of those mechanisms will depend on the level of Member States' involvement in the process. Once transposed and implemented, the new Directive will ensure that all Member States have in place a minimum level of national capabilities.

European Union Agency for Network and Information Security Agency (ENISA)

The European Union Agency for Network and Information Security (ENISA) was set up in 2004 with a regulation based on Article 114 TFEU. Its legal basis was revised in 2013 and this is the regulation currently applicable. The overall objective was to contribute to a high level of network and information security within the EU.[201]

The 2013 ENISA's Regulation mandated the agency to contribute to a high level of network and information security within the Union and to raise awareness on these matters for the benefit of citizens, consumers, enterprises and public sector organisations with the ultimate goal of supporting the single market.

ENISA helps the Commission, the Member States and the business community to address, respond and especially to prevent NIS problems. The main activities run by ENISA include:

- collecting and analysing data on security incidents in Europe and emerging risks;
- promoting risk assessment and risk management methods to enhance capability to deal with information security threats;
- running of pan-European cyber exercises;
- supporting Computer Emergency Response Teams (CERTs) cooperation in the Member States;
- awareness-raising and cooperation between different actors in the information security field.

ENISA carries out its activities according to an annual and multiannual work programme. It is granted an autonomous budget financed primarily through a contribution from the Union as well as contributions from third countries participating in the agency's work. Member States are also allowed to make voluntary contributions to the revenue of the agency.

The 2013 Regulation gave ENISA a very broad mandate in the cybersecurity area that allowed the agency to be flexible in terms of responding to new challenges not specifically mentioned in the legal text. However, since 2013, the cybersecurity context has evolved significantly, in terms of threat landscape, technology, market and policy developments. The ever increasing digital connectivity makes cyberspace more vulnerable and exposes the economy and society to cyber threats. On the regulatory front, delivering on the EU Cybersecurity Strategy, the adoption of the first EU wide legislation on cybersecurity – the Directive on security of network and information systems (the "NIS Directive") – constitutes a major development with impact also on ENISA, which is entrusted some important new tasks by the Directive.

[201] Regulation (EU) No 526/2013 of the European Parliament and of the Council concerning the European Union Agency for Network and Information Security (ENISA) and repealing Regulation (EC) No 460/2004.

The Commission is currently performing a full evaluation of ENISA, as requested by Article 32 of its Regulation, with a view to revise its mandate that is currently set to expire in 2020. The final results of the evaluation are expected in the third quarter of 2017. The evaluation aims to assess the relevance, impact, effectiveness, efficiency, coherence and EU added value of the agency having regard to its performance, governance, internal organisational structure and working practices. A public consultation on ENISA's evaluation and review has recently been concluded and its results are being analysed.

Contractual Public Private Partnership on Cybersecurity (cPPP)

The contractual Public Private Partnership on cybersecurity (cPPP) is one of the 16 initiatives put forward in the Commission's Digital Single Market Strategy. Its establishment was announced in the European Commission's Communication on Strengthening Europe's Cyber Resilience System and Fostering a Competitive and Innovative Cybersecurity Industry and constitutes an important element of the implementation of the 2013 EU Cybersecurity Strategy. The contract between the European Commission and the industry represented by the European Cybersecurity Organisation (ECSO) was signed on 05 July 2016.

The goal of this partnership is to stimulate European competitiveness and help overcome cybersecurity market fragmentation through innovation, building trust between Member States and industrial actors as well as helping align the demand and supply sectors for cybersecurity products and solutions. It aims at gathering industrial and public resources to deliver excellence in research and innovation and maximise the use of available funds through greater coordination with Member States and regions.

The EU will invest EUR 450 million in calls for proposal related to this partnership, under its research and innovation programme Horizon 2020. Cybersecurity market players, represented by ECSO[202], are expected to invest three times more bringing the total investment to EUR 1.8 billion. The Commission launched the first H2020 calls for proposals under the cybersecurity PPP at the end of 2016 and in the first quarter of 2017

Given that it is a recently created Partnership, with active involvement of industry partners and other stakeholders from the cybersecurity community, it can be assumed that the objectives are still consistent with the current needs. At the same time it is worth noting that the EU investment in the field of cybersecurity is substantially lower if compared to other key global players such as e.g. the US or China.

In this context the creation of the cPPP stimulated cybersecurity players to organise themselves at the European level. The European Cyber Security Organisation (ECSO) was launched on 13 June 2016 in Brussels.

Other funding

The **EU financial support** in the field of cybersecurity focusses on three main strands: research and innovation, infrastructure and capacity building in third countries.

[202] ECSO is a fully self-financed non-for-profit association (ASBL) under Belgian law and became a legal counterpart for the contractual cPPP in July 2016. Since its launch the organisation was joined by more than 190 members, with members including large European and global companies, SMEs and startups, research centres, universities, clusters and associations as well as local, regional and national administrations.

For research and innovation, during the 2007-2013 period, the EU invested EUR 334 million in cybersecurity and online privacy projects. Topics such as trustworthy network and service infrastructures, cryptology and advanced biometrics were addressed under the **7th Framework Programme (FP7)** and the **Competitiveness and Innovation Programme (CIP)**. During the same period, the Security Research theme of FP7 invested EUR 50 million in cybercrime projects addressing topics like the economy of cybercrime, risk analysis for infrastructure protection, money laundering and dedicated road mapping actions. For the period 2014-2016, the EU has so far invested EUR 160 million under the **H2020 Research and Innovation Framework Programme** in cybersecurity research and innovation projects.

Cybersecurity and privacy are part of two streams of the Horizon 2020 programme. Under the Societal Challenge "Secure societies – Protecting freedom and security of Europe and its citizens", there are two relevant strands - the Digital Security strand and fighting Crime and Terrorism strand.

The Digital Security strand focuses on increasing the security of current applications, services and infrastructures by integrating state-of-the-art security solutions or processes, supporting the creation of lead markets and market incentives in Europe. Security is also a so-called "digital focus area" under other challenges (privacy and security in ehealth; energy; transport; innovative security solutions for public administrations). The aim is to ensure digital security integration in the application domains.

The Fighting Crime and Terrorism strand focuses on increasing the knowledge of the cybercrime phenomenon - its specificities, its economy (including its unlawful markets and its use of virtual currencies) and the means for law enforcement authorities to fight it more efficiently and to prosecute offenders with more solid evidence from specialised forensic activities.

Under "Leadership in enabling and industrial technologies", projects on dedicated technology-driven digital security building blocks are funded (such as the 2014 calls on Cryptography and Security- by-Design). Security is also integrated as a functional requirement in specific technologies, such as the Internet of Things, 5G, Cloud, etc.

EU funding is also available for infrastructure projects. For the 2014-2020 period, the **European Structural and Investment (ESI**) Funds foresee a contribution of up to €400 million for investments in trust and cybersecurity. The ESI funds can finance security and data protection investments to enhance interoperability and interconnection of digital infrastructures, electronic identification, privacy and trust services.

Cybersecurity is one of the areas supported under the Digital Service Infrastructures (DSIs) stream within the **Connecting Europe Facility (CEF)**. The funded projects deploy trans-European digital services based on solutions such as e-identification and interoperable health services. One of the aims is to achieve cross-border cooperation in cybersecurity, enhancing the security and thus the trust in cross-border electronic communication, contributing to the creation of the Digital Single Market.

In 2014-2016, the EU invested about €20 million in such projects; an additional investment of EUR 12 million is earmarked for a call for proposals to open in May 2017.

The Communication on strengthening Europe's Cyber Resilience System and Fostering a Competitive and Innovative Cybersecurity Industry[203] announced the development of a Cybersecurity Smart Specialisation Platform to help Member States and regions interested in investing in innovation in the cyber-security sector (RIS3) with the European Regional Development Fund.

International

A coordinated EU action at international level in the field of cybersecurity is ensured by the European External Action Service (EEAS) and Commission services, together with the Member States. In doing so, they seek to uphold EU core values and promote a peaceful, open and transparent use of cyber technologies. The HR, the Commission and the Member States engage in policy dialogue with international partners and with international organisations such as the Council of Europe, the Organisation for Economic Co-operation and Development (OECD), the Organization for Security and Co-operation in Europe (OSCE), the North Atlantic Treaty Organization (NATO) and the United Nations (UN).

The EEAS and Commission services, in close cooperation with the Member States, also establish links and dialogues on international cyber policy and security of information and communication technologies with key strategic partners such as Brazil, China, India, Japan, the Republic of Korea and the United States.

The Commission also supports capacity building in third countries, recognising the strong link between increased cyber resilience and sustainable development. The objectives are to increase third countries' technical capabilities, preparedness, and establish effective legal frameworks to address cybercrime and cybersecurity problems; and at the same time enhance their capacity for effective international cooperation in these areas. The Commission has partnered with the Council of Europe and EU Member States for the implementation of these actions.

At a global and trans-regional level these initiatives are financed by the **Instrument contributing to Stability and Peace (IcSP)** where cybersecurity and combatting cybercrime have been identified as areas of priority since 2013 with an allocation of EUR 4.5 million for 2013, and an indicative allocation of EUR 21.5 million over the period 2014-2017.

In specific regions, the Commission has also used other instruments, including the **European Neighbourhood Instrument (ENI)**, to help countries of the Eastern Partnership (Armenia, Azerbaijan, Belarus, Georgia, Moldova, Ukraine) to define strategic priorities related to the fight against cybercrime. The Instrument of Pre-accession (IPA) finances a new action of EUR 5 million to help countries in South-Eastern Europe and Turkey to cooperate on cybercrime. The roll-out of more actions in these areas is foreseen in the next years, also through other financing instruments.

[203] COM (2016)0410 final.

V. INFORMATION EXCHANGE AND OPERATIONAL COOPERATION

Cooperation against crime and terrorism at EU level focuses primarily on the cross-border exchange of information and on different forms of operational cross-border cooperation. This has been a policy priority in the justice and home affairs area for the last 15 years. In order to enhance European cooperation, a number of tools have been set up for law enforcement, criminal investigation and judicial cooperation purposes, as well as EU centralised and decentralised information systems.

The Convention Implementing the Schengen Agreement (CISA), often referred to as the Schengen Convention, offers essential instruments for **cross-border operational police cooperation**. Title III on police cooperation and judicial cooperation contains provisions on cross-border surveillance (Art. 40) and hot pursuit (Art. 41). The Prüm Decisions on the stepping up of cross-border cooperation to combat terrorism and cross-border crime further complements this by adding other forms of cooperation, such as joint patrols and other joint operations in which officers from a Member State participate in operations within another Member State's' territory (Art. 17).

Together with Article 39 CISA on mutual assistance, the Prüm Decisions and the Swedish Framework Decision[204] constitute the backbone of the EU framework of **information exchange** between law enforcement authorities. It outlines conditions for the exchange of information in the context of conducting a criminal investigation or criminal intelligence operation. They are complemented by more specific instruments.

As regards **centralised information systems**, the second generation of the Schengen Information System (SIS II) is at the very heart of Schengen cooperation. Moreover, law enforcement authorities have access, under strict conditions and with the necessary safeguards, to EU databases containing data on visa and asylum purposes (Visa Information System and Eurodac).

The Commission has also made legislative proposals on two new IT systems. First, an Entry-Exit System (EES) which will modernise and strengthen the Schengen area's external border management and help Member States deal with ever-increasing numbers of travellers coming to the EU. The system will contribute to fighting identity fraud and promote mobility between the Schengen zone and third countries in a secure environment, while also contributing to the fight against terrorism and serious crimes. The EES will register the identities of third-country nationals (alphanumeric data, four fingerprints and facial image) together with details of their travel documents, and will link these to electronic entry and exit records.

Second, the Commission proposed European travel information and authorisation system (ETIAS) to allow for advance assessment of security, irregular migration and public health risks on visa exempt travellers planning to travel to the EU.

Both proposed systems aim at contributing to the security of the European Union and strengthening its external border management. The proposed systems will provide for law enforcement access. Provided the agreement by the co-legislators, both proposed systems are envisaged to be operational by 2020.

[204] Laying down common rules for Member States law enforcement authorities to exchange information and criminal intelligence.

Another set of information tools concerns **data held by private actors**. Such data have become an important source of information for law enforcement authorities, notably for the purpose of investigating crime, as they provide for criminal intelligence about the composition of criminal groups, the means used to commit certain crimes (like air travel to facilitate human trafficking and drugs trafficking, or their communications), the types of crime being committed and other elements of criminal modus operandi. Examples of such data are passenger name record (PNR) data used for the booking of air travel, as well as communications data and financial transaction data.

Information exchange tools and information systems need to comply with **fundamental rights**. An important development in relation to access to data held by private actors was the annulment, by the Court of Justice, of the Data Retention Directive[205] in 2014. The main objective of the Directive[206] was to harmonise Member States' provisions concerning the retention of certain data which are generated or processed by providers of publicly available electronic communications services or of public communications networks. It sought to ensure that the data were available for the purposes of the prevention, investigation, detection and prosecution of serious crime, such as, in particular, organised crime and terrorism. The Court considered that the retention of data for the purpose of allowing the competent national authorities to possibly access those data, as required by the Directive, genuinely satisfied an objective of general interest. However, since the Directive did not lay down clear and precise rules governing the extent of the interference with the fundamental rights enshrined in Articles 7 and 8 of the Charter, the Court concluded that, by adopting the Directive, the EU legislature had exceeded the limits imposed by the requirement of proportionality.

EU agencies (Europol and Eurojust) and bodies (OLAF) play a key role in assisting national law enforcement and judicial authorities in their efforts to prevent and fight crime and fostering cross-border cooperation.

Significant financial resources have been dedicated to research in the area of information exchange, under FP7 and H2020 Security Research Programmes, for a total of approximately EUR 182 million (covering information management; secure communications; information gathering; preparedness, prevention, mitigation and planning; organisational structure and cultures of public users; end users; other coordination; training).

1. Information systems and interoperability

a. Main findings

There are a number of information systems and databases at EU level that provide border guards, police officers and other authorities with relevant information on persons, in accordance with their respective purposes.[207]

However, there are also shortcomings related to information systems that impede the work of national authorities. The main shortcomings are: (a) sub-optimal functionalities of existing

[205] Judgment in Joined Cases C-293/12 and C-594/12 Digital Rights Ireland and Seitlinger and Others.

[206] Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC (OJ 2006 L 105, p. 54).

[207] Schengen Information System (SIS II), European Criminal Records Information System (ECRIS), Interpol database on Stolen and Lost Travel Documents (STLD), Eurodac, Visa Information System. Future systems include the Entry-Exit System (EES), the European Travel Information and. Authorisation System (ETIAS).

information systems, (b) gaps in the EU's architecture of data management, (c) a complex landscape of differently governed information systems, and (d) a fragmented architecture of data management for border control and security. These shortcomings have been confirmed in the evaluation.

To address these shortcomings, the Commission initiated a work process towards the interoperability of information systems. As part of that, the Commission set out an approach on how to achieve the interoperability of information systems for security, border and migration management by 2020 to ensure that border guards, law enforcement officers including customs officials, immigration officials and judicial authorities have the necessary information at their disposal. Work on implementing this approach is on-going.

According to stakeholders, the proposals for a new Entry/Exit System and a new European travel information and authorisation system constitute a stepping stone towards the interoperability of EU information systems.

b. Overview of EU action

The **Schengen Information System (**SIS)[208] is a centralised, large-scale information system supporting checks at the external Schengen borders and reinforcing law enforcement and judicial cooperation within 29 countries throughout Europe. It provides law enforcement with alerts on serious criminals and other people posing a threat to national security, people that should be arrested to face justice in another Member State, and missing persons who crossed a border into another Member State. The system also contains information about stolen motor vehicles, misuse of identity or travel documents, stolen firearms, stolen number plates and other lost or stolen property.

The first generation of the system was set up in 1995 as the major compensatory measure following the abolition of internal border controls, in line with the 1985 Schengen Agreement and the 1990 Schengen Implementing Convention. In the absence of internal border controls, Member States had to address the issues of cross-border crime and irregular migration. SIS allows for the effective and efficient implementation of the mutual recognition measures set out in the Schengen Implementing Convention. However, after the enlargement of the Schengen area, the system's capacity and functionalities needed updating. As a result, the second generation (SIS II) entered into operation on 9 April 2013 and provided Member States with enhanced functionalities and new object categories. In April 2017 the Commission launched an infringement procedure against Ireland for the failure to implement a connection with SIS II.

Since 2013 the Commission has undertaken intensive awareness-raising with Member States. In addition to awareness-raising, the Commission has also made legal and technical improvements and as of 1 February 2015 SIS provides for real-time communication in cases requiring special urgency and attention. As of the same date, SIS clearly displays if an identity document was invalidated by the issuing Member State for travel purposes. SIS alerts also display the "terrorism-related activity" of a person, vehicles and other means of transport.

[208] Council Decision 2007/533/JHA of 12 June 2007 on the establishment, operation and use of the second generation Schengen Information System (SIS II), Regulation (EC) No 1986/2006 of the European Parliament and of the Council of 20 December 2006 on the establishment, operation and use of the second generation Schengen Information System (SIS II).

The Commission presented on 21 December 2016 a report and a staff working document on the outcome of an evaluation of the Schengen Information System[209]. The operational effectiveness of SIS in supporting law enforcement authorities in combating crime and security threats is illustrated by the statistics collected during the Commission's evaluation. Since its entry into operation, queries in SIS have led to:

- Over 37 000 people arrested to face justice in another Member State;
- Over 110 000 people refused entry or stay in the Schengen area;
- Over 20 000 missing persons found having crossed a border into another Member State;
- Over 150 000 people traced to assist with a criminal judicial procedure;
- Over 123 000 travelling serious criminals and other people posing threat to national security located;
- Over 130 000 cases solved concerning stolen motor vehicles, misuse of identity or travel documents, stolen firearms, stolen number plates and other lost or stolen property.

The evidence collected during the evaluation showed that SIS is a tool with which the EU brings significant added value in combating crime and security threats – the scale of the system is such that similar results could not be achieved by action at national level or through bilateral cooperation. It supports European cooperation in the area by facilitating, and thereby increasing, information exchange between law enforcement officials across 30 Member States that use the system.

On 21 December 2016, the Commission adopted three legislative proposals[210], which aim to strengthen the operational effectiveness and efficiency of SIS and extend its functionalities and use. Among other changes, the proposals introduce new provisions regarding the use of biometric data and new types of alerts, such as preventive alerts on children at risk of abduction, alerts on unknown wanted persons, alerts for inquiry checks and alerts on return decisions.

The proposals introduce a number of measures specifically targeting more effective information exchange on terrorist suspects which include the following:

- indication in the alert itself if the person is involved in terrorism related activity;
- mandatory alert creation on persons and object sought by a Member State in relation to a terrorist offence;
- a new action which is the inquiry check allowing a more-in-depth questioning of the person. This measure does not involve temporary detention and physical search of the person or his belongings.

These changes involve technical and operational improvements to the SIS to address issues identified in the Commission's 2016 comprehensive evaluation of the system. They develop and improve the existing system, building on the effective safeguards already in place. As the system continues to process personal data (and it will process further categories of sensitive biometric data), there are potential impacts on individuals' fundamental right to the protection of such data. Hence, additional safeguards have been put in place to limit the collection and further processing of data to what is strictly necessary and operationally required, and granting access to data only to those who have an operational need to process them. Clear

209 COM(2016) 880 final.
210 COM(2016) 883 final; COM(2016) 882 final; COM(2016) 881 final.

data retention timeframes have been set out in the proposals and there is explicit recognition of and provision for individuals' rights to access and rectify data relating to them and to request erasure in line with their fundamental rights. In addition, the proposals set out requirements for an alert to be deleted and introduce a proportionality assessment if an alert is being extended. They also establish extensive and robust safeguards for the use of biometric identifiers to avoid innocent persons being inconvenienced. Lastly, they require the end-to-end security of the system, ensuring greater protection of the data stored in it.[211]

Council Decision 2008/633/JHA of 23 June 2008 provides a legal basis for the consultation of the **Visa Information System** by so-called "designated authorities" of Member States and by Europol for the purposes of the prevention, detection and investigation of terrorist offences and of other serious criminal offences. Regulation 603/2013 of 26 June 2013 provides a legal base for designated authorities of Member States and by Europol for a comparison of fingerprints with the fingerprints of persons registered in the **Eurodac** database for the purposes of the prevention, detection and investigation of terrorist offences and of other serious criminal offences. The 2016 evaluation of the VIS carried out in 2016 found that, in practice, access to the VIS for law enforcement purposes has been limited and fragmented across Member States.

The 2005 Council Common Position on exchanging certain data with INTERPOL[212] obliges Member States to ensure that their competent authorities will exchange data with the **INTERPOL database on Stolen Travel Documents (SLTD)**, in parallel to entering them in the relevant national database and, where applicable, the SIS.

In preamble 7, the Common Position "*obliges Member States to ensure that their competent authorities will exchange* […] their stolen and lost passports] *with the Interpol database on Stolen and Lost Travel Documents,* [...]". Article 3(3) states that "*Each Member State shall ensure immediately after data have been entered in its relevant national database or the SIS* […] *these data are also exchanged with Interpol*.", and article 3(4) that "*Member States shall ensure that their competent law enforcement authorities will query the Interpol database* […] *each time when appropriate for the performance of their task*". Article 6 states that "*Each Member State shall ensure that if a positive identification occurs against the Interpol database its competent authorities shall take action* […]".

The Commission submitted in 2006 a report to the Council on the operation of the Common Position. INTERPOL also presented to the EU in May 2009 and December 2013 two reports describing the state of contributions and use of INTERPOL's SLTD database by EU Member States. In its 2013 report, Interpol outlined that the overall contribution of EU Member States to the SLTD database was excellent, but called on them to use it more for travel documents' checks. The Council recalled in its October 2014 conclusions the obligations for EU Member States as outlined in its Common Position (2005/69/JHA), and called on them, the

[211] Commission Staff Working Document on the Application of the EU Charter of Fundamental Rights in 2016 Accompanying the document Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on 2016 Report on the Application of the EU Charter of Fundamental Rights, SWD(2017) 162 final.

[212] Council Common Position 2005/69/JHA of 24 January 2005 on exchanging certain data with Interpol as regards the obligation to feed and consult the data base on Stolen and Lost Travel Documents.

Commission and Interpol to take a number of actions as regards INTERPOL's SLTD database.[213]

The assessment shows that the calls on Member States to step up the use of the SLTD database of INTERPOL are still relevant, and that progress can and should still be made in that respect.

With the entry into force of the latest revisions of the Schengen Border Code (SBC) in April 2017, the objective of the Common Position as regards the consultation of INTERPOL's SLTD database is mirrored by the revised SBC as a legally binding instrument.

The **European Criminal Records Information System** (ECRIS) contributes to reduce crime by fostering crime prevention and by giving the adequate responses to crimes already committed as regards recidivism. It was established in 2012 on the basis of Council Framework Decision 2009/315/JHA on the exchange between the Member States of information extracted from criminal records and Council Decision 2009/316/JHA on ECRIS. It allows for an electronic, de-centralised information exchange between Member States regarding criminal convictions in the EU for the purpose of criminal proceedings and other purposes. The Commission has adopted on 29 June 2017 a legislative proposal for a Regulation to establish a centralised system supplementing ECRIS with regard to the exchange of information on convicted third country nationals.[214]

Data held by private actors is an increasingly important source of information for law enforcement authorities. Considering that processing passenger data against law enforcement databases and risk-based predetermined criteria can provide valuable and necessary information on persons that might be involved in criminal activities, Directive 2016/681 (the PNR Directive), adopted in April 2016, provides for the transfer by air carriers of passenger name record (PNR) data to the Member States' competent authorities. PNR is also a key part of the cooperation with EU strategic allies against terrorism and serious crime. Agreements were signed with Canada[215], Australia[216] and the United States[217] for the processing and transfer of passenger name record data.

---

213 The Council invited (1) Member States to (i) query Interpol's SLTD database each time when appropriate for the performance of their tasks and will revert to this issue by December 2015, (ii) use more extensively Article 7(2) of the Schengen Borders Code to consult at external borders the relevant databases exclusively on stolen and lost documents, (iii) ensure that data on travel documents that are stolen and lost are exchanged with Interpol.; (2) the Commission to (i) monitor the implementation of the 2005 Common Position, (ii) consider submitting a recommendation to the Council to open negotiations with Interpol to conclude an agreement establishing a connection between SIS II and Interpol's SLTD database so that end users can access both in a single search, (iii) consider, if a review of the Schengen Borders Code is conducted, to amend its Article 7(2) subparagraph 1 to introduce more frequent consultation of relevant databases such as Interpol's SLTD at border crossings; and (3) Interpol to engage with 3rd countries to populate and search SLTD.

214 COM(2017) 344 final (29.6.2017).

215 The EU-Canada PNR Agreement was signed on 25 June 2014 and sent to the European Parliament for consent on 8 July 2014. The European Parliament decided to seek an opinion from the European Court of Justice in order to ascertain whether the agreement envisaged was compatible with EU law guaranteeing the respect for private and family life and the protection of personal data.

216 Agreement between the European Union and Australia on the processing and transfer of European Union-sourced passenger name record (PNR) data by air carriers to the Australian customs service, OJ L 213, 8.8.2008, p. 49–57.

217 Agreement between the European Union and the United States of America on the processing and transfer of Passenger Name Record (PNR) data by air carriers to the United States Department of Homeland Security (DHS) (2007 PNR Agreement), OJ L 204, 4.8.2007, p. 18 and Agreement between the United States of America and the European Union on the use and transfer of passenger name records to the United States Department of Homeland Security, OJ L 215, 11.08.2012, p. 5.

In April 2016, the Commission presented a Communication on ***Stronger and smarter information systems for borders and security***[218], initiating a discussion on how information systems in the European Union can better enhance border management and internal security. The Communication takes stock on the situation of the various information systems for borders and security, highlighting the added-value, but also the challenges raised by the web of systems developed over time in the EU.

In April 2016, the Commission presented a proposal on the establishment of an **Entry/Exit System** (EES). The proposed system will modernise external border management by improving the quality and efficiency of border controls and will use new technologies to cope with the increasing flow of third-country travellers arriving at the external Schengen borders. The system will register entry and exit data of non-EU nationals crossing the EU's external borders and therefore contribute to contribute to enhancing external border management and internal security.

In November 2016, the Commission presented its proposal to set up a **European Travel Information and Authorisation System (ETIAS)**. ETIAS will allow assessing information declared by visa exempt third country nationals in advance of their arrival at the EU external borders (land, air, and sea). The aim of this assessment is to determine whether the presence of visa exempt travellers would pose a security, illegal immigration, or public health risk. The travel authorisation would only constitute an authorisation to travel to the Member States, but not a right of entry, as the decision to let a traveller enter the EU territory would still be taken by a border guard at the border-crossing point.

In June 2016, the Commission set up a **high-level expert group on information systems and interoperability** to address the legal, technical and operational challenges to achieve interoperability. The high-level expert group presented its final report on 11 May 2017[219]. Following this, the seventh report on progress made towards an effective and genuine Security Union[220] welcomed the group's report and recommendations, and proposed the way forward to address structural shortcomings under the three main areas:

- maximising the utility of existing information systems;
- where necessary, developing complementary systems to close information gaps; and
- ensuring interoperability between our systems.

The report sets out a new approach to the management of data, where all centralised EU information systems for security, border and migration management are interoperable in full respect of data protection and other fundamental rights.

The main features of this approach are:

- **European search portal** – allowing the systems to be searched simultaneously, in full compliance with data protection safeguards and possibly with more streamlined rules for access to the systems by law enforcement authorities;

218 COM(2016) 205 final (6.4.2016).

219 The final report and details about the work of the group are available on the Register of Commission expert groups and other similar entities: http://ec.europa.eu/transparency/regexpert/index.cfm?do=groupDetail.groupDetail&groupID=3435.

220 COM(2017) 261, 16 May 2017.

- **Shared biometric matching service** - enabling cross-links across different information systems holding biometric data, possibly with hit/no-hit flags indicating the connection with related biometric data found in another system;
- **Common identity repository** – based on alphanumeric identity data (e.g. dates of birth, passport numbers) and detecting whether a person is registered under multiple identities in different databases.

The proposed approach would overcome the current weakness in the EU's data management architecture eliminating blind spots. The EU agency responsible for information system management, eu-LISA, would play a crucial role in providing technical expertise and bringing the work towards the interoperability of information systems forward.

By 6 May 2019, the Commission needs to review the Prüm Decisions and the Swedish Framework Decision, in order to make, if necessary, proposals to align those instruments with Data Protection Directive (EU) 2016/680 for Police and Criminal Justice Authorities[221].

2. Law enforcement and judicial cooperation: the role of the EU agencies (Europol, CEPOL) and the EU Policy Cycle

a. Main findings

The assessment shows that EU agencies have proven essential in supporting Member States to deliver a more effective response to security challenges.

Europol offers a unique set of tools and serves as an EU hub for criminal information exchange, support centre for Members States' law enforcement operations and a platform for law enforcement experts' exchanges. It has quickly adapted its internal organisation by creating the European Counter-Terrorism Centre, the European Migrants Smuggling Centre, by establishing 24/7 services and by providing for new tools and services to best serve Member States' law enforcement services.

The **EU Policy Cycle on serious and organised crime** is a tool to foster effective cooperation between Member States' law enforcement agencies, EU institutions and EU agencies, aiming at coherent operational actions in Member States to target the key criminal threats facing the EU. The assessment indicates its importance to support intelligence led policing, and a recent study showed that it was successfully implemented during the period 2013-2017. Still, challenges were identifies as regards the need to streamline the Cycle, ensure the commitment and engagement of Member States, strengthen the multi-disciplinary and multi-agency approach, bring together the internal and external dimensions of security and better address cross-priority cooperation. Member States agreed to launch a new Policy Cycle for the period 2018-2021 which takes into account a number of the challenges identified.

EU security policies and instruments can only be successful if the law enforcement authorities and officers on the ground have full knowledge of these and acquire the competencies and skills to apply them. In this context **CEPOL** assists Member States in developing bilateral and regional cooperation via law enforcement training. The agency develops and coordinates the organisation of thematic training. The main challenge for the agency remains the need to focus on priority areas and deliver high quality training in the areas that influence most the

[221] Article 62(6) of the Directive (EU) 2016/680.

security of the EU. As the agency's governing Regulation entered into force only recently, it is too early to assess the impact of this new legal basis.

b. Overview of EU action

Europol

Europol is the EU agency for law enforcement cooperation. Created in 1995 by a Convention between Member States, it became an EU agency in 2010 on the basis of Council Decision 2009/371/JHA. As from 1 May 2017 its activities are regulated by Regulation 2016/794.

The agency supports and strengthens action by the law enforcement authorities of the Member States and their mutual cooperation in preventing and combatting serious crime affecting two or more Member States (including cybercrime), terrorism and forms of crime which affect a common interest covered by a Union policy. Europol has no autonomous investigative or coercive powers. In its activities, it must abide to the data protection rules. Besides further strengthening the agency, the Europol Regulation has introduced mechanisms for the scrutiny of Europol's activities by the European Parliament together with national Parliaments.

Connecting over 650 law enforcement agencies in Europe and beyond, Europol allows for pooling together information on serious cross-border crime and terrorism, providing analytical and operational support for Member States' investigations and operations.

The assessment shows that stakeholders value Europol's support to national law enforcement authorities through the collection, exchange and analysis of criminal information as well as operational assistance. The latter includes, for instance, providing the expertise of analysts in support of cross-border investigations, or by taking part in a Joint Investigation Team.

Europol also plays a significant role in strategic analysis. Its "Serious Organized Crime Threat Assessment" (SOCTA), produced every four years, gives a picture of the emerging threats to Europe in serious and organised crime.[222] The SOCTA is the basis for the Council to establish the EU priorities in the fight against the most serious phenomena of organized crime affecting Europe, becoming a key component of intelligence-led policing in Europe (under the EU Policy Cycle on serious and organised crime). Europol produces also the EU Terrorism Situation and Trend Report (TE-SAT), with a detailed account of the state of terrorism in the EU, and other more specific threat assessments and analytical products.

Europol plays a key role in the implementation of the operational phases of the EU Policy Cycle where it assists Member States in coordinating their joint actions (concrete projects and operations).

Europol's activities are essential for the achievement of all three priorities of the European Agenda on Security and contribute to the successful implementation of the European Agenda on Migration.

The new Europol Regulation[223] makes Europol more effective and efficient. It also ensures the scrutiny by the European Parliament and national Parliaments over Europol's activities. It

[222] https://www.europol.europa.eu/activities-services/main-reports/serious-and-organised-crime-threat-assessment.

[223] Regulation (EU) 2016/794 of the European Parliament and of the Council of 11 May 2016 on the European Union Agency for Law Enforcement Cooperation (Europol) and replacing and repealing Council Decisions 2009/371/JHA, 2009/934/JHA, 2009/935/JHA, 2009/936/JHA and 2009/968/JHA, OJ L 135, 24.5.2016, p. 53–114.

provides for a flexible data management architecture where information could be more easily cross-matched and criminal analyses be made in a more effective way. It also changes the rules on cooperation with external partners by simplifying strategic and technical cooperation, providing for flexible rules on the exchanges of data with the Union bodies, including e.g. CSDP missions, as well as making the Commission responsible for negotiating agreements allowing for operational cooperation with third countries (instead of Europol).

The assessment shows that one challenge will be to make the Europol databases interoperable with other EU databases, where necessary.

Policy Cycle

The **EU Policy Cycle for serious international and organised crime**[224] was adopted in 2010 to ensure an effective cooperation between Member States' law enforcement agencies, EU institutions and EU agencies with the aim to achieve coherent operational actions by national authorities targeting the key criminal threats facing the EU.

The Policy Cycle is based on Europol EU Serious and Organised Crime Threat Assessment (SOCTA), which recommends key crime threats on which the EU should focus. Following discussions with all relevant stakeholders (Member States, the Commission, EU JHA agencies), the Council adopts the EU crime priorities for the duration of the Policy Cycle. Subsequently the Commission, together with experts of relevant EU agencies, institutions and Member States, develops a four-year Multi-Annual Strategic Plan which contains a list of strategic goals to be achieved, implemented by annual Operational Action Plans. The monitoring and assessment of the effectiveness of the Policy Cycle is done by the Council's Standing Committee on operational cooperation on internal security (COSI), based on reports provided by Member States which have taken the lead on one or several crime areas and Europol. It allows to adapt or modify the process during the Cycle. After two years, an interim review allowing for a revision of the MASPs and priorities is foreseen. At the end of an EU Policy Cycle, a thorough evaluation is conducted and lessons learned serve as input for the next EU Policy Cycle.

An evaluation study contracted by the Commission and completed in early 2017 concluded that the EU Policy Cycle 2013-2017 had led to an improvement in the exchange of information, sharing of good practices and the launch of a significant number of joint investigations and operations by Member States. It also contributed to building relations and trust, including with third countries.

At the same time, the evaluation highlighted various challenges:

- need for a lighter and more streamlined EU Policy Cycle, with simplified and more targeted monitoring and reporting procedures which will reduce the administrative burden of those involved in the operational aspects of the Policy Cycle. Improved reporting should also facilitate the political level in its steering of the Policy Cycle process.
- need for a strengthened commitment and engagement of Member States to ensure an active and balanced contribution of all participants to the implementation of agreed

[224] Council conclusions on the creation and implementation of a EU policy cycle for organised and serious international crime, 8 and 9 November 2010.

actions. At national level, Member States should better integrate the EU Policy Cycle actions into their national planning. There is also a need to improve the awareness of the EU Policy Cycle among law enforcement practitioners at national level.

- need for strengthening the multi-disciplinary and multi-agency approach by involving non-law enforcement partners, including other public authorities and the private sector, whenever relevant. This could contribute to a better inclusion of preventive measures. At the same time, the EU Policy Cycle should remain a tool that, first and foremost, delivers operational results.
- need to bring together the internal and external dimensions of security since many of the criminal threats to the EU emanate from or through countries outside the EU. The new SOCTA concludes that around 40% of the suspects involved in serious and organised crime in the EU are non-EU nationals. Therefore, further strengthening of involvement and cooperation with relevant third countries is essential.
- need to better address cross-priority cooperation considering that, as underlined by the EU SOCTA 2017, poly-criminality is on the rise (45% of organised crime groups are involved in more than one criminal activity).

Following the EU SOCTA 2017 on 9 March 2017, the Commission' views on the priorities set out in its sixth progress report towards an effective and genuine Security Union[225], and a discussion between the relevant stakeholders, the Council adopted the new EU crime priorities for the EU Policy Cycle 2018-2021 on 18 May 2017. They include **eight specific** crime priorities: (1) cybercrime, (2) drug production, trafficking and distribution, (3) illegal immigration, (4) organised burglaries and theft (organised property crime), (5) trafficking in human beings, (6) firearms trafficking, (7) Missing Trade Intra Community (MTIC)/Excise fraud and (8) environmental crime, and two cross-cutting crime priorities: (9) document fraud and (10) criminal finance, money laundering and asset recovery.

CEPOL

The **European Union Agency for Law Enforcement Training (CEPOL)** is operational since 1st January 2001 and became an agency in 2005. On 1st July 2016 the CEPOL Regulation (Regulation (EU) 2015/2219) entered into application, replacing and repealing Council Decision 2005/681/JHA.

Since its creation in 2001, CEPOL training courses have aimed at raising awareness of law enforcement officials on existing EU instruments on tackling security challenges and provided knowledge of their use, thus facilitating cross-border cooperation between the Member States and promoting a common law enforcement culture. CEPOL has also developed, implemented and coordinated training in specific criminal or policing thematic areas and training of law enforcement officials in relation to Union missions and law enforcement capacity-building activities in third countries.

Trainings have covered a wide range of topics, ranging from key cross-border cooperation tools and mechanisms to law enforcement techniques and from serious criminal phenomena to leadership. They are carried out by the agency or by a network of national training institutes for law enforcement officials in the Member States, and in close cooperation with other

[225] COM(2017) 213 final.

European agencies (mainly Europol, European Coast and Border Guard, EMCDDA, FRA, EASO) and other EU partners (EEAS, European Security and Defence College and others).

After the Commission highlighted that the EU was lacking a systematic process for identifying and addressing strategic training needs, which are constantly evolving, a Law Enforcement Training Scheme (LETS) was established in March 2013. The objective of the LETS was to present a coordinated policy approach ensuring high quality training of law enforcement officials in all ranks, in order to increase their general and specific knowledge on cross-border policing issues.

The new CEPOL Regulation has widened the training target audience and allowed the agency to offer more targeted and relevant training with an EU dimension, in line with the European Law Enforcement Training Scheme. By conducting multi-annual strategic training needs analysis, CEPOL engages further in external relations cooperation, capacity building in third countries and preparations for Union missions.

Through capacity building CEPOL also contributes indirectly to operational cooperation between third country authorities and their counterparts in the EU. The agency has concluded working arrangements with third countries and international organisations specifying, in particular, the nature, extent and manner in which the authorities and training institutes of third countries, international organisations and private parties concerned may participate in CEPOL's work. CEPOL has also supported Union external missions with training activities focused on law enforcement and judicial cooperation.

3. Other Information Exchange and Police Cooperation instruments

a. Main findings

A number of legal frameworks aim at stepping up cooperation and the exchange of information and criminal intelligence. The most relevant are the **Prüm Decisions** and the so-called **Swedish initiative**. The increased awareness and understanding of the added value of enhanced information exchange among Member States and with EU agencies have contributed to significant progress in the volume and quality of information exchanged. It emerges from the assessment that Member States should make use of these instruments to their full potential.

In its report presented of May 2017, the hi**gh-level expert group on information systems and interoperability** noted a number of transversal issues to be addressed in relation with existing EU information systems and exchange of information. This includes the need to raise the standard of data quality and data use across all systems, the need for criteria to prioritise in order to deal with the huge amount of data, the importance to move away from a silo approach, and the need to keep procedures simple for comparing and transmitting data for law enforcement purposes to ensure that available instruments will be used and their potential fully delivered.

As regards the Prüm Decisions, the report of the high-level expert group emphasised the need for full implementation and application. The Commission pursues its efforts to ensure that all Member States comply with the conditions set up by the Decisions, including by pursuing its structured dialogue with those Member States meeting delays and using its enforcement powers. As for the Swedish Initiative, the Commission services are conducting a study examining in further detail how the instrument is applied.

OLAF, as an independent EU body, investigates or coordinates Member States' investigations into fraud, corruption and other illegal activity affecting negatively the financial interests of the Union as well as serious misconduct within the European Institutions, and, as a service of the Commission, develops anti-fraud policy for the European Commission.

b. Overview of EU action

The Prüm Decisions on the stepping up of cross-border cooperation, particularly in combating terrorism and cross-border crime and the Framework Decision 2006/960/JHA, known as the "Swedish initiative", which lays down common rules for Member States law enforcement authorities to exchange information and criminal intelligence, are the most relevant legal frameworks to facilitate and foster information exchange. The principles of *availability* and *equivalent access* are key notions underlying this legal framework. According to the former, a law enforcement officer in one Member State who needs information in order to perform his duties can obtain this from another Member State; the law enforcement agency in the other Member State holding this information will make it available for the stated purpose, taking into account the requirement of ongoing investigations in the requesting State. The principle of *equivalent access* means that common rules ensure that the conditions applied to requests made by other Member States are not stricter than those applicable at national level. At the same time they foresee that data exchange would take place according to national data protection rules.

Prüm

In 2005, seven Member States signed the Treaty of Prüm to step up cross-border cooperation in relation to countering terrorism, cross-border crime and illegal migration[226]. In 2008, Member States adopted Council Decisions 2008/615/JHA and 2008/616/JHA to incorporate the Treaty provisions into the EU acquis. The Prüm Decisions aim at speeding up the procedures enabling Member States to find out whether any other Member State, and if so which one, has the information sought regarding DNA files, fingerprints and vehicle registration data in the context of an investigation to combat terrorism or cross border crime. Based on a hit/no hit system, the Prüm framework allows comparing anonymous profiles which can lead to requests for further information through mutual assistance procedures, including those adopted pursuant to the Swedish Framework Decision.

Depending on the type of information concerned, 23 Member States are connected to the automated exchange of DNA profiles, 22 Member States to the fingerprint data and 21 Member States – to the vehicle registration data pursuant to the Prüm Decisions[227]. The assessment shows that the framework is highly valued by stakeholders as an investigative tool allowing accelerating the exchange of information and is complementary to other systems. Its importance for operational cooperation was emphasised by a number of stakeholders during the assessment. The establishment of a European network of automated data exchanges has brought concrete benefits, supporting forensic activities and allowing solving criminal, search and identification cases. It has also facilitated the organisation of joint patrols and cross border operations and the provision of assistance during major events.

[226] Austria, Belgium, France, Germany, Luxembourg, the Netherlands and Spain.
[227] See for details, Council document 5081/3/17 rev3, of 17 July 2017.

The Commission has promoted the use of the Prüm framework by supporting its practical implementation and by funding of over EUR 20 million for related projects.

The Prüm Decisions have not yet been fully implemented by all Member States. In 2016 the Commission launched infringements procedures against five Member States for failing to comply with the Prüm Decisions. Delays in the implementation of the Decisions and a lack of consistency in their application have a detrimental effect on the use of the framework, preventing the instrument to deliver its full potential. The need to fully implement and apply the Prüm Decisions without further delay has also been recently underlined by the EU experts in the context of the high-level expert group on interoperability.

The Commission is committed to enhance the implementation of the Prüm framework by all Member States, looking at an increase of the number of connections between Member States with a view to maximise its effectiveness and added value. Based on the high-level expert group's report, the Commission decided to conduct a feasibility study on possible improvements to the Prüm framework, notably in the area of fingerprints.

Swedish Initiative

Following the Council Declaration on combating Terrorism of 25 March 2004 that called for 'exploration of possibilities of greater intelligence sharing on terrorist matters', Sweden presented a legislative initiative to set out common rules for Member States' law enforcement authorities to exchange information and criminal intelligence. The adoption in 2006 of Framework Decision 2006/960/JHA, known as the "Swedish Initiative", was a major step forward in cross-border law information exchange as the essence of the Decision is to provide an "equivalent access" to information detained by a Member State to national and other Member States law enforcement authorities.

Studies on the transposition and implementation of the Decision and feedback from stakeholders in the framework of the assessment have confirmed the practical added value of this instrument, outlining the short delays in the responses received to requests and the few refusals faced. The possibility to create organisational sub-entity (like counter terrorism units) in line with the principles of the Decision allowing for a point to point communication in some operational cases was seen as crucial.

The Commission has continuously supported a more extensive use of the Decision, including by using its infringement powers as necessary[228]. However, more needs to be known on the practical implementation of the Decision by Member States and on how to ensure it delivers its full potential. More information is needed on practical difficulties which may be faced by practitioners, for example when preparing information requests. The Commission has decided therefore to launch a study which will examine further in details how the Decision is applied.

Other instruments

There are other examples of instruments aimed at facilitating operational law enforcement cooperation, in particular Council Decision 2004/919/EC on tackling vehicle crime with cross-border implications and Council Decision 2006/560/JHA on the common use of liaison officers posted abroad by the law enforcement agencies of the Member States.

[228] The Commission launched an infringement procedure in November 2016 against one Member State for failure to communicate national implementing measures in full transposition of this Framework Decision.

The 2004 Council Decision on **tackling vehicle crime with cross-border implications** facilitates procedures for a quick repatriation of vehicles seized, designating a contact point in Member States for tackling cross-border vehicle crime and, whenever a vehicle is reported stolen, entering it in the Schengen Information system (SIS) and, where possible, in INTERPOL's stolen motor vehicle database. The EU network of the Member States contact points, CARPOL, was positively evaluated.

In 2006, Council Decision 2006/560/JHA amended Decision 2003/170/JHA on the **common use of liaison officers posted abroad by the law enforcement agencies** of the Member States.[229] The objective of the 2003 Council Decision was to provide the legal basis under which Member States law enforcement authorities may pool the capacities of their liaison officers in a third country or an international organisation. The 2006 amendments aimed to facilitate Member States use of the Europol liaison officers abroad. The main added value of the legislation is to provide for the possibility that Member States may agree that liaison officers posted abroad by one Member State shall also look after the interests of one or more other Member States. With the growing nexus of internal and external security and the growing financial constraints this is still very important.

4. Eurojust and related judicial cooperation tools

a. Main findings

Eurojust was set up to facilitate coordination and cooperation between national investigative and prosecutorial authorities in dealing with cases affecting various Member States. It has helped to build mutual trust and to bridge the EU's wide variety of legal systems and traditions. By rapidly solving legal problems, and identifying competent authorities in other countries, Eurojust has facilitated the execution of requests for cooperation and mutual recognition instruments. These years have witnessed the continued growth of the organisation into what is now a central player in judicial cooperation in criminal matters.

Eurojust is regularly called upon to undertake more activities, for example in the field of e-evidence, encryption, data retention, and the implementation of the European Arrest Warrant and the European Investigation Order.

While the role of Eurojust has already been reinforced by the 2008 Eurojust Decision, Art. 85 TFEU provides potential for a significant further strengthening of the organisation. This is one of the main aims pursued by the Commission's proposal for a new Regulation laying down the functions of Eurojust presented in 2013 which should increase Eurojust's efficiency and effectiveness with a new governance structure and homogeneous status and powers of National Members, and would ensure that Eurojust can cooperate closely with the European Public Prosecutor's Office once this is established, and provide the European Parliament and national Parliaments a role in the evaluation of Eurojust's activities in line with the Lisbon Treaty.

b. Overview of EU action

Eurojust was established in 2002 to stimulate and improve the coordination of investigations and prosecutions and the cooperation between the competent authorities in the Member States

[229] Council Decision 2006/560/JHA of 24 July 2006 amending Decision 2003/170/JHA on the common use of liaison officers posted abroad by the law enforcement agencies of the Member States.

in relation to serious cross-border crime. It also ensures early consideration of judicial issues such as conflicts of jurisdiction, admissibility of evidence and proper follow-up to freezing and confiscation orders.

Eurojust's specific structure and character have enabled it to play an active role in facilitating prosecutions and building mutual trust in the field of criminal justice cooperation. Its role in judicial cooperation and coordination has over the years proven vital in dismantling organised crime groups (OCGs) and terrorist networks and in confiscating the proceeds of crime. The constant increase of casework since 2002, with 2306 cases in 2016 up from only a few hundred cases in 2002, demonstrated the recognition by the Member States of the added value of Eurojust.

In most of the cases referred to Eurojust, the solution is found through the interaction of the prosecutors working at the Eurojust National desks, which are in contact with their national authorities. Coordination meetings and coordination centres were set up as specific operational tools to speed up and improve judicial cooperation across borders within the EU and beyond. They bring together judicial and law enforcement authorities from the involved Member States – and third States in some cases – to enable real-time transmission of information in cases of serious cross-border crimes among national authorities and coordinated responses during common action days.

Eurojust is increasingly asked to support the setting up and functioning of Joint Investigation Teams (JITs). The Eurojust support to JITs included, since 2009, also their funding in the framework of two grants awarded to Eurojust within the ISEC programme and since July 2013 from Eurojust's own budget. As underlined by stakeholders in the assessment, the availability of EU funding has proven highly valuable in allowing Member States to share information directly without the need for formal requests and enabled them to request investigative measures amongst themselves directly. A constant increase in the applications for JIT funding is noted at Eurojust. Since 2009, Eurojust has provided financial support to 251 JITs. Stakeholders stressed that is important that sufficient funds are secured in the future for the setting up of JITs.

As a centralised, permanent body, Eurojust has been instrumental in fostering a climate of mutual trust, overcoming inherent barriers in cross-border cooperation in criminal matters relating to lack of knowledge of substantive and procedural rules, institutions, formalised and informal practice or reluctance to cooperate by law enforcement authorities.

The role of Eurojust in providing support for speeding up and facilitating the execution of European Arrest Warrants (EAW)[230] is seen as very valuable by stakeholders. This mutual recognition instrument has proven to be a vital EU measure that helps all Member States to bring criminals to justice by improving and simplifying judicial procedures designed to surrender persons for the purpose of conducting a criminal prosecution or executing a custodial sentence or detention order, replacing lengthy extradition procedures within the EU. The traditional extradition procedures used to take on average one year to surrender a person from one state to another. The EAW has had a marked effect in speeding up the procedures, with 15 days on average to have a person surrendered from another Member State in case of the requested person's consent and 54 days if the requested person did not consent. While the

[230] 14% of Eurojust casework in 2016.

EAW covers a broad range of crimes, it operates most efficiently with serious crimes, including terrorism and organised crime, by abolishing the so called double criminality check.

Eurojust has also provided useful support to Member States to coordinate cross-border investigations and prosecutions, and assist them for complex mutual legal assistance requests with countries outside the EU, especially with a number of Cooperation Agreements and the network of Eurojust contact points.

Eurojust has also assisted Member States in addressing the question of which jurisdiction is best placed to prosecute in cross-border cases in which a prosecution might be or has been launched in two or more jurisdictions. To prevent and support the settling of conflicts of jurisdiction that could result in an infringement of the principle of ne bis in idem, and to ensure that the most effective practices with regard to criminal proceedings are in place in the

In 2003 Eurojust published guidelines for deciding which jurisdiction should prosecute. The guidelines suggest factors to be taken into consideration in multi-jurisdictional cases. Since their publication, they have been of assistance to the competent national authorities for determining which jurisdiction is best placed to prosecute in cross-border cases. The guidelines also assist Eurojust, which may advise the competent national authorities on this matter. In addition, since their publication, the Guidelines have been used by some Member States as a reference point when developing their own legislation or guidelines.

In respect of terrorism, the exchange of information with Eurojust on terrorist offences based on Council Decision 2005/671/JHA has brought benefits to all Member States. It allows Member States' competent authorities to be notified immediately by Eurojust if links between cases or criminal networks are detected as a result of Eurojust's cross-checking of the information it receives. It also allows providing Member States' competent authorities regularly with analyses of the judicial responses to terrorism and best practice from Member States through the Terrorism Convictions Monitor. The network of national correspondents for Eurojust for terrorism matters served as a primary point of contact for the response to the 2016 Brussels terrorist attacks. It was activated within an hour of the attacks and facilitated the provision of quick and comprehensive assistance to the Belgian investigation.

In the field of cybercrime, Eurojust also offers operational support to cases and organises coordination meetings and JITs. In addition, it facilitates the sharing of experience and expertise among national practitioners in critical areas such as cooperation with ISPs located in the USA and encryption of data. Since 2016, Eurojust support the European judicial Cybercrime Network (EJCN) created by the Council in June 2016.

Combating organised crime is also a priority for Eurojust, and since 2012, more than 145 Eurojust cases dealt with Italian mafia-type organised criminal groups.

Judicial cooperation work also requires analysing recurrent legal issues and developing best practices. Eurojust has become a centre of legal and judicial expertise on an array of issues such as *ne bis in idem*, controlled deliveries and interception of telecommunications. Eurojust identifies best practice to improve the effectiveness of and speedy responses in the fight against serious cross-border crime. Eurojust operates as a permanent network and works closely with other specialised judicial networks.

Eurojust and Europol maintain close relations. For example, a Eurojust expert on cybercrime was placed at the European Cybercrime Center (EC3), and Eurojust will second a

prosecutor/judge to the European Counter Terrorism Centre (ECTC) and the European Migrant Smuggling Centre (EMCS) at Europol to ensure early judicial follow up.

Eurojust plays an essential role in the external dimension of EU internal security. Eurojust has developed extensive expertise regarding the application of Mutual Legal Assistance agreements with third countries and, in cooperation with the JITs Network secretariat, promote the involvement of third States in JITS. Many operational cases extend beyond the EU, and Eurojust has a specific mandate to facilitate judicial cooperation with third countries. It has so far concluded nine cooperation agreements with third countries (seven of which have entered into force), providing a solid legal basis for the exchange of operational information, including personal data. On the basis of such agreements, Norway, Switzerland and the USA have seconded liaison prosecutors to Eurojust. Eurojust has also established a network of judicial contact points in third countries that facilitates judicial cooperation with 41 countries.

5. Security dimension of borders

a. Main findings

An important set of measures was adopted to manage the EU's external borders and protect the Schengen area without internal borders. These include information systems and frameworks such as the Schengen Information System and Eurosur, and the common rules set by the Schengen Border Code. A major coordinating role is also played at EU level by the European Border and Coast Guard Agency. Given their recent adoption, it is too early to assess the exact extent to which these new measures help to manage migration more effectively, improve the internal security in the EU and safeguard the principle of free movement of persons, while ensuring respect of fundamental rights.

In the related area of **customs**, the creation of databases and IT systems centralised at EU level (including those managed by OLAF, such as notably the Anti-Fraud Information System AFIS) allows Member States' authorities to have direct access to relevant information and to exchange information between each other and the Commission for anti-fraud purposes. This has contributed to supporting and facilitating European co-operation, improving national capabilities and complementing Member States action. OLAF takes an active approach in the realisation of Policy Cycle priorities, notably Missing Trader Intra Community (MTIC) and Excise fraud, and supports the organisation and implementation of Joint Custom Operations (JCO) by Member States. These are organised within the framework of the Excise priority and include supporting the exchange of information between various services.

The assessment suggests that the potential of border checks as means to combat terrorism, fight criminality and manage migration can be further exploited. Better implementation of the rules in place must be a priority. Insufficient implementation can hamper the EU's ability to strengthen its internal security. According to stakeholders, strengthening security through border management also requires a better coordination of the tasks of different players such as customs, border guards and police forces at national level and enhancing coordination at Union level. Further synergies can be achieved through cooperation between Europol and the European Border and Coast Guard Agency, especially when it comes to on-the-spot cooperation. Cooperation has improved considerably over the last months, and according to stakeholders it is expected to be further consolidated.

b. Overview of EU action

The absence of internal borders in the Schengen area and the freedom of movement enjoyed by Union citizens require strong and reliable management of the movement of persons and goods across the external borders. In order to preserve security, law enforcement authorities in the Member States have been granted access to relevant databases on persons. There are information systems and databases in place at EU level that provide border guards, police officers and other authorities with relevant information on persons and documents, in accordance with their respective purposes.

As part of the development of an integrated border management system, developments occurred both internally, through the inclusion of biometric data in passports, establishment of the Visa Information System and the second generation of the Schengen Information System (SIS), and externally, particularly in the field of transatlantic cooperation with initiatives such as the Passenger Name Records (PNR) Agreements or the Visa Waiver programme.

The **Schengen Borders Code** imposes an obligation to check visa holders against the Visa Information System (VIS) in order to verify the identity of the visa holder and the authenticity of the visa. The evaluation of the VIS carried out in 2016 indicated however that on average only one in two visas is checked at borders. The Schengen Borders Code also imposes an obligation to check all travellers and their documents against the Schengen Information System (SIS). The evaluation of SIS, carried out in 2016, however indicated that in some Member States border checks against databases are not consistently carried out, due to deficiencies in procedures, lack of staff or technical failures. This demonstrates that further investments and awareness-raising at national level will be needed, especially taking into account the introduction of systematic checks on all persons against databases since April 2017[231]. Due account was taken of fundamental rights requirements when designing the amendment to the Schengen Borders Code. To minimise the impact on the fundamental rights related to the respect of private and family life (Article 7) and the protection of personal data (Article 8), the databases are consulted on the basis of a hit/no-hit system and the consultation is neither registered nor further processed.

As regards the **Schengen Information System**, its potential to tackle document fraud will grow with the implementation of a 'fingerprint search' functionality. This will enable the successful identification (via their fingerprints) of persons sought by the authorities. The automated fingerprint identification system (AFIS) will perform identity checks and contribute significantly to the detection of document and identity fraud. Member States will be phasing it in from the start of 2018.

These tools coexist with EU instruments already developed in the past at EU level, such as the European Border and Coast Guard Agency, the European Surveillance System (Eurosur)[232],

[231] Regulation (EU) 2017/458 of the European Parliament and of the Council of 15 March 2017 amending Regulation (EU) 2016/399 as regards the reinforcement of checks against relevant databases at external borders. Following its entry into force on 7 April, Member States are obliged, when persons enjoying the right of free movement under Union law cross the external border, to carry out systematic checks against a series of databases in order to verify that the persons do not represent a threat to public order and internal security.

[232] Regulation (EU) 1052/2013 of the European Parliament and of the Council of 22 October 2013 establishing the European Border Surveillance System (Eurosur).

the Schengen evaluation and monitoring mechanism[233] and the Directive on advance passenger information (API)[234].

The European Border and Coast Guard Agency (formerly Frontex) is the main instrument created by the EU to reinforce border management[235]. It started its operations in 2005. Under the previous Frontex Regulation, border control fell into the sole competence of the Member States. The agency's main task at the time was to render border control more effective by coordinating Member States' joint activities and providing surveillance data, technical support and expertise. The agencies' success was confirmed by the successive external evaluations.[236] The Council and the European Parliament have supported its rapid growth in staffing and budget since its launch.

The need for stepping up the management of external borders and in particular the Schengen acquis regarding control on persons crossing the external borders led to the establishment of a new European Border and Coast Guard (EBCG) with Regulation (EU) 2016/1624[237] replacing the former framework. The new Regulation entered into force on 6 October 2016. The European Border and Coast Guard consists of the EBCG Agency and the national border and coast guards of the Member States[238]. Although Member States retain primary responsibility for border management, there is a clear shift towards responsibility shared with the agency. To this end, the agency's staff will grow from 309 in 2015 to 1,000 in 2020. At the same time, a rapid reaction pool of 1,500 European border guards as a standing corps was inscribed in the Regulation. It could be deployed for a rapid border intervention within five days from the adoption of an operational plan. The agency continues to maintain a technical equipment pool composed of equipment owned by either the Member States or by the agency itself. With an increase in budget to more than twice the amount of 2015 (EUR 143.3 million compared to EUR 322 million in 2020), the agency may start acquiring equipment on its own in the future.

A number of other legal instruments complete the EBCG's operational framework. Regulation (EU) No 656/2014[239] establishing rules for the surveillance of the external sea borders set out rules on maritime surveillance and rescue operations coordinated by the agency. These new rules are a response to the current migratory situation and to the need of placing human rights protection at their centre.

---

233 Council Regulation (EU) no. 1053/2013 of 7 October 2013 establishing an evaluation and monitoring mechanism to verify the application of the Schengen acquis and repealing the Decision of the Executive Committee of 16 September 1998 setting up a Standing Committee on the evaluation and implementation of Schengen.

234 Directive on advance passenger information (API) - Council Directive 2004/82/EC of 29 April 2004 on the obligation to communicate passenger data.

235 Council Regulation (EC) No 2007/2004 of 26 October 2004 establishing a European Agency for the Management of Operational Cooperation at the External Borders of the Member States of the European Union, OJ L 349, 25.11.2004, p. 1.

236 The latest report can be found at: http://frontex.europa.eu/assets/Publications/General/Final_Report_on_External_Evaluation_of_Frontex.pdf.

237 Regulation (EU) 2016/1626 of the European Parliament and of the Council of 14 September 2016 amending Council Regulation (EC) No 768/2005 establishing a Community Fisheries Control Agency, OJ L 251, 16.9.2016, p. 80.

238 The term "Member States" in this context means Member States of the EU applying the Schengen acquis regarding the control on persons at the external borders and the Schengen Associated Countries (Iceland, Liechtenstein, Norway and Switzerland).

239 Regulation (EU) No 656/2014 of the European Parliament and of the Council of 15 May 2014 establishing rules for the surveillance of the external sea borders in the context of operational cooperation coordinated by the European Agency for the Management of Operational Cooperation at the External Borders of the Member States of the European Union, OJ L 189, 27.6.2014, p. 93.

Activities of the EBCG are complemented by the **European Border Surveillance System** (EUROSUR), established by Regulation (EU) 1052/2013. The main aim of this system is to establish a common framework for information exchange and cooperation amongst Member States, the European Border and Coast Guard Agency and neighbouring countries in order to strengthen external border controls, in particular at the southern maritime and eastern land borders.

There are important fundamental-rights implications related to the tasks performed by the European Border and Coast Guard Agency, including the use of identification and verification technology in the context of border control. There is a significant body of European Court of Human Rights and Court of Justice case law clarifying the scope and guarantees related to the protection of fundamental rights during border checks, including on the guarantees derived from the right to liberty when a person is held in transit zones (Amuur v. France), the respect of human dignity when performing border checks (Mohamed Zakaria CJEU case 23/12), the access to an effective remedy to challenge the enforcement of removal measures on board the ships (Hirsi Jamaa et al. v. Italy) and application of detailed rules and minimum safeguards on measures that impact privacy (S. And Marper v. UK).

While the initial Frontex founding Regulation did not contain any specific references to fundamental rights, the agency drew up a dedicated strategy and action plan in 2011. At the same time, a consultative forum and a Fundamental Rights Officer were established to give advice on these matters and strengthen mechanisms to ensure fundamental rights compliance. With the new EBCG Regulation, Article 1 now recognises the nexus between an integrated border management and ensuring a high level of internal security within the Union in full respect for fundamental rights, while safeguarding the free movement of persons within it. The European Border and Coast Guard Agency shall guarantee the protection of fundamental rights in the performance of its tasks, and there is a single comprehensive provision spelling out related obligations (Article 34). The new Regulation also introduces a fundamental rights complaints mechanism (Article 72) as demanded by European Parliament, EU Ombudsman and Council of Europe. Any person directly affected by actions of staff during EBCG operations can file a complaint about fundamental rights violations with the fundamental rights officer, further directed on the merits and for appropriate follow-up by the Executive Director or the competent national authority.

Security of identity and travel documents

The strengthening of the security of identity and travel documents was already identified as an important measure for combating terrorism as early as September 2001. In response, the EU has adopted various measures aiming to improve the security of identity documents for both EU citizens and third country nationals in order to prevent identity fraud. With regard to the security of the passports of EU citizens, the Council adopted Regulation (EC) No 2252/2004[240]. It aims to establish higher harmonised security standards for greater protection against falsification and to integrate biometric identifiers in passports and travel documents by laying down minimum security standards of passports and travel documents. On 8 December 2016, the Commission also adopted an Action Plan to strengthen the European response to

[240] Council Regulation (EC) No 2252/2004 of 13 December 2004 on standards for security features and biometrics in passports and travel documents issued by Member States, OJ L 385, 29.12.2004, p. 1.

travel document fraud.[241] The Action Plan aims at improving the overall security of travel documents issued in the EU for identification and border crossing purposes.

As for residence permits delivered to third-country nationals, they are required to conform to the uniform format established by the EU and to include the same biometric features as passports since May 2012[242].

Various measures have also been adopted concerning visas. A uniform format for visas was adopted. It requires the use of biometric identifiers, which are not stored in the visa sticker itself, but in the Visa Information System.

The Commission is currently conducting a study on the feasibility of storing long stay visas and residence document in a EU repository, with the purpose of facilitating the checks at external borders to prevent fraud.

The role of customs

Customs is the lead authority for control of goods at the external border and has the co-ordinating role in that regard. Under the Union Customs Code (UCC), Member States' customs authorities are responsible for the supervision and control of all goods entering, passing through or leaving the EU. Customs supervision applies to all goods whether carried by persons or in commercial supply chains.

Customs carry out controls on the supply chain based on a risk-based approach that is part of a common risk management framework (CRMF). Security based controls aim at tackling a wide spectrum of risks, including financing, related to terrorist and criminal activity embodied in commercial supply chains. These include firearms and ammunition, explosives, drugs and their precursors, CBRN, illicit trafficking in cultural goods and protected species, counterfeit goods, waste, financial fraud and other trafficking.

The CRMF includes EU common risk criteria for real-time analysis of security risks at all EU border posts and a common IT platform, the Customs Risk Management System (CRMS) for customs collaboration on implementing controls, sharing of risk information and control results and customs crisis response.

An **EU Strategy and Action Plan for customs risk management and supply chain security**[243] adopted in 2014 seeks to ensure that customs has the capacities to fulfil its security mission in cooperation with law enforcement and security agencies and is part and parcel of the EU security agenda. Key priorities include improving co-operation between customs and other agencies at national and EU level in order to enhance the effectiveness of supply chain risk management. Another objective is to adapt the cargo information systems used by customs to tackle security risks including the exploitation of cargo and parcel traffic by organised criminal or terrorist groups for trafficking in dangerous goods and supplies or for directly delivering an attack (e.g. explosives) on transport operations.

241 COM/2016/0790 final.

242 Council Regulation (EC) No 1030/2002 of 13 June 2002 laying down a uniform format for residence permits for third-country nationals, OJ L 157, 15.6.2002, p. 1, as amended.

243 COM (2014) 527, 21.8.2014, endorsed by the Council Conclusions on the EU Strategy and Action Plan on customs risk management: tackling risks, strengthening supply chain security and facilitating trade of 4 December 2014 (15383/14).

The 2016 progress report on the implementation of the strategy confirmed that the reform of customs risk management is adapted to today's reality of increased volume and speed of international trade. However, stakeholders underlined that this is a resource-intensive exercise. According to stakeholders, the financing to develop the required IT systems to ensure the availability and sharing of supply chain-data and risk relevant information is a challenge.

The assessment also shows that further synergies and multi-agency cooperation are needed between customs and other law enforcement authorities in the area of organised crime, security and fight against terrorism both at the national and EU level.

Member States' customs co-operation and mutual administrative assistance in customs matters are governed by three main instruments on administrative assistance, notably mutual exchange of information (Regulation 515/1997[244]), mutual assistance and cooperation between customs administrations in order to investigate and prosecute customs infringements ("Naples II" Convention[245]) and the Customs Information System ("CIS Decision"[246]). CIS and the Customs Files Identification Database (FIDE) assist in preventing, investigating and prosecuting serious contraventions of national laws, for example in the areas of **weapons and drug trafficking**, by making information available more rapidly.

Regulation 515/1997 was updated in 2015 and amended by Regulation 2015/1525. Despite the progress brought by this reform, there are still a number of points which could be improved. In particular, some stakeholders considered the legal basis to exchange information with a third country insufficient in the absence of a mutual administrative assistance agreement between the EU and this country.

Responding to the need of Member States' customs authorities to co-operate with each other in order to successfully tackle customs fraud and transnational trafficking, and to prosecute and punish the offenders, the Naples II Convention is used by Member States in order to exchange information: (a) with a view to prosecuting and punishing infringements of EU and national customs laws, and (b) for mutual administrative assistance purposes with regard to national customs law. To this end, it is fully complementary to Regulation 515/97 which covers mutual administrative assistance with regard to EU customs law. However, according to stakeholders, the Naples II Convention may need to be updated in order to take account of the development of fraud methods and adapt to Member States needs for the exchange of information.

244 Regulation 515/97 of 13 March 1997 (lastly revised by Regulation 1525/2015 of 9 September 2015 on mutual assistance between the administrative authorities of the Member States and co-operation between those authorities and the Commission to ensure the correct application of the law on customs (and agricultural) matters.

245 Council Act of 18 December 1997 drawing up the Convention on mutual assistance and cooperation between customs administrations (also called 'Naples II' Convention).

246 Council Decision 2009/917/JHA of 30 November 2009 on the use of information technology for customs purposes (based on Art. 30(1)(a) and Art. 34(2)(c) TEU, currently Art. 87 of the TFEU).