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).

EUROPEAN
COMMISSION

Brussels, 26.7.2017
SWD(2017) 278 final

PART 2/2

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
Annexes

Contents

I. Methodology

In order to be comprehensive the Commission services have taken into consideration all key policy instruments for each of the three priority areas of the European Agenda on Security which have been adopted in the last 15 years. This included the main strategic documents, regulatory and funding instruments, as well as research programmes. Overall, the Commission services have covered around a hundred relevant acts.

The Commission services have applied a three stages analysis. Inputs received from those directly involved in the implementation of EU instruments, at EU and national levels, have been taken into account in the comprehensive assessment and in the thematic fiches on the main instruments relevant to the assessment (replies to the questionnaire, workshops and hearings).

In addition to a general overview of the instruments developed at EU level under the key pillars of the European Agenda on Security, their general achievements and the support provided at EU level, notably through funding programmes, the assessment went more in detail as regards a number of specific instruments. The key questions underlying this analysis related to the relevance of the instruments, and how and to what extent they have led to achievements as well as good practices which could be further supported. The analysis also aimed at identifying possible weaknesses met by the EU instruments in achieving their objectives, related for example to unnecessary burden, overlaps, gaps and other failures.

On that basis, main findings are presented, responding to the questions whether the acquis and supporting activities have achieved results and are still relevant in today's reality and whether there are needs and gaps which would call for reviewing existing policies and legislation or new policy initiatives.

To provide more details to support the conclusions, the Commission services have prepared fiches annexed to the overall assessment (see Annex 2 to 5) relying on the evidence collected through monitoring and – when available – existing reviews and evaluations.

In these fiches, and taking into consideration the objectives of the policy measures at the moment of their adoption and how they were expected to achieve their objectives, the Commission services have addressed the following questions:

1. To what extent are objectives and instruments still adapted to current needs?

To address this question, the Commission services have considered, as relevant, the evolution of the needs in the policy area related to the measure and assessed the extent to which the existing instrument meet the current needs.

2. To what extent have EU measures offered added value?

To address this question, the Commission services have assessed the effects brought in by the EU measure and if and to what extent EU action has been necessary to complement/stimulate/leverage action at national level. The EU added value to be identified was linked to the different ways of supporting the EU has provided (including through funding), taking into consideration the coherence of this action with other programmes/initiatives.

3. To what extent have fundamental rights been safeguarded by EU measures?

To address this question, the Commission services have referred to the provisions in the measure which relate to the protection of fundamental rights and aimed at assessing the proportionality of the EU measure adopted when a fundamental right was at stake.

4. To what extent has the external dimension of internal security been incorporated in EU security policies?

To address this question, the Commission services have taken into consideration the external dimension of the policy area covered by the measure and whether the measure had external relations objectives, and if so, whether these objectives have been achieved.

As detailed below, the approach followed by the Commission service has been inclusive. The mainly qualitative assessment made by the Commission services relies on existing data regarding the implementation and application of the EU instruments and the outcome of the work done in the context of recent evaluations and reviews of legislative and policy instruments. It is also based on the assessment and inputs from the full spectrum of stakeholders: Member States authorities and experts, representatives of the European and National Parliaments, EU Agencies, representatives of civil society and think tanks, researchers and industry representatives.

The workshops hosted by the Commission, Europol and the EU Counter-Terrorism Coordinator as well as the hearing organised by the European Parliament allowed for an extensive exchange of views on the EU internal security policy and thematic issues related to terrorism, organised crime and cybercrime.

Member States were consulted with a questionnaire[1] to collect their views, data and evidence on the effects and added value of EU instruments as well as their assessment of existing shortcomings and priority actions at EU level in the short to medium term.[2] Additional inputs were provided by Member States experts at a workshop to assess EU Counterterrorism Policies hosted by the EU Counter Terrorism Coordinator on 10 April 2017 in Brussels and a joint Commission-Europol workshop (with a focus on organised crime, in particular asset recovery, firearms and cybercrime) held on 19 April 2017.

The **European Parliament Committee on Civil Liberties, Justice and Home Affairs** (LIBE) organised a hearing with representatives of national Parliaments and civil society on 11 May 2017 in Brussels. Members of national Parliaments from 14 EU Member States and Norway participated, together with Members of the European Parliament. Written contributions were also received from the Italian and the Croatian Parliament.

EU Agencies contributed to the process by responding to the questionnaire sent to the Member States and participating to some of the consultation events, in particular those with Member States and with think tanks and academics and researchers.[3]

Representatives from **civil society** and **think tanks** were associated to the exercise. Civil society organisations (Amnesty International, International Commission of Jurists and EuroCop) participated to the exchange of views organised by LIBE on 11 May 2017 in Brussels.

Representatives of think tanks working in the field of security provided input in the framework of a high-level seminar on the state of play and future perspectives of the Security Union, organised by the Commission European Political Strategy Centre (EPSC) on 3 April 2017 in Brussels.

Input was also provided by a seminar organised by a Brussels-based think tank, CEPS, on 12 May 2017, with a number of scholars having played a key role in EU and nationally-funded social sciences and humanities research projects covering themes of direct relevance to the Security Union. Participants discussed challenges and gaps in the existing EU security policy instruments in relation to the use of information systems and EU databases, cross-border criminal and judicial investigations and international cooperation, and paid a particular attention to effectiveness, proportionality, fundamental rights and societal implications.

[1] See Annex VII - Questionnaires to Member States and EU Agencies.
[2] For a summary of Member States and Agencies replies to the questionnaires, see Annex VII.
[3] The following EU agencies have been consulted: CEPOL, EMCDDA, eu-LISA, Eurojust, Europol, FRA and the European Border and Coast Guard Agency.

Discussions with **industry representatives** on security research activities and EU industrial policy took place in the framework of a High-Level Event on European Security hosted by the European Organisation for Security (EOS) on 15 May 2017 in Brussels[4].

The subsequent annexes contain the thematic fiches on the main instruments relevant to the assessment, a summary of the various workshops held during this process as well as a summary of the feedback received from Member States and EU Agencies to the Commission's questionnaire.

The assessment, and the annexes, covers policy developments until 1st of July 2017.

[4] 28 representatives from different companies - members of EOS, participated in the event.

II. Counter-terrorism

1. Counter-Terrorism Strategy and Horizontal Instruments

Combating terrorism by criminal law (Framework Decision 2002/475/JHA, last amended by 2008/919/JHA and Directive 2017/541/EU)

1. Legal framework

Council Framework Decision 2002/475/JHA of 13 June 2002 on combating terrorism (OJ L 164, 22.6.2002, p. 3), amended by Framework Decision 2008/919/JHA of 28 November 2008

Directive 2017/541/EU of the European Parliament and 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 88/6, 31.03.2017)

2. Analysis

The objectives are:

- Criminalising terrorism and offences related to terrorism, such as its financing and travelling for terrorist purposes throughout the EU
- Facilitating international cooperation and the exchange of information on terrorist offences
- Improving the position of victims of terrorism by responding to their specific needs
- Setting up of national measures to ensure that terrorist online content is taken down

Framework Decision 2002/475/JHA criminalised certain terrorist acts, including in particular the commission of terrorist attacks, participation in the activities of a terrorist group, public provocation, recruitment and training to terrorism. However, it needed to be reviewed to implement new international standards and obligations taken by the EU and to tackle the evolving terrorist threat in a more effective way, thereby enhancing the security of the EU and the safety of its citizens.

Directive 2017/541/EU also provides for specific provisions on victims of terrorism. It builds on the existing general EU rules on victims, mainly Directive 2012/29/EU Directive 2017/541/EU also provides for specific provisions on victims of terrorism. It builds on the existing general EU rules on victims, mainly lays down a set of binding rights for all victims of crime without however providing for any specific measures for victims of terrorism.

The Commission therefore made a proposal on 2 December 2015 to strengthen Framework Decision 2002/475/JHA by extending the crimes related to terrorism and to include measures that respond more precisely to the needs of victims of terrorism. The co-legislator adopted the Directive on 15 March 2017.

The Directive strengthens the obligation to exchange information on terrorism between Member States under Decision 2005/671/EC, and sets up an obligation for Member States to take down terrorist content online.

EU-wide definitions of terrorist and terrorist-related offences avoid any legal gaps that may result from a fragmented approach and are 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 transposition of the relevant provisions into national law of Framework Decision 2002/475/JHA has been the subject of several implementation reports,[5] including the report of September 2014 on the implementation of the amendments introduced by Framework Decision 2008/919/JHA.[6]

The 2014 implementation report was supported by an external study carrying out an evaluation of the legal framework adopted by the EU Member States to combat terrorism in practice. The study concluded that the changes introduced in 2008 were seen as useful in helping to combat the changing nature of the terrorist threats faced by EU Member States. The added value of the Framework Decision was considered as high for EU Member States that did not already have a legal framework specifically 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.

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

Member States are bound to respect the rights enshrined in the Charter when they implement EU legislation. Therefore, Member States will have to respect the Charter when they implement the Framework Decision 2002/475/JHA and the more recent Directive 2017/541/EU. The Commission uses all tools available, including infringement proceedings when necessary, to ensure compliance with the EU Charter of Fundamental Rights. The abovementioned report on the added value of Directive 2017/541/EU will also cover the impact of that Directive on fundamental rights and freedoms, including on non-discrimination and on the rule of law.

The respect of fundamental rights in general and the principle of proportionality is respected in limiting the scope of the offences to what is necessary to allow for the effective prosecution of acts that pose a particular threat to security. Framework Decision 2002/475/JHA and Directive 2017/541/EU for instance make clear that the expression of radical, polemic or controversial views in the public debate on sensitive political questions should not be considered as terrorism.

The Directive does not provide for specific rules in relation to third countries. However, minimum rules on criminal offences in line with the UNSCR 2178(2014) and the Additional Protocol facilitate cooperation with third countries providing a common benchmark both within the EU and with international partners.

Information sharing mechanism on changes in the national threat level

1. Legal framework

European Commission, *The EU Internal Security Strategy in Action: Five steps towards a more secure Europe*, COM(2010) 673 final, 22 November 2010.[7]

[5] Reports from the Commission based on Article 11 of the Council Framework Decision of 13 June 2002 on combating terrorism: COM(2004)409 final of 8 June 2004 and COM(2007) 681 final of 6 November 2007.
[6] COM(2014) 554 final 05.09.2014.
[7] http://register.consilium.europa.eu/doc/srv?l=EN&f=ST%2016797%202010%20INIT.

Council of the European Union, *Council conclusions on the information sharing mechanism on changes in the national threat level*, 3051st Justice and Home Affairs Council meeting, 2 and 3 December 2010.[8]

2. Analysis

The objectives are

- Improve the mutual understanding of the various definitions of threat levels;
- Improve the communication among Member States and with EU institutions when threat levels are subject to change.

While the terrorism threat is shared across the EU, there are differences in the threat level faced by the different Member States.

A majority of Member States have developed national threat alert systems to inform the public but this information is not always easily accessible (including for linguistic reasons).

In the event of a major terrorist attack or significant increase of the threat, other Member States need to be informed of the evolution of the threat (imminence of an attack) as well as the security measures adopted to respond to the threat. In the aftermath of the recent attacks in Europe (e.g. after the Paris and Brussels attacks in 2015 and 2016), citizens and Member States' authorities expressed the need to be informed of the changes in threat level and their impacts (e.g. reinforced controls at border crossing points, major transport hubs, deployment of military patrols, etc.).

The mechanism promotes the sharing of information, not only on the threat level, but also on the reasons for the change in the threat level. It relies on the 24/7 capability and secure communications of the EU Intelligence and Situation Centre.

It has been used several times since 2010 (most recently UK, ES, NL and LT) to ensure that all Member States are aware of changes and the underlying decisions.

Since 2010, several Member States have developed new system. Yet some Member States still see no value in defining a threat level system which is too rigid[9] and does not take into account regional differences.[10] There is still no common understanding or definitions of threat levels in Member States.

The 2010 Council Conclusions providing only for the exchange of information at strategic level of the threat levels set by Member States, there is not particular international dimension in this instrument.

Considering that the mechanism is at strategic level, it does not impact on individual fundamental rights.

Among possible avenues for improving the status quo, the following have been raised:

- The *IPCR Web Platform*[11] could host a common repository of information on threat levels in EU Member States (available to Member States and EU institutions) but the project discussed in the framework of the Friends of Presidency IPCR/SCI was never tested or implemented.

[8] https://www.consilium.europa.eu/uedocs/cms_data/docs/pressdata/en/jha/118175.pdf.
[9] http://yle.fi/uutiset/osasto/news/supo_no_need_for_new_security_threat_ranking/8459389. Supo: No need for new security threat ranking, 16 November 2015
[10] http://www.bmi.bund.de/SharedDocs/FAQs/DE/Themen/Sicherheit/Islamismus/05.html.
[11] https://ipcr.consilium.europa.eu/.

- The *Overview of natural and man-made disaster risks in the EU* (SWD(2014)0134)[12] prepared by the European Commission with inputs from Member States at the request of the Council could include an overview of threat levels.
- A regular review of Member States' threat level could contribute to the assessment of the threats faced by the EU foreseen by the *Solidarity Clause* (art. 222 TFEU) and its implementing decision.[13]

2. Prevent

EU PREVENT Policies

1. Legal framework

In line with **Article 3 (2) TEU**, the Union shall offer its citizens an area of freedom, security and justice with **appropriate measures in place to prevent and combat crime** (including radicalisation leading to acts of terrorism or violent extremism). The design and implementation of measures countering radicalisation falls primarily within the **competence of the Member States** and takes place mainly at local but also regional or national level.

EU prevent policies find their origin in the 2005 EU Counter Terrorism Strategy[14]. They were further refined in the EU Strategy on radicalisation and recruitment (as revised in 2014) as well as in the Internal Security Strategy 2010-2014 followed by the Commission European Agenda on Security, which is a building block of the renewed EU Internal Security Strategy adopted by the Council in June 2015. These policy documents set out the general approach to prevention of radicalisation with an increasing focus on the inclusion of all relevant policy areas (including inter alia education, social inclusion, etc.).

More targeted interventions tackling radicalisation leading to terrorism and violent extremism have been identified by the Commission in several Communications on the prevention of radicalisation (of 2014 and 2016) as well as by Council Conclusions on specific aspects (such as criminal justice response to radicalisation of November 2015 or Council Conclusions of June 2016 focussing on the role of the youth sector in an integrated and cross-sectoral approach to preventing and combating violent radicalisation of young people).[15] These policy documents are complemented by reports and recommendations from other institutional players such as Reports from the European Parliament, Opinions from the Committee of the Regions, reports from the EU Counter-Terrorism Coordinator.

The main purpose of the EU policy on radicalisation is to **support the variety of stakeholders in Member States to effectively prevent and counter radicalisation.**

EU policy documents and instruments support and facilitate cooperation, networking, and exchange of good practices at EU level with a view to enhancing the stakeholders' capabilities in tackling the phenomenon. Supporting actions at EU level provide added value not only

[12] http://eur-lex.europa.eu/legal-content/en/ALL/?uri=CELEX:52014SC0134.
[13] http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32014D0415.
[14] http://register.consilium.europa.eu/doc/srv?l=EN&f=ST%2014469%202005%20REV%204.
[15] EU Strategy for Combating Radicalisation and Recruitment to Terrorism (14781/1/05); Council Conclusions calling for an update of the EU Strategy for Combating Radicalisation and Recruitment to Terrorism (9447/13); Revised EU Strategy for Combating Radicalisation and Recruitment to Terrorism, adopted by the Justice and Home Affairs Council at its meeting on 19 May 2014 and approved by the Council at its meeting of 5 and 6 June 2014 (9956/14); Commission communication of 15 January 2014 entitled 'Preventing radicalisation to terrorism and violent extremism: Strengthening the EU's Response' (COM(2013)0941); Conclusions of the Council of the European Union and of the Member States meeting within the Council on enhancing the criminal justice response to radicalisation leading to terrorism and violent extremism (14382/15); Commission Communication supporting the prevention of radicalisation leading to violent extremism COM(2016) 379 final Council Conclusions on the role of the youth sector in an integrated and cross-sectoral approach to preventing and combating violent radicalisation of young people (9640/16); Council Conclusions on the prevention of radicalisation leading to violent extremism (2016/C 467/02).

because of the similar nature of the challenges faced by Member States but also because of the scale, complexity and interconnected nature of the problem.

The efforts are targeted on three key areas:

- support **front-line practitioners** through exchange of experiences and best practices equipping them with the necessary skills to prevent and counter radicalisation in their daily work (for example in the RAN, Radicalisation Awareness Network);
- support prevent **policy makers** in developing appropriate framework conditions for cooperation among and support to the relevant stakeholders, (Network of Prevent Policy Makers, RAN, European Strategic Communications Network);
- support Member States in tapping the potential of formal and non-formal learning in preventing radicalisation leading to violent extremism by promoting social cohesion and ownership of shared values;
- engage with the **private sector** in tackling terrorists' use of the internet with a view to enhancing the swift removal of terrorist content as well as promoting alternative and counter narratives (EU Internet Forum incl. cooperation with the EU Internet Referral Unit in Europol and the Civil Society Empowerment Programme).

2. Analysis

The most recent manifestations of radicalisation, its accelerating pace and scale, as well as the use of new communication tools present new challenges that call for **immediate action and the use of existing (and where appropriate new) instruments to respond effectively to new needs and tackle effectively the root causes of radicalisation**. Prevention of radicalisation and violent extremism is being tackled through so-called "soft" measures. This **non-legislative approach** lacking legally binding monitoring mechanisms may raise issues of full implementation on behalf of Member States. However, it allows for an **overall broader approach** to radicalisation including a number of policy areas such as education or social inclusion. It is also **more flexible and easier to adapt** to new developments considering that this phenomenon is constantly evolving. Finally, full and effective application of preventive measures seems to be achieved most effectively through **cooperative, trust and capacity building measures**.

The problem of radicalisation is multidimensional and complex, and there is an ever increasing need to develop effective evidence-based prevent measures. This in turn requires timely and targeted research in the various areas. The research programmes in place (e.g. H2020) look at complementary aspects of the radicalisation phenomenon. While the different ongoing EU initiatives (such as e.g. the Radicalisation Awareness Network) feed into the identification of priority research areas, incorporating research findings into the development of prevent action (both as regards policy and concrete interventions) in a timely manner remains a challenge. In that spirit, a number of EU initiatives have been complemented by research capabilities (e.g. under the EU Internet Forum, Voxpol is tasked to provide relevant research findings, the EU Internet Referral Unit has its own advisory research body, the RAN established an editorial board with researchers from different areas providing input for the work in the 9 RAN working groups, and the European Strategic Communications Network (ESCN) is developing complementary research activities). There is scope for further streamlining research activities. The creation of an overview or database of EU funded programmes and projects could be a first step in that direction. It should serve as a starting point for a more systematic exchange on findings and lessons learned.

At the same time, there is an increased need to evaluate the results and effectiveness of prevent policies and interventions.

There is a **wide convergence and consensus in the approach and priorities** for prevent work across all EU institutions and Member States. However, the approaches, priorities and available instruments, measures and initiatives are contained in a multitude of documents with

no one single strategy serving as a common reference document to streamline and steer actions at EU level and which could allow for monitoring and evaluation of effectiveness of implementation of prevent measures jointly with Member States.

The different policy initiatives and measures, such as the **creation of EU wide networks or platforms (such as the RAN, ESCN or the EU Internet Forum) facilitate cooperation** between the relevant stakeholders across the EU, including first line practitioners, civil society organisations, law enforcement and government officials. The ESCN evolved from the Syria Strategic Communications Advisory Team, increased its outreach and became a collaborative network of 26 Member States which shares analysis, good practice and ideas on the use of strategic communications in countering violent extremism. It develops and deepens a common understanding of the terrorist communications challenge and has recently launched a research and analysis strand in which Member States work even closer on most burning strategic communications challenges.

Measures and initiatives such as the ESCN or the RAN also support the relevant stakeholders in Member States in the **development of national capabilities**: the RAN helps developing the skills of first line practitioners in responding to signs of radicalisation, advises policy makers on the necessary framework conditions for effective prevent work and offers concrete counselling and support to Member States for instance through workshops and trainings. The ESCN helps in developing strategic communication capabilities in Member States like specialised research or communication units. The newly created Network of Prevent Policy Makers facilitates strategic exchanges and lessons learned among policy makers and strengthens the link between the latter and the RAN community. The Civil Society Empowerment Programme (CSEP) aims at empowering European civil society organisations to increase the volume of effective narratives online which counter and challenge that of the terrorist narrative, and provide positive alternatives. Furthermore, these initiatives **encourage Member States to take corresponding actions at national level**. For instance, discussions in the EU Internet Forum encourage Member States to take measures to reduce the accessibility to terrorist and radicalising material online (in addition to the work of the EU IRU in Europol). The ESCN supports Member States in the creation of national strategic communication campaigns.

To support Member States in their action to fight radicalisation, the EU also **funds** initiatives with focus on priority policy areas:

- **Internal Security Fund - Police** supporting actions addressing internal security challenges such as preventing terrorism and addressing radicalisation and recruitment;
- **Erasmus+** not only to foster core European values, but also to fund valuable anti-radicalisation projects in the education field,
- **Justice Programme** funding training programmes for prison and probation staff as well as judges and prosecutors, to provide them with the necessary knowledge and skills to deal with radicalised people, and make available risk assessment tools and methodologies for determining the level of threat posed by suspects of terrorist crimes.
- **ESF**, where the focus is, inter alia, on the re-integration of de-radicalised people;
- **Horizon 2020** funding research on radicalisation.

Managing the different funds and aligning existing instruments in a number of policy areas to the new needs being done by different services within the Commission, the establishment of the Security Union Task Force supporting the work of Commissioner King, is facilitating coordination, coherence and the creation of synergies within the Task Force subgroup on radicalisation.

On the other hand, there is a clear need for concrete guidance and tailored trainings of the relevant stakeholders. As handbooks, toolkits etc as well as trainings are increasingly being developed by the different stakeholders (including the EU), mapping and rolling out the most relevant trainings is needed.

Support to the policy implementation in the field of radicalisation has also been provided by the security research programme and the Social Sciences and Humanities programme managed by the European Commission, in both Framework Programme 7[16] and Societal Challenge 6 (Inclusive, Innovative and Reflective societies)[17] and Societal Challenge 7 (Secure Societies) in Horizon 2020[18].[19] Specifically, the projects SAFIRE, PRIME, VOX-POL, IMPACT-EUROPE, RELIGARE, EURISLAM, ReligioWest, EuroPublicislam and MYPLACE have provided scientific tools and policy suggestions directly usable by law enforcement agencies and security policy makers, including by the experts of the RAN.

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.

All EU prevent-related activities are based on the **respect for fundamental rights**. The actions presented in the key policy documents reflect the EU's commitment to ensure security and respect of fundamental rights and freedoms of EU citizens, as enshrined in the EU Charter on Fundamental Rights, including freedom of expression and information, assembly and association, and respect for linguistic, cultural and religious diversity.

Prevent policies at EU Level are deeply rooted in common EU values including those of an inclusive society and a participatory democracy, fighting social exclusion and discrimination. The objectives of promoting inclusive education and EU common values and an inclusive, open and resilient society as well as reaching out to young people were highlighted in the Communication on radicalisation of June 2016. The "Paris Declaration"[20] on promoting citizenship and the common values of freedom, tolerance and non-discrimination through education (March 2015) identifies key areas for cooperation at EU level, as well as objectives to be pursued at national, regional and local level. In this context, the Commission has launched a series of measures in order to reach out to young people, especially the disadvantaged, and help them become engaged citizens, avoiding marginalisation and vulnerability to extremist views(e.g. virtual youth exchanges; toolkit for youth workers to work with young people at risk of radicalisation; a role models initiative under Erasmus+; mobilising eTwinning to foster exchanges among schools and teachers; reinforcing the European Voluntary Service or RAN Young. An ET 2020 Working Group on Promoting citizenship and the common values of freedom, tolerance and non-discrimination through education[21] is working on a policy framework for promoting social inclusion and shared values through education. Moreover, the Erasmus+ programme has devoted more than 200M euros in 2016 to support transnational cooperation projects covering the scope of the Paris Declaration. Given the long-term impact of actions in the field of education, it is important to keep up these efforts and reinforce further support to Member States in implementing education policies that promote social inclusion and shared values in order to trigger systemic change.

A more institutionalised, systematic or regular exchange with civil society organisations, think tanks or other EU agencies (such as the Fundamental Rights Agency) on the implications of prevent policies on fundamental rights could be envisaged.

---

[16] See: https://ec.europa.eu/research/fp7/index_en.cfm?pg=security.
[17] See http://ec.europa.eu/research/social-sciences/index.cfm
[18] See: https://ec.europa.eu/programmes/horizon2020/en/h2020-section/secure-societies-%E2%80%93-protecting-freedom-and-security-europe-and-its-citizens.
[19] The full list of security research projects can be found here: https://ec.europa.eu/home-affairs/financing/fundings/research-for-security_en.
[20] http://ec.europa.eu/dgs/education_culture/repository/education/news/2015/documents/citizenship-education-declaration_en.pdf.
[21] http://ec.europa.eu/education/policy/strategic-framework/expert-groups/citizenship-common-values_en

On the external dimension, the EU has been supporting capacity building efforts in third countries, inter alia, to tackle the root causes of radicalisation and support the establishment of sustainable structures for cooperation with the relevant stakeholders, including where feasible with local civil society actors. To that end, there is cooperation with third countries and international organisations and the EU provides financial support to a number of initiatives and projects, including in particular the Instrument contributing to Stability and Peace (IcSP) and the European Neighbourhood Instrument (ENI). At the same time, a number of instruments and networks are extended to benefit third countries (such as the eTwinning network or Erasmus+). The financial resources spent on CVE-specific actions increased from EUR 34 million in 2015 to EUR 400 million in 2016.

However, other initiatives and networks such as the RAN have a clear focus on the EU and have a relatively limited budget for external engagement. There is further scope for stronger links and coordination of the internal and external actions on prevention of radicalisation and the activation of financial resources from different EU programmes. External engagement needs to increasingly focus on countries and regions most relevant from an internal security perspective. Further engagement would presuppose a needs assessment, focus on sustainability and should be implemented in close coordination with Member States and international partners.

Overall, the acquis and **supporting instruments** (funding, training, networking…) are considered to be largely **satisfactory** but may need an additional effort as regards implementation and streamlining:

- Engagement with Member State can be enhanced to support the implementation of prevent actions at national level;
- Funding programmes and opportunities at EU and national level could be better targeted and coordinated towards priority areas;
- Research results should be synthetized and inform in a more timely and targeted manner both policy decisions and operational interventions;
- Links between the different initiatives and networks addressing each a distinct category of stakeholders should be further strengthened;
- There is an opportunity to collect and support the further development and dissemination of the most relevant trainings at EU level;
- More systematic evaluations of prevent interventions should be supported.

On the other hand, new avenues could be further explored, including:

- Establishing a single strategy (e.g. document reflecting a "European consensus") to streamline and steer actions at EU and Member States level providing the basis for monitoring and evaluating of the implementation of prevent measures in Member States.
- Setting up a High Level Expert Group on Radicalisation (HLEG-R) to advise the Commission on options for a more permanent structure for collaboration and coordination of prevent work and the further development of EU prevent policies.
- Considering follow up initiatives by the Commission to take into account recommendations and opinions issued by the HLEG-R.

The Radicalisation Awareness Network Centre of Excellence

1. Legal framework

In its Communication on "Preventing Radicalisation to Terrorism and Violent Extremism: Strengthening the EU's Response" adopted on 15 January 2014, and later in the European Agenda on Security of April 2015, the Commission announced the establishment of a "Centre of Excellence" acting as an EU knowledge hub.

The Radicalisation Awareness Network Centre of Excellence (RAN CoE) is funded under the Internal Security Fund – Police.22 The contract for managing the RAN CoE was awarded to RADAR following an open tender. The framework contract foresees a maximum duration of 4 years with a maximum budget of 25.000.000 EUR starting on 1 October 2015. Activities for each calendar year are laid down in a specific contract based on an annual activity plan.

The Commission steers the work of the RAN CoE while involving practitioners in the decision making process in particular through the RAN CoE Steering Committee which meets on a quarterly basis, allowing the Commission to redirect where necessary and appropriate the focus of activities in line with practitioners' needs and changing priorities.

2. Analysis

The RAN CoE has been identified as the main policy tool in countering and preventing radicalisation. It pursues three main objectives:

- to **facilitate and enhance the exchange of experiences and cooperation** between the relevant stakeholders (inside and outside the EU), in particular through the RAN;
- to **support the EU and the relevant stakeholders in Member States** (under certain conditions also stakeholders from **third countries**) in their prevent efforts through different support services, practical tools and policy recommendations;
- to **consolidate, disseminate and share expertise, best practices and targeted research** in the field of preventing radicalisation.

The RAN CoE is mandated to **raise awareness among practitioners and equip them with the necessary skills to recognise signs of radicalisation, to understand the drivers and pathways towards violent extremism and to respond** accordingly. The **exchange of experiences and expertise** among – by now about 3000 - practitioners with very diverse professional background from across Europe[23] remains an adequate way to achieve these objectives. However, in order to increase the number of practitioners to benefit from learnings and insights exchanged at RAN events the **dissemination of RAN findings in Member States should be further enhanced**. Furthermore, the inclusion of **new categories of practitioners** (such as judges and prosecutors and increasingly probation officers) may be beneficial.

The seriousness of the phenomenon of radicalisation and its effects on societal cohesion call for targeted, timely and effective measures with regard to interventions to be implemented at local level, the policy framework and cooperation mechanisms. Targeted research, peer review of practices and approaches, the development of practical guidelines, handbooks and toolkits as well as policy recommendations are part of RAN activities and remain pertinent in achieving these objectives. However, in order to ensure that **national policy makers** get the full benefit from RAN activities and findings, their **increased involvement** could be envisaged. Furthermore, more emphasis could be put on **measuring effectiveness and impact** of RAN deliverables. Expectations go beyond reports on best or inspiring practices calling for concrete guidelines, handbooks and toolkits for practitioners and policy makers alike.

The RAN **addresses all forms of extremism and radicalisation** but has recently focussed increasingly on departing as well as returning Foreign Terrorist Fighters (FTFs) while also looking into the challenges of growing polarisation in society, including the rise in political right or left wing extremism but also recruitment and radicalisation in refugee camps. There is

[22] Regulation (EU) No 513/2014 of the European Parliament and of the Council of 16 April 2014 establishing, as part of the Internal Security Fund, the instrument for financial support for police cooperation, preventing and combating crime, and crisis management and repealing Council Decision 2007/125/JHA.

[23] Practitioners include police, prison and local authorities, but also those who are not traditionally involved in counter-terrorism activities, such as teachers, youth workers and healthcare professionals.

an increasing need to **enhance work with most advanced practitioners and experts on high priority topics** to provide timely, operational and state of the art guidance.

The RAN CoE being **a virtual entity** and services being provided under a procurement contract with limited duration, there is a risk that expertise and relations built in the course of one contract period are lost. In addition, the **lack of permanent structures** may limit the visibility of the work of Centre of Excellence and limit the scope and impact of its actions and their sustainability.

The RAN is **a platform** for prevent practitioners from across Europe to exchange experience, expertise and best practices. This EU wide network facilitates EU wide cooperation. Through RAN working group meetings and other RAN events, the participating frontline practitioners from different EU Member States establish new contacts which in turn facilitate cooperation also on a bilateral basis. These exchanges in turn improve the skills and capabilities of practitioners at local, regional and national level.

The RAN was conceived to be **a network of networks**, i.e. relying on existing practitioners' networks in Member States. The Commission has continuously encouraged Member States to **establish similar practitioner networks in their countries**. However, not many Member States seem to have established such networks which may limit outreach and wider dissemination.

The RAN has established a **list of national RAN contact points** which should facilitate the further **dissemination of outcomes** of meetings to the relevant stakeholders in the respective country. Furthermore, the Commission has created a **Network of national prevent policy makers** facilitating cooperation and exchange of experience and expertise among Member States in relation to policy priorities (two meetings already took place).

Member States may receive **tailor made support** from the RAN Centre of Excellence, in the form of trainings, workshops and RAN missions. The purpose of these support services is to **strengthen the Member States' capability** to tackle radicalisation more effectively, in particular in a more structural and strategic way (e.g. through advice on how to set up a prevent strategy, establish networks of practitioners, etc.). Almost all Member States benefited from different types of RAN support services, with a preference for trainings and workshops whereas tailor made counselling services or RAN expert missions were not deployed to the extent offered. An **enhanced engagement with Member States** should contribute to **Member States being encouraged to establish the necessary framework conditions** and implement the necessary measures in their countries building on insights and learnings from the RAN.

Support to policy implementation in the field of radicalisation has also been provided by the security research programme, under management of the European Commission under the 7th Framework Programme[24] and Horizon 2020[25] [26]. Specifically, the projects SAFIRE, PRIME, VOX-POL and IMPACT-EUROPE have provided scientific tools and policy suggestions directly usable by law enforcement agencies and security policy makers, including the experts of the Radicalisation Awareness Network (RAN).

All RAN activities are based on the **respect for fundamental rights** and all RAN members and participants are to adhere to EU fundamental rights as stated in the Charter of Principles Governing the activities of the RAN CoE. Best practices promoted by the RAN favour trust building measures between the different stakeholders, community engagement, empowerment of stakeholders and a bottom up approach. RAN CoE activities implement EU policies

[24] See: https://ec.europa.eu/research/fp7/index_en.cfm?pg=security.
[25] See: https://ec.europa.eu/programmes/horizon2020/en/h2020-section/secure-societies-%E2%80%93-protecting-freedom-and-security-europe-and-its-citizens.
[26] The full list of security research projects can be found here: https://ec.europa.eu/home-affairs/financing/fundings/research-for-security_en.

pursuing the overall aim of safeguarding security but also building an inclusive society avoiding stigmatisation of any community.

RAN CoE can offer its expertise to Member States where this is requested and provides expertise to a selected number of **priority third countries** (including Western Balkans, Tunisia, Jordan, Lebanon and Turkey). However, financial resources for such deployments to third countries are limited. Also, RAN activities are in principle limited to EU (EEA) countries and third country practitioners are not systematically invited to participate. Furthermore, while RAN establishes working relationships with selected international organisations, networks and initiatives, the resources for more advanced partnerships and cooperation are again limited.

Overall, the policy acquis and supporting activities (funding, training and networking) in this area are considered as satisfactory and providing a good basis for further development.

RAN has been one of the biggest success stories in terms of establishing a network of practitioners across Europe. It is performing in a satisfactory manner although dissemination and closer linkage with Member States could be further enhanced to increase outreach and impact.

Impact of the RAN CoE could be increased if Member States had similar practitioners' networks in place and if prevent work was embedded into national or regional prevent strategies. Closer involvement of Member States in prevent work (such as the establishment of a network of national prevent policy makers) could help encouraging the establishment of such networks or strategies. Also, in order to enhance the implementation of initiatives and best practices discussed at EU level project funding also at the national level should be promoted (e.g. under ISF police shared management).

Training of practitioners is one of the priorities to enhance their skills and the advance the effectiveness of their interventions. The mapping and development of tailor made training material, in close cooperation with the relevant organisations and EU agencies, could further improve capacity building.

Stepping up efforts in evaluating the effectiveness of the interventions is crucial.

Furthermore, the extent to which the establishment of more permanent structures for the RAN CoE would require a new legal basis could be explored. Such a permanent Centre of Excellence could encompass not only the RAN as its exists today but also the network of national prevent coordinators, the closer involvement of academics, the development and provision of trainings and other support services, the development of state of the art handbooks and tools and possibly increased outreach to external partners. As a first step, the Commission envisages to call upon the expertise of high-level experts in an advisory body (e.g. High Level Expert group on Radicalisation) which would contribute to the further development and implementation of EU prevent policies, instruments and initiatives and could provide advice on more permanent and structured cooperation.

Possible new initiatives to be further explored could include:

- Setting up a High Level Expert Group on Radicalisation (HLEG-R) to advise the Commission on options for a more permanent structure for collaboration and coordination of prevent work and the further development of EU prevent policies;
- Follow up initiatives by the Commission taking into account recommendations and opinions issued by the HLEG-R.

The EU Internet Forum

1. Legal framework

In light of the growing use of the internet by terrorists, the **European Agenda on Security committed in April 2015 to the establishment of an EU Internet Forum**.

The **objectives of the EU Internet Forum are implemented through a number of EU led initiatives** including the **EU Internet referral Unit** (EU IRU, which received its mandate to address the challenges of terrorist material online from Council Conclusions[27] with its activities being based on the existing legal framework for Europol) and the **Civil Society Empowerment Programme** (parts of which will be implemented through the Radicalisation Awareness Network while the envisaged call for proposals to support civil society in developing counter or alternative narratives would take place under ISF Police).

The work of the EU Internet Forum draws upon the expertise of the RAN, the European Strategic Communications Network (ESCN, funded under ISF - Police for a period of 1 year until September 2017) and Europol.

2. Analysis

The Internet Forum was established in order to bring Member States and the industry together to enhance understanding of the threat, improve understanding about respective capabilities and agree and explore mitigating measures. The EU Internet Forum is based on the understanding that the urgency to take action requires swift responses for which cooperation with in particular the internet industry on a voluntary basis is needed.

Main objectives for the work under the EU Internet Forum are:

- To reduce accessibility to terrorist content online;
- To increase the volume of effective alternative narratives online.

The Forum can also provide an adequate platform for the inclusion of other policy objectives and initiatives, such as the work on access to e-evidence.

It should be noted that work with industry on hate speech is pursued under the framework of a distinct dialogue with industry.

Since the Forum's launch in December 2015, there have been some changes in the overall threat. Nevertheless terrorists have continued to demonstrate their intent to use the internet to radicalise, recruit, instil fear, advise on and direct terrorist activity, and glorify their atrocities.

Whilst the output of Daesh propaganda has seen a drop, its dissemination across platforms continues. At the same time, there is a resurgence of Al Qaeda propaganda as well as other terrorist groups – particularly violent right wing extremists. Within the Forum there is a strong focus on Daesh propaganda. Propaganda of violent extremist groups, particularly from the right wing, need to be also taken into consideration, as well as the reciprocal radicalisation potential of such propaganda with further negative spill-over effects in terms of polarisation in society.

There is general consensus that no one party can tackle this problem on its own. It is clear that a public-private partnership is required, using the capability and expertise of all involved. The members of the Internet Forum, including companies, remain committed to implement further actions.

The EU Internet Forum has assisted in bringing Member States and the industry together, and achieved the following. Contacts, which were previously lacking or proving difficult (particularly for the smaller Member States) have been established. It has also led to a better understanding of respective capabilities. The Forum's stakeholders have shown a willingness to work collaboratively. This has resulted in progress, such as the development of a database of hashes which helps prevent removed terrorist material from one site, simply being re-uploaded onto another, as well as the launch of the Civil Society Empowerment Programme.

[27] On 12 March 2015, the JHA Council agreed that, building upon Europol's Check the Web service, Europol should develop an Internet Referral Unit by 1 July 2015.

The EU Internet Referral Unit at Europol is playing a significant role in addressing the first objective, providing expertise facilitating the referrals process. The companies appreciate the quality of the referrals from IRU which are accompanied by an expert assessment, thereby enabling the companies to quickly take action. Speed is essential so as to mitigate the harm. The rate of success is between 80%-and 90% in responding to over 30.000 referrals by the IRU. Furthermore, the IRU provides significant operational and analytical support to Member States.

The EU Internet Forum has also extended its reach to platforms which were not originally part of the Forum, thus raising awareness of terrorists' modus operandi online and broadening the referrals service of the IRU. This ongoing effort is helping protect online users from harmful material, and has also helped increase the resilience of platforms thereby making them less attractive to terrorists.

As to the second objective of the Forum, the Civil Society Empowerment Programme will help ramp up civil society expertise across the EU in the development of powerful alternative narratives online. Member States all acknowledge the importance of online campaigns which challenge and undermine the terrorist narrative, but resource and technical knowledge is often lacking. The CSEP will therefore go some way in addressing this gap.

The EU Internet Forum has been set up to tackle abuse on the Internet, whilst fully **safeguarding fundamental rights**, such as freedom of expression. To the extent that material is referred by Europol to the companies, Europol examines such material against companies' terms and conditions (which prohibit in most cases terrorist content or incitement to violence and hate), taking into account the existing EU legal framework on terrorist offences (including incitement, recruitment or instructions to commit terrorist attacks online). It focusses its actions on material produced by those groups designated as terrorist organisations by both the UN and EU.

Furthermore, the 2017 Directive on Countering Terrorism harmonises the definition of terrorist offences, clarifying and defining the incitement of others to commit acts of terrorism or providing instructions and training material online as a criminal offence. This in turn helps in identifying and removing such content.

The Commission has engaged in some international fora such as the United Nations and the Global Counter Terrorism Forum.

Overall, the acquis and supporting activities (funding, training, and networking) are performing in a satisfactory manner. More may be needed however as regards implementation.

The stated objectives of the forum for 2017 include the full implementation of the "database of hashes", reaching out to newer and younger companies, exploring further automated detection capabilities, as well as fully implementing the Civil Society Empowerment Programme.

3. Protect

COUNCIL RECOMMENDATION of 6 December 2001 setting a common scale for assessing threats to public figures visiting the European Union (2001/C 356/01)

1. Legal framework

COUNCIL RECOMMENDATION of 6 December 2001 setting a common scale for assessing threats to public figures visiting the European Union (2001/C 356/01) as well as the COUNCIL DECISION 2009/796/JHA of 4 June 2009 amending DECISION 2002/956/JHA setting up a European Network for the Protection of Public Figures.

2. Analysis

The basis for the 2001 recommendation was the need to improve cooperation between Member States in the field of the prevention of terrorism[28] and the increased number of official visits from and to the Union.[29] Although public figures had been attacked on a number of occasions, there was no strategy for counter measures and prevention.[30]

In order to comply with such standards, a number of measures had been taken into consideration by the implementation of the European network for the protection of public figures (ENPPF).

Useful tools had been identified, such as the exchange of information, development of best practices as regards operational activities, mutual secondments and exchanges inside the network, developing common strategies on improving working methods and on prevention of assaults and attacks.[31]

In a self-assessment in April 2014, delegations of Member States gave their feedback on several aspects, such as the organisation of the ENPPF network itself, the work planning, the cooperation with other partners as well as a general evaluation of the network. The overall evaluation was that most Member States agree that the ENPPF was achieving the goal set by the Council.[32]

However, there were also some criticisms on the success of the network and the commitment of the Member States themselves was identified as an important issue. ENPPF activities should be leading to more practical results. Closer and more informal contacts between members would enhance that strategy.

It was suggested to make better use of communication channels, such as the EUROPOL Platform for Experts (EPE) or EUROPOL's Secure Information Exchange Network Application (SIENA), in order to contribute to the better spread of best practices and to share knowledge on different fields.[33]

Apart from some logistical and structural aspects (location and preparation of meetings, creating of working groups and election of the Presidency of the network and a management board, set up of a web platform for dissemination of information to the members) it was highlighted to better cooperate by organising joint trainings between respective services and mixed protection teams for a more standardised training. Also the mutual secondment of staff of different departments of the network was emphasised.[34]

[28] COUNCIL RECOMMENDATION of 6 December 2001 (2001/C 356/01), (1).
[29] COUNCIL RECOMMENDATION of 6 December 2001 (2001/C 356/01), (2).
[30] Initiative of the Kingdom of Spain (2002/C 42/08), (1), (2).
[31] COUNCIL DECISION of 28 November 2002 (2002/956/JHA), Art. 4.
[32] Council document Note 10611/14.
[33] Council document 10611/14.
[34] Council document 10611/14.

In the agenda of the ENPPF work program for 2016, the following actions had been in the focus to be carried out, mainly by sub-working groups[35]:

- General coordination, cooperation with ENPFTAA, CEPOL, Europol and coordination of subworking groups;
- Unmanned aerial vehicles (UAV);
- Mixed closed protection teams and common training;
- Information platform and secure communication.

It can be concluded that the creation of the ENPPF network by the Council Decision 2009/796/JHA (amending decision 2002/956/JHA) was a useful tool for the further development of the protection standards inside the union. Some of the main objectives have been taken up consequently and are processed by working groups.

Most importantly from an operational point of view, and as clearly stated by some members of the network, are the improvement of the exchange of information, the development of best practices as regards operational activities, mutual secondment of officials between the members and common procedures, methods, protocol and collaboration when it comes to analysis, execution and training.

As mentioned in the last annual program, information platform and secure communication, like SIENA from EUROPOL, are currently in the focus and likely to be applied by the network. It is also aimed at going for more common training activities.

However, other practical issues such as adapting common procedures, agreeing on same operational standards and promoting secondments between agencies stil need further progress. Active engagement from all members remain needed.

Prevention, Preparedness and Consequence Management of Terrorism and other Security related risks (CIPS) 2007-2013

1. Legal framework

The legal basis of the CIPS 2007-2013 programme is Council Decision (EU, Euratom) No 2007/124/EC, Euratom which established for the period 2007-2013 the Specific Programme "Prevention, Preparedness and Consequence Management of Terrorism and other Security related risks" as part of the General Programme on Security and Safeguarding Liberties ("CIPS Decision").

2. Analysis

CIPS had the following general objectives (article 3 of the CIPS Decision):

> 1. contribute to support Member States' efforts to prevent, prepare for, and to protect people and critical infrastructure against terrorist attacks and other security related incidents;
>
> 2. contribute to ensuring protection in the areas such as the crisis management, environment, public health, transport, research and technological development and economic and social cohesion, in the field of terrorism and other security related risks within the area of freedom, security and justice.

CIPS had the following specific objectives (article 4 of the CIPS Decision):

1. protecting people and critical infrastructure by stimulating, promoting and supporting:

> (a) risk assessments on critical infrastructure, in order to upgrade security;

[35] Note 9742/15 from Presidency to LEWP (ENPPF) from 19th June 2015, page 6.

(b) the development of methodologies for the protection of critical infrastructure, in particular related to risk assessment;

(c) shared operational measures to improve security in cross-border supply chains, provided that the rules of competition within the internal market are not distorted;

(d) the development of security standards, and an exchange of know-how and experience on protection of people and critical infrastructure;

(e) Community wide coordination and cooperation on protection of critical infrastructure.

2. developing the "consequences management" in case of terrorist attack or other security related incident by:

(a) stimulating, promoting and supporting exchange of know-how and experience, in order to establish best practices with the view to coordinate the response measures and to achieve cooperation between various actors of crisis management and security actions;

(b) promoting joint exercises and practical scenarios including security and safety components, in order to enhance coordination and cooperation between relevant actors at the European level;

(c) contributing to the development of innovative methods and/or technologies with a potential for transferability to actions at Community level; at Member State level; and/or acceding or candidate countries.

The CIPS 2007-2013 financial allocation was 140 million EUR and was implemented under the direct management mode. Projects were supported by grants awarded by the Commission or via contracts for services concluded following the calls for tenders published by the Commission.

The following types of actions could be financed (article 5 of the CIPS Decision):

(a) projects initiated and managed by the Commission with a European dimension;

(b) transnational projects involving partners in at least two Member States, or at least one Member State and one acceding or a candidate country;

(c) national projects within Member States, which:

(i) prepare transnational projects and/or Community actions (starter measures);

(ii) complement transnational projects and/or Community actions (complementary measures);

The CIPS objectives were to be achieved by the financing of:

a) projects on operational cooperation and coordination (strengthening networking, mutual confidence and understanding, development of contingency plans, exchange and dissemination of information, experience and best practices);

b) analytical, monitoring, evaluation and audit activities;

c) development and transfer of technology and methodology; particularly regarding information sharing and inter-operability ;

d) training, exchange of staff and experts; and

e) awareness and dissemination activities.

A mid-term evaluation of CIPS was done in 2010, and the results are available in Communication COM(2011)318. An ex-post evaluation is ongoing and the final report is expected in the second half of 2017.

CIPS, i.e. the Council Decision 2007/124/EC was repealed by the Council Decision (EU, Euratom) 2015/457 with effect from 1 January 2014, considering the new regulation providing for financial support for police cooperation, preventing and combating crime, and crisis management as part of the Internal Security Fund established for the period from 1 January 2014 to 31 December 2020 by Regulation (EU) No 513/2014 of the European Parliament and of the Council

Without prejudging the findings of the ex-post evaluation, some preliminary observations can be made at this stage.

CIPS projects were primarily led by universities and research institutes, followed by private sector companies and national Ministries. Activities implemented as part of actions grants were mostly focused on analytical, monitoring and evaluation activities (72% of projects); development and transfer of technology and methodology (69%) and exchange of know-how and best practices (52%).

CIPS Programme was relevant to the needs on the ground, in particular for cooperation between Member States due to the often transnational nature of terrorism and other security-related threats and the likely cross-border effects of disasters affecting critical infrastructure.

Member States as well as the Commission's relevant services were every year consulted on the Annual Work Programmes (AWPs). The consultation procedure served to ensure that relevant priorities were defined in the AWPs.

The priorities set in the AWPs furthered notably the implementation of Council Directive 2008/114/EC on the identification and designation of European critical infrastructures and the European Programme for Critical Infrastructure Protection (EPCIP).

Both transnational and national projects generated EU added value especially in the area of the development of tools and methodologies. This included concrete examples of added value through the development of common models, protocols, guidelines and processes. A potentially significant part of activities developed under CIPS would not have been developed in the absence of this EU funding.

With regards to fundamental rights, the basic acts establishing the Asylum, Migration and Integration Fund (AMIF) and the Internal Security Fund (ISF) for the programming period 2014-2020 contain various relevant provisions stressing the relevance and importance of **the Charter of Fundamental Rights** of the European Union.

Regulation (EU) No 513/2014 of the European Parliament and of the Council of 16 April 2014 establishing, as part of the Internal Security Fund, the instrument for financial support for police cooperation, preventing and combating crime, and crisis management and repealing Council Decision 2007/125/JHA ('ISF Police Regulation') has the following provisions:

- Recital 19: "The Instrument should be implemented in full respect for the rights and principles enshrined in the Charter of Fundamental Rights of the European Union and for the Union's international obligations."
- Recital 20: "Pursuant to Article 3 of the Treaty on European Union (TEU), the Instrument should support activities which ensure the protection of children against violence, abuse, exploitation and neglect. The Instrument should also support safeguards and assistance for child witnesses and victims, in particular those who are unaccompanied or otherwise in need of guardianship."
- Article 3(5): "Actions funded under the Instrument shall be implemented in full respect for fundamental rights and human dignity. In particular, actions shall comply with the provisions of the Charter of Fundamental Rights of the European Union, Union data protection law and the European Convention for the Protection of Human Rights and Fundamental Freedoms (ECHR). In particular, wherever possible, special attention shall

be given by Member States when implementing actions to the assistance and protection of vulnerable persons, in particular children and unaccompanied minors."

The 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

1. Legal framework

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.[36]

2. Analysis

The Directive aims to establish an EU-wide process for identifying and designating European Critical Infrastructures (ECIs) in energy and transport sectors and sets out an approach for assessing the need to improve their protection. Member States must identify potential ECIs, with the help of the European Commission if required, using cross-cutting criteria (possible casualties and economic/public effects) and sectorial criteria (specificities of each ECI sector). Member States go through a cooperative designation process (e.g. discussions with the other Member States) for potential ECIs located on their territory and review regularly the identification and designation of ECIs. They also ensure that for each ECI an operator security plan (OSP) or an equivalent measure is in place and a security liaison officer is designated, to be the contact point between the owner/operator of the ECI and the EU country's authority concerned. Member States also conduct threat assessments in relation to ECIs and report every year to the Commission generic data on the types of risks, threats and vulnerabilities encountered.

The EU is facing an unprecedented level of terrorist threat. Recent attacks and available assessment indicate that the threat against critical infrastructures is likely to rise. There is a need to enhance preparation and response capabilities. In this context the main weakness of the existing directive is its limited scope, covering only sectors of transport and energy. Another issue is the limited character of the mandate given to the Commission and the limited obligations imposed to the Members States.

While the Directive has brought clean benefits in awareness raising and exchange of good practices, its overall impact has remained more limited than initially expected.

Recent studies[37] have brought into question whether the Directive is the most appropriate tool to produce the expected benefits. The main objective of increased CIP has seen only limited progress (only 89 ECIs identified and registered), while secondary benefits were markedly achieved (awareness-raising, increased cooperation and coordination, kick-starting CIP programmes, etc.). Studies also reflected the perception that resources and capacity required by the application of Directive 2008/114 were taken away from other possible measures that could produce higher impacts, such as establishment on voluntary basis of Commission led coordination of CIP-related activities across all sectors in Member States willing to participate.

Other CIP related initiatives, specific to different sectors, have developed in recent years with, for example, the 2016 NIS Directive[38] and Decision 541/2014/EU of 16 April 2014

[36] http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32008L0114.

[37] Those (non-public) reports were respectively an impact assessment study (Ramboll) and study to support the preparation of the review of the Directives ordered by the Commission from management consultants Ramboll (2011) and Booz & Co (2012).

[38] http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2016.194.01.0001.01.ENG&toc=OJ:L:2016:194:TOC.

establishing a Framework for Space Surveillance and Tracking Support[39]. In 2015 a consultation on risk preparedness in the area of security of electricity supply was also carried out. More and more initiatives are expected, raising the issue of clarity and coordination, and of the coherence with the mechanisms set up by the Directive 2008/114.

Considerable support to the policy implementation in the field of Critical Infrastructure Protection has been provided by the security research programme in both Framework Programme 7[40] and Horizon 2020[41]. A wide array of projects launched the development of innovative solutions (including analyses, technologies and processes) to protect European Critical Infrastructures. Examples include threats foresight, "stress tests" on, and resilience of, Critical Infrastructures (IMPROVER, INFRARISK, STREST, CIPRNET, RESILIENS, CRISALIS, DARWIN); protection of critical infrastructures against electromagnetic radiation (HIPOW, STRUCTURES, VIKING), cyber-threats (MICIE, SIRINITI), or other threats (SERCSIS, WSAN4CIP); protection of specific types of infrastructures such as the European smart electrical and energy grids of the future (AFTER, SEGRID, SPARKS, SESAME, ARGOS, EURACOM, SUCCESS), European railways (PROTECTRAIL, SECRET), airports (TASS, XP-DITE, FLYSEC), urban transportation networks (SECUR-ED, RESOLUTE), larger transportation networks (SERON, STAR-TRANS, DEMASST), ports (SECTRONIC, SUPPORT), or space systems (PROGRESS, SCOUT). The Commission also supports actions in pre-normative research and harmonisation that could improve the efficiency of protecting Europe's critical infrastructures. Many of these projects are directly linked to the goals of the legislation on Critical Infrastructure Protection. Furthermore, three projects addressing the prevention, detection, response and mitigation of the combination of physical and cyber threats to the critical infrastructure of Europe are to be launched in 2017.

The scope of the directive only marginally concerns fundamental rights. Its preamble (point 21) however requires that its application complies with the principles recognised by the Charter of Fundamental Rights of the EU.

The directive does not have a clear external reach. However a limited external dimension was observed in practice, with experience sharing between EU Member States and USA and Canada. This approach has had positive results and is likely to be extended to the Western Balkans countries and the Eastern Europe neighbouring states.

EU CBRN Action Plan

1. Legal framework

Council Conclusions 15505/1/09 of 30 November 2009 on strengthening chemical, biological, radiological and nuclear (CBRN) security in the European Union - an EU CBRN Action Plan.[42]

2. Analysis

The overall goal of the 2009 Council conclusions was to reduce the threat of and damage from CBRN incidents of accidental, natural or intentional origin, including acts of terrorism.

The EU CBRN Action Plan was developed at a time when efforts to strengthen chemical, biological, radiological and nuclear security in the European Union were fragmented and required a more comprehensive approach. There had been several earlier initiatives in the CBRN area, with a limited scope, e.g. 2008 Conclusions on the creation of a CBRN

[39] http://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX%3A32014D0541.
[40] See: https://ec.europa.eu/research/fp7/index_en.cfm?pg=security.
[41] See: https://ec.europa.eu/programmes/horizon2020/en/h2020-section/secure-societies-%E2%80%93-protecting-freedom-and-security-europe-and-its-citizens.
[42] http://register.consilium.europa.eu/doc/srv?l=EN&f=ST%2015505%202009%20REV%201.

database[43], which resulted in an extension of the European Bomb Data System (EBDS) to CBRN or setting up of the European Centre for Disease Prevention and Control[44]. At that point in time, a 124-actions long action plan was a useful concept, gathering all the CBRN-related needs and gaps in one document. It helped both the Member States as well as the EU to systematise work in this area.

The implementation of the Action Plan was envisaged for the period 2010-2015; therefore as such it is expired. The Commission supported the approach adopted in 2012, when the Member States in Council Conclusions encouraged the Commission to limit the number of priorities and look for synergies between CBRN and explosives policies, and to focus on key priorities. Over past years Member States – also thanks to the incentives from the Action Plan – have increased their CBRN preparedness level. Moreover, many actions have been fully implemented and therefore became obsolete. The CBRN Action Plan remains however an important guidance document listing actions which need to be taken for a Member State to significantly enhance its CBRN safety and security. The CBRN threat is evolving, and there is a need to reflect on new initiatives in this area notably on security aspects of the CBRN policy, and building on the achievements of the CBRN Action Plan.

The EU CBRN Action Plan, with 124 actions, was crucial for developing the European cooperation in the CBRN area. Some of the actions were to be implemented at EU level (by the Commission or Europol), others at national level by each country.

There are numerous examples of actions which supported and facilitated European cooperation. CBRN experts started to use tools designed initially for explosives experts, such as the European Bomb Data System (IT tool allowing secure exchange of information; at the end of 2016 it had more than 2000 entries - files/incidents/posts) and EEODN – European Explosive Ordinance Detection Network, which organises yearly conferences with a training component. Moreover Europol, which manages EEODN on a daily basis, organised additional trainings for EEODN members on response to radiological emergency (more than 50 policemen from the EU Member States as well as Moldova and Ukraine participated).

The Commission furthermore organised many trainings and exercises intended for different target groups. It set up EUSECTRA – European Nuclear Security Training Centre – at JRCs premises in Karlsruhe which provides hands-on training using real nuclear materials to front line officers, their management, trainers and other experts in the field. Training has also been provided on radiological-nuclear detection for custom officials. Only in 2016 there were around 300 people trained in EUSECTRA.

The issue of cross-sectorial cooperation was addressed during Commission trainings in recent years[45], including on the triage, monitoring and treatment of mass casualties resulting from a terrorist attack involving ionising radiation (i.e. dirty bomb scenario). More than 100 participants – police, firefighters, incident commanders and medical staff – from almost all (26) Member States were trained.

In absence of any major CBRN attacks so far in EU, exercises have been the best way to test procedures and to verify preparedness. In the context of the civil protection cooperation, the Commission supports the organisation of exercises (on average four per year; more than 50 since 2002). Most of them concern natural disasters, but e.g. in 2013 Spain in cooperation with Morocco and four other Member States organised the CURIEX exercise focusing on contamination in case of a nuclear incident.

[43] http://data.consilium.europa.eu/doc/document/ST-15294-2008-REV-2/en/pdf.
[44] Regulation (EC) No 851/2004 of the European Parliament and of the Council of 21 April 2004 establishing a European Centre for disease prevention and control; http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32004R0851&from=EN.
[45] There were altogether 5 training sessions: October and December 2015, February, May, and September 2016.

In the public health area, the Commission proposed new legislation[46] on cross-border threats to public health, which provides the framework to improve preparedness and strengthen the capacity to coordinate response to health emergencies. It set up e.g. the Early Warning and Response System, which allows Member States to send alerts about events with a potential impact on the EU, to share information and coordinate their response. The system has already been successfully used for previous outbreaks of SARS, Pandemic Influenza A(H1N1) and other communicable diseases.

For most of the Member States the Action Plan constituted an incentive to enhance their CBRN preparedness. In some cases it proved to be challenging due to the fact that – as one of the Member States reports - this area falls within the competence of many actors and it is very difficult to take stock of who is doing what and who is responsible for what.

In general however, Member States have reported that working on the CBRN action plan has raised the overall awareness and acceptance for CBRN issues and CBRN protection and that exchange of information between Member States at the meetings, and the reports from the studies initiated by the Commission, have given a better understanding of similarities and differences between the Member States.

The EU CBRN Action Plan was an umbrella initiative which served as a basis for many other initiatives at EU level, e.g. several actions of the Joint Research Centre (as mentioned above development of EUSECTRA training facility or testing of detection equipment etc), or Commission's CBRN modules within the Civil Protection Mechanism[47].

The EU CBRN Action Plan served also as a point of reference for the EU CBRN Risk Mitigation Centres of Excellence (CoE) initiative.

In 2012, the Commission reviewed progress[48] in implementing the EU CBRN Action Plan[49] and the 2008 Action Plan on Enhancing the Security of Explosives[50]. Discussions with EU Member States and stakeholders resulted in the new comprehensive EU CBRN-E Agenda[51], in which the Council encouraged the Commission to develop a new and more focused policy, building upon the work carried out under the two Action Plans and looking for synergies between the CBRN and explosives policies. The 2014 Communication on a new EU approach to the detection and mitigation of CBRN-E risks[52] was the first expression of the new CBRN-E Agenda.

The EU CBRN Action Plan also provided guidance for the European security research and development on CBRN risk mitigation, in the 7th Framework Programme[53] and in Horizon 2020[54], primarily under the Disaster Resilient Societies area. Several research projects supported the implementation of the Action Plan, launching the development of innovative technological solutions for CBRN risks prevention, detection, protection or response; demonstrating new processes at EU-level; and/or delivering novel risk assessments for CBRN

[46] Decision 1082/2013/EU of 22 October 2013 on serious cross-border threats to health. https://ec.europa.eu/health/sites/health/files/preparedness_response/docs/decision_serious_crossborder_threats_22102013_en.pdf.
[47] http://ec.europa.eu/echo/files/civil_protection/civil/prote/pdfdocs/Summary.pdf.
[48] http://ec.europa.eu/dgs/home-affairs/what-we-do/policies/crisis-and-terrorism/explosives/docs/progress_report_on_explosives_security_2012_en.pdf.
[49] http://ec.europa.eu/dgs/home-affairs/what-we-do/policies/crisis-and-terrorism/securing-dangerous-material/docs/eu_cbrn_action_plan_progress_report_en.pdf.
[50] Council document Doc. 8109/08.
[51] Council Conclusions 16980/12.
[52] Communication on a new EU approach to the detection and mitigation of CBRN-E risks; COM(2014) 247 final; http://ec.europa.eu/dgs/home-affairs/what-we-do/policies/crisis-and-terrorism/explosives/docs/20140505_detection_and_mitigation_of_cbrn-e_risks_at_eu_level_en.pdf.
[53] See: https://ec.europa.eu/research/fp7/index_en.cfm?pg=security.
[54] See: https://ec.europa.eu/programmes/horizon2020/en/h2020-section/secure-societies-%E2%80%93-protecting-freedom-and-security-europe-and-its-citizens.

risks. Examples mentioned here represent a project value of over 160 M€ on CBRN security research from FP7 and H2020 Secure Societies projects and other security-relevant projects, up to 2015. They include roadmapping (CBRNEMAP, DECOTESSC1) and large-scale demonstration projects on CBRN(E) crisis management (EDEN); detection of radio/nuclear sources (COCAE; SCINTILLA; MODES-SNM; REWARD; NERIS-TIP; DETECT; MULTIBIODOSE); response to radiological emergencies (PREPARE); CBRN post-crisis assessment and management for civil security (HANDHOLD, LOTUS, CREATIF, CATO, PRACTICE, COUNTERFOG), including mobile detectors (IMSK, MIRACLE), decision support tools for responders to deal with contamination (DESTRIERO), CBRN forensics toolboxes (GIFT-CBRN), and response to toxic emergencies (BOOSTER, TOXI-TRIAGE). Examples of research on detection of biological threats include work on simpler and/or more reliable systems (MULTISENSE CHIP, TWOBIAS, BIO-PROTECT, ANTIBIOBABE), and improved respiratory protective equipment (FRESP, IF REACT). Other projects looked at specific threats, like C, B or R contamination of drinking water (SECUREAU, ISIS, SAFEWATER, TAWARA_RTM), or to the food supply chain (SNIFFER 2, PLATFOODSEC, SPICED). The Commission also supports actions to facilitate harmonisation that could improve the efficiency of CBRN risk mitigation in the EU with projects (EQUATOX, SLAM) and mandates to European Standardisation Organisations. Furthermore, research projects to develop validation capacity of biological toxins after an incident, supporting a European CBRN cluster, and improving networking among EU CBRN risk management training centres, are being launched in 2017.

As to fundamental rights, the EU CBRN Action Plan did not include any measures aiming at safeguarding them fundamental rights, nor did it affect in any negative way fundamental rights of EU citizens.

With regard to the external dimension, the EU CBRN Action Plan did not have an external dimension per se. Nevertheless, there are many international institutions, initiatives and instruments, which are relevant for CBRN. In the RN area (radiological and nuclear) the most important is the International Atomic Energy Agency. The Commission cooperates regularly with the IAEA (in the security area, the two organizations signed a document called Practical Arrangements, which details the means of cooperation) and the EU supports the IAEA financially (for concrete tasks defined by Member States). The Action Plan underlined also that *Member States together with the Commission to progress the ratification of the amendment to the Convention on the Physical Protection of Nuclear Materials by the EU Member States/Community* (action RN.18). The convention is deposited with the IAEA.

Not included in the EU CBRN Action Plan, but closely related to it is the EU CBRN Risk Mitigation Centres of Excellence (CoE) initiative, which is being implemented with EU financial support in 55 countries around the world. The CoE is benefiting from tools developed within the framework of the CBRN Action Plan, e.g. the CBRN-E Glossary developed for the EU Member States is being also used by the CoE countries and is to be translated into Russian and Arabic in order to maximise its usefulness and impact.

Overall, the EU CBRN Action Plan remains an important guiding document, presenting an all-hazard approach and listing actions which have to be implemented in order to significantly improve preparedness of Member States and the EU for the CBRN incidents.

Nevertheless, the raising level and evolving nature of the CBRN threat calls for exploring new initiatives at the EU level which would support ambitious objectives concerning the overall EU preparedness for the CBRN threats.

COMMISSION DIRECTIVE 2008/43/EC of 4 April 2008 setting up, pursuant to Council Directive 93/15/EEC, a system for the identification and traceability of explosives for civil uses, as amended by Commission Directive 2012/4/EU

1. Legal framework

Delegation of powers contained in Article 14, second paragraph of Council Directive 93/15/EEC to adopt via committee procedure rules on a system for keeping track of explosives. When Directive 93/15/EEC was repealed and replaced by Directive 2014/28/EU, Article 51(3) of the new directive provided for the continued legal basis for Commission Directive 2008/43/EC under Directive 2014/28/EU.

The Council Directive 93/15/EEC of 5 April 1993 on the harmonisation of the provisions relating to the placing on the market and supervision of explosives for civil uses was based on Article 100a of the TEC (which is now Article 114 of the TFEU).

Additionally, the Directive 2014/28/EU of the European Parliament and of the Council of 26 February 2014 on the harmonisation of the laws of the Member States relating to the making available on the market and supervision of explosives for civil uses (recast) is based on Article 114 (Common rules on Competition, Taxation and Approximation of laws) of the TFEU.

In its 25 March 2004 Declaration, the European Council recognised the need to explore a more harmonised system that would prevent explosives, detonators, bomb-making equipment and fire-arms from falling into the hands of terrorists. In response to the European Council's declaration, the Commission adopted on 18 July 2005 Communication COM(2005) 329 on "Measures to ensure greater security in explosives, detonators, bomb-making equipment and firearms". In this Communication the Commission mentioned that the option of setting up a traceability system for civil explosives should be envisaged. This option was retained and included as one of the specific action points of the "EU Action Plan on Enhancing the Security of Explosives" proposed by the Commission with the Communication COM(2007) 651 of 6 November 2007 and adopted by the Council on 11 April 2008.

2. Analysis

The objective of Commission Directive 2008/43/EC is to establish a harmonised system in the EU for the identification and traceability of explosives for civil uses (i.e. commercial explosives). The system is based on two pillars: a harmonised marking system ensuring the unique identification of most kind of explosives (including detonators, primers, boosters and detonating cords) placed on the EU market for the purpose of their use in the civil sector; and an obligation for all undertakings in the explosives sector to put in place a system for the collection of data related to each explosive throughout the supply chain and its life cycle. The data collection system must allow the undertakings to keep track of the explosives in such a way that those holding the explosives can be identified at any time.

The undertakings have the obligation to keep the collected data for each explosive for 10 years, and to provide it to the competent authorities upon request.

Some types of explosives for civil uses (like unpackaged bulk explosives delivered in pump trucks, explosives manufactured on the blasting site immediately prior to their use, certain fuses and safety fuses) are exempted from the scope of the directive, as well as ammunition and pyrotechnic articles.

Furthermore, the Directive 2008/43/EC has become fully applicable only recently (on 5 April 2015), so no comprehensive evaluation of this legislative act has been carried out so far. However, in all meetings of the relevant expert groups, the Commission has been gathering the feedback from the competent authorities of the Member States (and of the EEA/EFTA countries), from the market surveillance authorities and from the stakeholders concerning the implementation of the directive's provisions. The general conclusions that can be drawn from the information received during these meetings is that, after an initial year in which several problems (mostly of a technical nature) were encountered in implementing the system, the situation is now satisfactory in terms of the system's functioning. There are concrete cases of

investigations on explosives disappearances which were solved thanks to the traceability system introduced by the directive.

It is important to mention that the UN body in charge of the international regulations on the transport of dangerous goods, the ECOSOC Sub-Committee of Experts on the Transport of Dangerous Goods, has analysed and discussed the provisions of Directive 2008/43/EC, as it is the only and first ever supra-national explosives traceability system. In its 50th session (held on 28.11.2016 - 6.12.2016), this UN body adopted an amendment to the UN Model Regulations on the transport of dangerous goods, which added a new note recommending the introduction of a global harmonised marking system for explosives security during transport, specifically mentioning the EU system as an example to follow[55].

The main added value of the system set-up by Directive 2008/43/EC is that it establishes a harmonised and unique identification marking for civil explosives placed on the EU market, and that it sets common obligations in terms of record-keeping and provision of information to the competent authorities for all undertakings of the explosives sector throughout the supply chain. These elements facilitate the work of national inspectors and investigators. Before the entry into force of the directive, in some Member States there were already national legal requirements for the purpose of explosives traceability. These provisions however differed significantly from country to country, thus with different levels of control effectiveness and of burden on the economic operators. These national rules also did often not apply to the whole supply chain. The provisions of Directive 2008/43/EC have established a traceability system for explosives also in the Member States that did not already have national provisions in place, and have created a system with a high degree of interoperability for supply chains running across Member States, thus facilitating cross-border cooperation on investigations. It has also created a level-playing field for European companies in terms of the burden deriving from compliance with traceability rules.

The creation of an EU traceability system for civil explosives is one of the action points recommended by the "EU Action Plan on Enhancing the Security of Explosives".

The measures of Directive 2008/43/EC could potentially impact the rights which are enshrined in the following articles of the Charter of Fundamental Rights of the EU (hereinafter: 'CFR'):

- the protection of personal data (Article 8 CFR)
- the freedom to conduct a business (Article 16 CFR)

Regarding the protection of personal data, the provisions of the directive impose that undertakings keep records of, among other things, information on the company or person having the custody of each explosive article at a certain time. The directive however specifies that such records must be kept for a limited amount of time (10 years) and that the correct functioning of the data collection and record-keeping systems must be tested regularly by all undertakings subject to the directive's provisions, and protected against accidental or malicious damage or destruction.

Regarding the freedom to conduct a business, the directive has had a long transitional period before becoming applicable, in order to allow economic operators to spread the initial costs for the setting up of the traceability system (which were known to be significant) over several years. To minimise the burden even further, in particular for SMEs, Directive 2008/43/EC was amended in 2012 by Directive 2012/4/EU. This amendment postponed the entry into force of the traceability provisions, which were initially due to become applicable on 5 April

[55] Text of the adopted note: "In addition to the security provisions of these Regulations, competent authorities may implement further security provisions for reasons other than safety of dangerous goods during transport. In order to not impede international and multimodal transport by different explosives security markings, it is recommended that such markings be formatted consistent with an internationally harmonized standard (e.g. European Union Commission Directive 2008/43/EC)."

2012, to the 5th of April 2013 for the marking of each explosive with the harmonised unique identification, and to the 5th of April 2015 for the data collection and record-keeping obligation. Additionally, Directive 2012/4/EU exempted from the scope of Directive 2008/43/EC three types of explosive articles (certain fuses, safety fuses and cap-type primers), due to their very low-risk in terms of security, which would have made the application of the traceability rules to these articles disproportionate in terms of burden and with no real added value in terms of security.

Directive 2008/43/EC has primarily an internal dimension, as its objective is to ensure full traceability of explosives for civil uses placed on the EU market. However, it can potentially facilitate international investigations on explosives originating from the EU which would be diverted for illicit uses to third, non-EU countries. Also, in the UN ECOSOC Sub-Committee of Experts on the Transport of Dangerous Goods some countries and stakeholders have suggested that the EU explosives traceability system could be used as the basis for a global explosives traceability system or, at least, for a global harmonised unique identification marking which would increase the security of explosives transports against illegal diversion.

Regulation (EU) 98/2013 on explosives precursors

1. Legal framework

Article 114 TFEU.

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.[56]

2. Analysis

Regulation (EU) 98/2013 on explosives precursors aims at:

- restricting access by the members of the general public to chemical substances that can be misused for the illicit manufacturing of home-made explosives;
- ensuring the reporting of suspicious transactions, disappearances and thefts along the supply chain.

Recent attacks and incidents involving home-made explosives in Europe[57] provide evidence of the persisting threat posed by explosives precursor substances. According to Europol's 2016 EU Terrorism Situation and Trend Report,[58] 'home-made explosives remain a preferred weapon of terrorists, along with conventional firearms, because of their availability, simplicity and effectiveness.'

In this context, EU-harmonised rules concerning the making available, introduction, possession and use of explosives precursors are considered necessary because, in a non-harmonised environment, the free movement of people and goods in Europe may facilitate illicit access to, and use of, explosives precursors. Terrorists could exploit regimes where there are no restrictions and controls.

The Regulation has created a legal basis for EU Member States to raise awareness among economic operators in the supply chain about the dangerous properties of some of their products, and to gather information from them on suspicious transactions, disappearances and

[56] OJ L 39, 9.2.2013, p. 1. {HYPERLINK "http://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1427121796620&uri=CELEX:32013R0098"}.
[57] Notably: Brussels (March 2016), Paris (November 2015), Verviers (January 2015). Also, arrests and seizures of home-made explosives in Dublin (April 2016), Cannes (February 2014).
[58] https://www.europol.europa.eu/activities-services/main-reports/european-union-terrorism-situation-and-trend-report-te-sat-2016.

thefts. Reports have led to seizures of illegally possessed substances and to arrests and convictions of individuals.[59]

Finally, many economic operators in the supply chain of explosives precursors conduct business across several EU Member States. EU-harmonised rules on the marketing and use of explosives precursors contribute to the proper functioning of the EU internal market.

The Regulation has supported efforts by Member States to reduce the amount of explosives precursors available on the market and access by members of the general public. Specifically,

- Economic operators all across the EU must apply the restrictions and, although there needs to be further awareness-raising to ensure all operators correctly apply the restrictions, many Member States have conducted inspection actions which evidence that a large number of operators are complying with their obligations.
- Some economic operators have stopped carrying some of the restricted/controlled substances, without significant disturbances or economic losses as a result of this.
- Some Member States that maintain licensing regimes refuse requests for licenses if there exist alternative (non-sensitive) substances for a legitimate non-professional activity.
- Member States applying a complete ban on the restricted substances have not reported complaints from their members of the public. This also suggests that for many non-professional activities there exist alternatives.

The Regulation has also supported efforts by Member States to conduct early investigations into suspicious incidents involving explosives precursors. In particular,

- Member States have reported an increase in the number of reported suspicious transactions, disappearances and thefts due to greater awareness among economic operators who handle explosives precursors.
- Some Member States have, on an ad hoc basis, exchanged information on reports and refused licences which could have cross-border relevance.

The Regulation gives leverage to Member States in their efforts to engage the economic operators in the supply chain, because failure to comply with the restriction and reporting obligations carry penalties. Member States have reported that, regardless of the penalties, the chemical supply chain and retail sector have been eager to contribute to increased security against the threat posed by home-made explosives.

The Commission actively facilitates efforts by Member States and the supply chain through the Standing Committee on Precursors (SCP) where they are all represented, and through the organisation of a series of regional workshops[60] in 2016-2017.

The Commission has also aimed to keep abreast of the evolving security threat, in order to adapt the Regulation to the use of new chemical substances and to enhance the overall system around explosives precursors. In 2016, efforts channelled through the SCP have led to three threat substances being added to Annex II[61]. Early 2017, the Commission adopted a report on the application of the Regulation.

- The Regulation was a key delivery of the **2008 EU Action Plan on Enhancing the Security of Explosives**;[62]

[59] One example is the arrest near Frankfurt, in April 2015, of a couple who had purchased hydrogen peroxide, after the store reported the purchase as suspicious. http://www.nbcnews.com/news/world/turkish-couple-arrested-germany-suspicion-plotting-criminal-act-n351036. Other cases have been reported by Member States to the Standing Committee on Precursors.
[60] Four regional workshops have been planned/carried out so far, involving a total of 15 Member States.
[61] C(2016) 7647 final; C(2016) 7650 final; C(2016) 7657 final.
[62] {HYPERLINK http://register.consilium.europa.eu/pdf/en/08/st08/st08311.en08.pdf }

- in its EU action plan against illicit trafficking in and use of firearms and explosives, [63] which implements the **European Agenda on Security**, the Commission announced that it would strengthen efforts to 1) promote harmonised measures, 2) further engage the supply chain, and 3) accelerate work towards a revision of the Regulation;
- **Europol** has created a Focal Point on Weapons and Explosives which can receive relevant information from Member States and analyse it at EU-level.
- Support to the policy implementation in the field of explosive precursors has also been provided by the security research programme in both Framework Programme 7[64] and Horizon 2020[65,66]. Specifically, the projects PREVAIL and EXPEDIA have worked on the inhibition of acetone, peroxide, hexamine, nitro-methane and ammonium nitrate with good laboratory results. These projects were coordinated by the Swedish Defence Research Agency. More generally, the security research programme funded the study of innovative solutions and contributed to advancing technological capacities for the detection of explosives and of their precursors (projects DOGGIES, OPTIX, SNIFFER, SNIFFLES, CRIM-TRACK, ACES, ChemSniff, etc) as well as the detection of bomb factories (projects LOTUS, EMPHASIS, BONAS, COMMONSENSE, etc.).

The Regulation includes Article 10 on **data protection**, which refers to provisions of the Data Protection Directive 95/46/EC.[67]

As to the external dimension, there is no external reach as it concerns the availability of precursors within the EU. However, issues such as the role of customs and the way to deal with sales over the internet are being addressed and discussed in the Standing Committee on Precursors. Evidence suggest that some explosives precursors' substances and mixtures produced by European companies are being exported to Turkey and later, illegally, diverted towards Iraq and Syria, where they are used by ISIS[68]. This supply chain has been documented by Conflict Armament Research, an independent organisation with a mandate from the Council of the EU and funding from the EEAS. The Commission supports the work of CAR by inviting representatives to brief the Standing Committee on Precursors on their findings. EU companies exporting to Turkey have been are encouraged to be vigilant on the end-use of the products and to report suspicious transactions, even if this falls outside of the scope of the Regulation.

[63] COM(2015) 624 final. http://ec.europa.eu/dgs/home-affairs/what-we-do/policies/european-agenda-security/legislative-documents/docs/20151202_communication_firearms_and_the_security_of_the_eu_en.pdf.
[64] See: https://ec.europa.eu/research/fp7/index_en.cfm?pg=security.
[65] See: https://ec.europa.eu/programmes/horizon2020/en/h2020-section/secure-societies-%E2%80%93-protecting-freedom-and-security-europe-and-its-citizens.
[66] The full list of security research projects can be found here: https://ec.europa.eu/home-affairs/financing/fundings/research-for-security_en.
[67] http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A31995L0046.
[68] http://www.conflictarm.com/download-file/?report_id=2279&file_id=2284.

Transport security legislation

1. Legal framework

European security legislation is well developed for air and maritime transport and has been promoted because of the strong international dimension of these modes. In contrary, there is virtually no legislation on land transport security and on the protection of the open areas of transport terminals, although, since the terrorist attacks of 11 September 2001, there have been more people killed in terrorist attacks in land transport than in all other modes.

EU legislation is based on Article 91 TFEU, stipulating that the common rules applicable to international transport to or from the territory of a Member State or passing across the territory of one or more Member States shall be laid down by the European Parliament and the Council, and Article 222 TFEU.

2. Analysis

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.

The EU has a robust **aviation security** legislation which aims at protecting persons and goods from unlawful interference with civil aircraft, ensuring secure air transport, balancing security needs and passengers and industry interests. Following the terrorist attacks of 11 September 2001, the European Parliament and the Council adopted Regulation (EC) No 2320/2002, which provided a framework for civil aviation security. Detailed supplementing and implementing rules were subsequently added and continuously updated. Regulation (EC) No 2320/2002 has been in particular replaced by framework Regulation (EC) No 300/2008.

The overall objective of the EU's **maritime security policy** is to protect the citizens and our economies from the consequences of unlawful intentional acts against shipping and port operations. 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 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 legislation in **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. Cooperation through AVSEC (committee on civil aviation security) and the commitment of Member States to the aviation security inspection regime with its continuous reviewing effect are remarkable and provide indication on possible improvement of security measures. New emerging topics being considered as having relevance to aviation security are, inter alia, cybersecurity, incoming flights from third countries notably for freight; overflight of conflict zones, protection of public areas of airports, adaptability to imminent threats.

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. Avenue for further work could include would be to consider some security issues for ferries and cruise ships based on a dialogue with the Memebr States and the stakeholders.

There seems to be scope for developing EU policy in the field of **land transport security**. Most experts of land transport security consulted via the LANDSEC group 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 latest security

incidents since 2015, 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 attacks in Brussels in 2016 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.

Transport can be subject to cyber-attacks, which can have serious consequences, including loss of life. Many ongoing cyber security activities are being carried out by different agencies and a major effort should be made to coordinate work and eliminate gaps.

Ensuring a high level of protection against cybercrime is a necessity for the security of today's means of transport (especially infrastructure, signalling and ticketing) as well as for the dissemination of future innovations such as autonomous vehicles and drones, automated driving, vehicle-to-vehicle information exchange or infrastructure-to-vehicle information exchange). It is necessary to develop sectorial initiatives that must be linked to the overall cybersecurity strategy and therefore to work together in a complementary manner both at the specific transport level and at the general level.

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, a large proportion of transport operations occur among Member States and there is clear added value for certain actions to be taken at the EU level. The risk of terrorism and criminal acts has, potentially, a cross-border dimension, especially with the free movement of persons and cargo, therefore common approaches to ensure a good baseline level of transport security throughout the EU is desirable.

Finally, where the EU has no baseline standards for transport security there is a risk that those countries with low levels of security become the 'entry point' into the EU for security risks.

In practice, the situation differs significantly between the different transport modes, according to their respective characteristics.

The European Commission has a strong cooperation on security matters with international aviation and maritime organisations (ICAO - International Civil Aviation Organization, ECAC - European Civil Aviation Conference, IMO), as well as with international partners (USA, Canada, Australia) to establish mutual recognition, exchange best practices and promote transport security. An EU-US Aviation Agreement allows for cooperation in the field of aviation security. In maritime security there is a Memorandum of Understanding between DG MOVE and the US Coast Guard. For aviation and maritime security, the European Commission has close relations with the respective parts of the US Department of Homeland Security.

EU is currently developing a common risk assessment process to improve the security of incoming flights from third countries. This should be complemented by an ambitious capacity-building effort in third countries.

4. Crisis Management

EU Integrated Political Crisis Response (IPCR) arrangements

1. Legal framework

Council of the European Union, *Finalisation of the CCA review process: the EU Integrated Political Crisis Response (IPCR) arrangements*, document 10708/13, 7 June 2013 (LIMITE)

European Commission, *Commission provisions on "ARGUS" general rapid alert system*, COM(2005) 662 final, 23.12.2005[69]

2. Analysis

The objective is to:

- Improve the mutual understanding of the various definitions of threat levels;
- Improve the communication among Member States and with EU institutions when threat levels are subject to change.

Major emergencies or crises (both natural and man-made disasters as well as acts of terrorism), whether inside or outside the EU, may have a wide-ranging multi-sectorial and cross-border impact. This requires a coordinate response at European level, bringing political and operational coordination in the use of EU instruments and cooperation among Member States: "the *raison d'être* of the IPCR arrangements is to foster the joined-up approach – i.e. the mobilisation of all relevant services and bodies among EU institutions and member states and ensure a coordinated set of actions."[70]

The Integrated Political Crisis Response (IPCR) arrangements were developed drawing on the lessons of the former Crisis Coordination Arrangements. The IPCR follows the key principles of flexibility, scalability and subsidiarity to tailor the response to the needs and specificities of the situation.[71]

The first activation of the IPCR arrangements in response to the Migration and Refugee crisis in 2015 has demonstrated the added value of the arrangements. This activation was supported by the Council[72] and contributed to establish a common picture of the situation (improving the collection and analysis of data) with the "crucial support of the Commission, the EEAS and EU agencies."[73]

The IPCR arrangements have also played a role in stimulating/leveraging Member States' action:

- Despite the limited testing of the IPCR arrangements, the adoption of the Solidarity Clause decision and the first activation of the IPCR in October 2015 provided strong incentives for Member States to integrate the EU arrangements into their national crisis response procedures.
- The two support instruments (the IPCR Web Platform and the questionnaires feeding the Integrated Situational Awareness and Analysis (ISAA) reports produced by the Commission and the EEAS) rely on inputs from all stakeholders, and in particular Member States. The IPCR have contributed to the development of a network of crisis management points of contact at EU level.

The ISAA reports offer a **common situation picture** to the Council, building on existing sectorial instruments. Prior to the first activation, this support instrument was assessed as a "promising tool" although "one of its greatest weaknesses comes from the fact that the IPCR

---

[69] http://ec.europa.eu/transparency/regdoc/rep/1/2005/EN/1-2005-662-EN-F1-1.Pdf.
[70] http://www.iss.europa.eu/uploads/media/Brief_38_IPCR.pdf.
[71] Council of the European Union, *The EU Integrated Political Crisis Response – IPCR – arrangements – In brief*, 2016: http://www.consilium.europa.eu/en/documents-publications/publications/2016/the-eu-integrated-political-crisis-response-ipcr-arrangements/.
[72] Luxembourg Presidency of the Council of the EU, *Report on the achievements of the Luxembourg Presidency*, December 2015: http://www.eu2015lu.eu/en/actualites/communiques/2015/12/31-bilan/Report-LU-EU-Council-Presidency_Final-EN-Version_18-January-2016.pdf.
[73] 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.

lack practical resources."[74] While the role of the Commission (in particular its alleged reluctance to "engage fully when it feels that its systems suffice to provide the functions being developed independently by the Council"[75]) was questioned, the IPCR have proved an extremely useful tool to collect, process and analyse data from a wide range of actors (Commission systems, EU agencies, Member States and even international organisations) integrated in the ISAA reports produced under the lead of the Commission.

While the IPCR rely on Council procedures, the informal Presidency Roundtables allow for focused discussions on concrete issues identified. It is now acknowledged that "because of strong buy-in from key stakeholders, including the Commission, the EEAS, agencies and member states, the IPCR has become an **effective tool in agenda-setting and coordinated fact-finding**."[76]

- The IPCR arrangements are automatically activated in case of invocation of the *Solidarity Clause*.
- While the *Emergency Response Coordination Centre* (ERCC) acts as the 24/7 point of contact, it can rely on a network of sectorial crisis response capacities at EU level within the EEAS, Commission services and EU agencies.
- Within the Commission, *ARGUS* provides the internal backbone for internal coordination.
- Support to policy implementation in the field of crisis management, response and coordination has been provided by the security research programme, in both Framework Programme 7[77] and Horizon 2020[78]. Projects launched the development of innovative technological solutions, designed processes and/or completed analyses. Examples mentioned here represent a project value of over 240 M€ on CBRN security research from FP7 and H2020 Secure Societies research. Examples include on tools, methods and training for crisis situational awareness, modelling, prevention and preparedness (CRISMA, TACTIC, MOSAIC, COPE, INACHUS, SICMA, CRISIS, CAST, SICMA, NEXES); emergency information and decision-support systems and tools (ESS, AIRBEAM, CASCEFF, SNOWBALL, EVACUATE, PREDICT, SPEEDKITS, FORTRESS, INDIGO, ELITE, PANDEM); networking for crisis and emergency responders (ESENET, EDUCEN); alert systems and communication strategies for before, during and after crises (A4A, OPTI-ALERT, SAFE-COMMS, POP-ALERT, BESECU, PEP, EMERGENT, COSMIC); post-crisis management and recovery (ACRIMAS, FASTID, CAERUS, OPSIC, COBACORE); search & rescue and/or medical and social capabilities (ICARUS, NMFRDISASTER, PSYCRIS, PULSE, SGL FOR USAR); innovative, reliable and coordinated/interoperable emergency management systems and procedures (DISASTER, IDIRA, HIT-GATE, BRIDGE, EMILI, CONCORDE, CRISCOMSCORE, E-SPONDER, SPARTACUS, DARIUS, EPISECC, CIVILEX); critical (tele)communication systems during crisis and emergencies (SECINCORE, ISITEP, C2-SENSE, INFRA, DITSEF, EULER, SECRICOM, GERYON, REDIRNET, FREESIC, CRYSIS, SALUS, SECTOR, PPDR-TC, ISAR+, HELP, SOTERIA, EMYNOS, BROADMAP). The European Commission also supports actions to facilitate harmonisation (pre-normative research, standardisation and certification) that could

[74] Iñigo de Miguel Beriain, Elena Atienza-Macías, and Emilio Armaza Armaza, "The European Union Integrated Political Crisis Response Arrangements: Improving the European Union's Major Crisis Response Coordination Capacities" in *Disaster Medicine and Public Health Preparedness*, Vol. 9/No. 3, 2013

[75] Boin A, Ekengren M, Rhinard M. *Making Sense of Sense-Making: The EU's Role in Collecting, Analysing, and Disseminating Information in Times of Crisis*. Research Report Presented to the Swedish Civil Contingencies Agency (Myndigheten for Samhällskydd och Beredskap),

[76] Council of the European Union, *op.cit.*

[77] See: https://ec.europa.eu/research/fp7/index_en.cfm?pg=security.

[78] See: https://ec.europa.eu/programmes/horizon2020/en/h2020-section/secure-societies-%E2%80%93-protecting-freedom-and-security-europe-and-its-citizens.

improve security crisis and emergencies management in the EU, with projects and mandates to European Standardisation Organisations. Furthermore, research projects on situational awareness systems to support civil protection preparation and operational decision making, and two pre-commercial procurement (PCP) actions to generate systems for the next generation of information systems to support EU external policies, and on broadband communication systems, are to be launched in 2017-2018.

The process aims at sharing information of strategic nature (no personal data) and coordinating policy response building on regular EU instruments.

The IPCR arrangements can be activated to respond to major emergencies or crises, whether inside or outside the EU. The ISAA is developed by the Commission and the EEAS within their respective roles and responsibilities and can integrate information provided by international organisations and third countries, where relevant.

Solidarity Clause (article 222 TFEU)

1. Legal framework

Title VII Solidarity Clause, Article 222 TFEU.[79]

European Commission, The EU Internal Security Strategy in Action: Five steps towards a more secure Europe, COM(2010) 673 final, 22 November 2010.[80]

European Commission and High Representative, Joint Proposal for a Council Decision on the arrangements for the implementation by the Union of the Solidarity clause, JOIN(2012) 39, 21.12.2012.[81]

European Parliament, Resolution on the EU's mutual defence and solidarity clauses: political and operational dimensions, 2012/2223, 22 November 2012.[82]

Council of the European Union, Council decision of 24 June 2014 on the arrangements for the implementation by the Union of the solidarity clause, 2014/415/EU, 24 June 2014.

2. Analysis

- Contribute to the prevention of the terrorist threat in the territory of the Member States;
- Protect institutions and civilian population from any terrorist attack;
- Assist a Member State in its territory, at the request of its political authorities, in the event of a terrorist attack or a natural or man-made disaster.

Major terrorist attack and disasters are of a cross-border and multi-sectorial natures, and therefore may require a coordinated European response. The instrument embodies the spirit of solidarity in which the Union and its Member States would act to assist a Member State victim of a terrorist attack or a natural or man-made disaster.

While the basic principle remains valid that Member States are primarily responsible for managing crises arising within their territory, the clause is meant to be used in case of "large-scale crises, which are often trans-border and trans-sectoral and thus exceed the response capacity of one individual Member States."[83]

[79] http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:12012E/TXT. (Consolidated version)
[80] http://register.consilium.europa.eu/doc/srv?l=EN&f=ST%2016797%202010%20INIT.
[81] http://eur-lex.europa.eu/legal-content/EN/HIS/?uri=celex:32014D0415.
[82] http://www.europarl.europa.eu/sides/getDoc.do?type=TA&reference=P7-TA-2012-0456&language=EN&ring=A7-2012-0356.
[83] https://europe-liberte-securite-justice.org/2015/07/27/the-solidarity-clause-one-of-the-most-unacknowledged-innovations-of-the-lisbon-treaty-the-european-parliament-debates-its-implementation-but-also-its-ambiguities/.

The instrument is fully in line with the principles of subsidiarity, proportionality as well as sovereignty and national security as the Solidarity clause should only be activated in exceptional circumstances and the assistance provided by the Union and its Member States would only be triggered at the request of the political authorities of the affected Member States.

Yet the strict wording of the Council decision (the affected and requesting Member State would consider "that the situation overwhelms its response capacity) could potentially excessively discourage Member States to activate an instrument, due to the reputational risk (activation could be seen as an incapacity to discharge a core and regalian function of security).

The Solidarity Clause has never been activated so far (after the Paris and Brussels attacks of 2015/2016 the "mutual assistance clause" of article 42.7 was activated, which provides for a purely intergovernmental solution whereas the European Parliament noted that "Article 222 is specifically designed to deal with the consequences of the terrorist attacks in Europe"[84]). It has not been tested in a full scale crisis management exercise. Its impact can therefore not be fully assessed.

The Council decision only focuses on the implementation "by the Union" of the Solidarity Clause: Member States adopted a Declaration on Article 222 stressing that "none of the provisions of Article 222 is intended to affect the right of another Member State to choose the most appropriate means to comply with its own solidarity obligation towards that Member State."[85]

Yet, as part of the negotiations of the EU Integrated Political Crisis Response (IPCR) arrangements and their first activation, Member States have further integrated the European dimension of crisis management in their national procedures.

Whereas para 1 (a) of the article 222 clearly refers to "prevent the terrorist threat" and "protect democratic institutions, the Council decision has focused on the "assistance".

- The possibility to activate the clause in the case of an "imminent terrorist attack" has been removed.
- The provision on regular "integrated threat and threat assessment" have been reduced to ad hoc "reports on specified threats", upon request of the European Council.
- The proposed article 9 "Preparedness" (aiming to identify potential gaps on the means to meet the major threats) was removed from the text.
- The EU IPCR arrangements are automatically activated in the event of an activation of the Solidarity Clause and provided the framework for political coordination in the Council, with the support of the Commission and the EEAS.

This Council Decision does not appear to negatively affect fundamental rights of EU citizens.

Article 2 of the Council decision defines its territorial scope (territory of Member States to which the Treaty apply as well as critical infrastructure in the exclusive economic zone or the continental shelf of a Member State).

The instruments, capabilities or instruments which shall be identified and mobilised by the Commission and the High Representative do not exclude foreign policy and the structures developed under the Common Security and Defence Policy.

[84] European Parliament, *Resolution of 21 January 2016 on the mutual defence clause (Article 42(7) TEU*, P8_TA(2016)0019 http://www.europarl.europa.eu/sides/getDoc.do?type=TA&reference=P8-TA-2016-0019&language=EN&ring=B8-2016-0058.

[85] Declaration on Article 222 TFSU.

The "ATLAS decision": cooperation between special intervention units

1. Legal framework

European Parliament legislative resolution of 31 January 2008 on the initiative of the Republic of Austria with a view to adopting a Council decision on the improvement of cooperation between the special intervention units of the Member States of the European Union in crisis situations.[86]

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.[87]

2. Analysis

The Decision lays down rules and conditions to allow for special intervention units of one Member State to provide assistance and/or operate on the territory of another Member States in cases where they have been invited to do so to deal with a crisis situation (notably terrorist-related); The Decision also foresees that meetings, training and exercises may be funded under possibilities offered by the financial programmes of the Union.

One Member State can receive assistance of another Member State's unit to deal effectively with a **large-scale attack**, a scenario requiring **specific expertise** or **multiple simultaneous attacks** exceeding the national response capability. French and Belgian authorities publicly acknowledged that the French special intervention unit assisted their Belgian counterparts during the counterterrorism raid in Verviers in January 2015.[88]

The evolving nature of the threat (new modi operandi, new weapons and explosives) requires **regular cooperation and exchange of best practices** to ensure that all Member States have access to the most effective techniques to respond to sophisticated threats. This has been **recognised by Member States** (cf. Poland[89], Estonia[90], Sweden[91]), **the EU CTC**[92] **and specialised expert**[93].

The ATLAS members organise regular training and exercises, with EU financial support.

- Trainings allow for the exchange of best practices, notably the sharing of technical capabilities, modi operandi, special tactics, etc.
- ATLAS has developed thematic working groups on i.a. sniper, command and control, explosive ordnance disposal, etc.
- Recent exercises such as *Atlas Common Challenges* 2013 or *ARETE 2014* have highlighted the importance of cooperation. Such exercises have also "anticipated" threats and allowed for better preparation to new threats and modi operandi (e.g. ACC 2013 focused on soft target attacks such as train, ferries, schools and power plants).
- The decision explicitly ensures **complementarity with other cooperation frameworks** (bilateral and EU level, such as Prüm Decision): cf. article 7 "Relation to other instruments".
- some trainings have been organised within **CEPOL framework.**

[86] http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.CE.2009.068.01.0040.01.ENG&toc=OJ:C:2009:068E:TOC.
[87] http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2008:210:0073:0075:EN:PDF.
[88] http://www.europe1.fr/international/belgique-plusieurs-victimes-lors-d-une-operation-anti-terroriste-2345317; http://www.lameuse.be/1564026/article/2016-05-03/hubert-bonneau-patron-du-gign-francais-les-terroristes-de-verviers-voulaient-dec
[89] http://www.antyterroryzm.gov.pl/eng/anti-terrorism/foreign-cooperation/atlas-platform/686,dok.html.
[90] https://www.siseministeerium.ee/en/news/international-counter-terrorism-training-athos-held-estonia.
[91] http://fhs.diva-portal.org/smash/get/diva2:428775/FULLTEXT01.pdf.
[92] http://www.consilium.europa.eu/uedocs/cms_data/docs/pressdata/en/jha/136832.pdf.
[93] https://jamestown.org/program/europes-emerging-counter-terrorism-elite-the-atlas-network/.

- **Europol** contributes to the dissemination of some knowledge products, notably through the EPE (Europol Platform for Experts).
- trainings and exercises have been organised jointly with **other actors** (e.g. transport authorities in ACC2013[94], civil protection in ARETE 2014[95]) to ensure coherence and preparedness to respond to multi-sectorial threats.

The decision includes in its article 4 **provisions on civil and criminal liability** (referring to provisions of the Prüm Decision 2008/615/JHA[96]).

There have been neither any provisions nor actions for ATLAS's involvement outside the EU.

5. Terrorist Financing

Fourth Anti-money laundering directive (4AMLD) - Directive (EU) 2015/849 of the European Parliament and of the Council of 20 May 2015 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing and repealing Directive 2005/60/EC of the European Parliament and of the Council and Commission Directive 2006/70/EC

1. Legal framework

Art 114 TFEU (internal market harmonisation).

This Directive is the fourth directive to address the threat of money laundering. Council Directive 91/308/EEC (4) defined money laundering in terms of drugs offences and imposed obligations solely on the financial sector.

Directive 2001/97/EC of the European Parliament and of the Council (1) extended the scope of Directive 91/308/EEC both in terms of the crimes covered and in terms of the range of professions and activities covered. In June 2003, the Financial Action Task Force (FATF) revised its Recommendations to cover terrorist financing, and provided more detailed requirements in relation to customer identification and verification, the situations where a higher risk of money laundering or terrorist financing may justify enhanced measures and also the situations where a reduced risk may justify less rigorous controls. Those changes were reflected in Directive 2005/60/EC of the European Parliament and of the Council (2) and in Commission Directive 2006/70/EC (3).

2. Analysis

The 4th anti-money laundering Directive is a preventive instrument; its main aim is to protect the Union financial system against money laundering and terrorist financing while minimising the burden on legitimate business.

The main building blocks of the Directive include: identification of customers, proxies, and beneficial owner; ongoing monitoring; obligation to report suspicious transactions; record keeping; supervision and cooperation; staff protection; sanctions.

The Directive had to be transposed into national law by Member States by 26 June 2016.

The adoption of the Directive was a major step forward in improving the existing "anty-money laundering/countering financing of terrorism" (AML/CFT) framework, by 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. It **still represents an advanced standard:** fully in line with international commitments and going beyond them in certain areas (eg. the Directive exceeds FATF standards in covering the gambling sector, cash

[94] http://www.consilium.europa.eu/uedocs/cms_data/docs/pressdata/en/jha/136832.pdf.
[95] http://europa.eu/rapid/press-release_SPEECH-14-2020_fr.htm.
[96] http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2008:210:0001:0011:EN:PDF.

payments in excess of 10 000 EUR, politically exposed persons, identification of beneficial owners, sanctions).

However, **recent game-changers**, including the terrorist attacks and the Panama Papers scandal, have exposed gaps in the regulatory framework. Therefore, in line with the Commission's 2016 Action Plan against terrorist financing, the Commission has proposed targeted amendments to the Directive. Five major problems have been identified as to be addressed in relation to the financing of terrorism:

- Uncoordinated customer due diligence for transactions involving high risk-third countries;
- Suspicious transactions made through virtual currencies;
- Mitigate risks associated with anonymous prepaid instruments;
- Financial Intelligence Units' (FIUs) timely access to – and exchange of – information;
- FIU access to information on the identity of holders of bank and payment accounts.

Adding to this, and as a direct response to the Panama Papers, and also with a view to strengthen **the transparency and the fight against tax evasion** (see Communication COM(2016) 451), the Commission has proposed:

- public access to beneficial ownership information for companies and trusts engaged in commercial or business-like activities;
- access to bank ownership information on a legitimate-interest basis for family or charitable trusts.

The Commission proposal is still being discussed with the co-legislators.

The abovementioned recent game-changers show that money laundering, terrorist financing and organised crime remain significant problems which should be addressed at Union level. Some Member States already voiced their intention to take action in the abovementioned areas. However, uncoordinated action may reduce the good functioning of financial intelligence at EU level, and create gaps or weak spots that can be exploited by criminals and terrorists to channel their funds in and out the EU financial system, thus threatening the good functioning of the Internal Market.

The 4AMLD is an essential element to ensure that harmonised rules allow effective coordination between EU Member States' various competent authorities, and a level playing field for all obliged entities- which are economic actors subject to obligations and sanctions.

The 4AMLD is instrumental in tackling a major challenge: to ensure that the provisions in Member States' laws – and their enforcement – keep pace with evolving trends, developments in technology and the seemingly limitless ingenuity of criminals to exploit any gaps or loopholes in the system.

Support to the policy implementation in the field of AML has also been provided by the security research programme, in both Framework Programme 7[97] and Horizon 2020[98]. Specifically, the FP7 project HEMOLIA ("Hybrid Enhanced Money Laundering Intelligence, Investigation, Incrimination and Alerts"), proposing a new generation AML intelligent multi-agent alert and investigation system, delivered a set of guidelines for the ML fighters on the exchange and use of data.

[97] https://ec.europa.eu/research/fp7/index_en.cfm?pg=security.
[98] https://ec.europa.eu/programmes/horizon2020/en/h2020-section/secure-societies-%E2%80%93-protecting-freedom-and-security-europe-and-its-citizens.

In terms of fundamental rights, the 4AMLD affects mainly: the right to private and family life (Article 7 of the Charter), the protection of personal data (Article 8) and the freedom to conduct a business (Article 16), as it sets out obligations on private entities to file suspicion transaction reports and rules on the collection, storing and access to information on the ultimate beneficial owners of companies, trusts and other types of legal arrangements.

Obliged entities need to retain a series of documents and information for the purpose of preventing, detecting and investigating possible money laundering/terrorist financing. The retention period is a total of 5 (+5 under certain circumstances, where necessary and proportionate). This is in line with the General Data Protection Regulation.

External aspects are essential to the 4AMLD with regard to a number of aspects: regulating the use of anonymous prepaid cards issued outside the Union; designating high-risk third countries for which enhanced customer due diligence is required and, finally, setting out a framework for cooperation with third countries FIUs and supervisory authorities.

The "EU-US Agreement on the Terrorist Finance Tracking Programme"

1. Legal framework

Agreement between the European Union and the United States of America on the processing and transfer of Financial Messaging Data from the European Union to the United States for the purposes of the Terrorist Finance Tracking Program.[99]

2. Analysis

- The Terrorist Finance Tracking Program (TFTP) contains financial transaction data with a link to geographical areas that are particularly at risk of terrorism, both in and outside the EU.
- the Agreement lays down the conditions and safeguards for transfer and processing of financial transaction data from the EU to the US.

As noted in the most recent report on the review of the Agreement,[100] the TFTP remains an important instrument to provide timely, accurate and reliable information about activities associated with suspected acts of terrorist planning and financing. It helps to identify and track terrorists and their support networks worldwide.

The TFTP has provided useful information in several recent terrorist attacks carried out in the EU. This has helped raise awareness of the TFTP among EU authorities, resulting in an increased use of the TFTP by those authorities.

Given the rapidly evolving pattern of terrorist financing, the Commission will analyse the need for complementary mechanisms to the EU-US TFTP to fill any potential gaps (i.e. transactions which are excluded from the EU-US TFTP agreement – notably intra-EU payments in euro – and may not be possible to track otherwise). The Commission will report on its findings during the second half of 2017.

The TFTP provided concrete leads relating to several terrorist suspects, including foreign fighters travelling to or returning from Syria and the support networks facilitating or funding their movements and training. The TFTP also played an important role in the investigations following the terrorist attacks in Paris of 13 November 2015, where it provided EU authorities with more than 900 TFTP-derived leads.

[99] http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2010.195.01.0003.01.ENG&toc=OJ:L:2010:195:TOC#L_2010195EN.01000501.

[100] https://ec.europa.eu/home-affairs/sites/homeaffairs/files/e-library/documents/policies/crisis-and-terrorism/19012017_tftp_report_en.pdf.

Throughout the implementation of the Agreement, Europol played an active role in raising the awareness on the possibilities available under the TFTP by promoting the reciprocity provisions through dedicated campaigns in Member States and initiating requests for searches itself. This has helped raise awareness of added value of the TFTP among EU authorities, resulting in an increased use of the TFTP by those authorities.

The Agreement provides for several safeguards relating to the transfer and processing of personal data, including:

- Data is processed exclusively for the prevention, investigation, detection, or prosecution of terrorism or its financing.
- The TFTP shall not involve data mining or any other type of algorithmic or automated profiling or computer filtering.
- The Provided Data is held in a secure physical environment, stored separately from any other data.
- All searches of Provided Data shall be based upon pre-existing information or evidence which demonstrates a reason to believe that the subject of the search has a nexus to terrorism or its financing.
- Compliance with these safeguards in relation to purpose limitation is subject to monitoring and oversight by independent overseers, including by a person appointed by the European Commission.
- Provided Data should be deleted not later than five years after transfer, unless this data has been the object of a search. In any case, data is not kept longer than necessary to combat terrorism or its financing.
- Any person has the right to enquire whether that person's data protection rights have been respected in compliance with this Agreement.
- Any person has the right to seek the rectification, erasure, or blocking of his or her personal data processed pursuant to the Agreement.
- The implementation of all safeguards is also object of regular joint reviews to be conducted by review teams from the European Union and the United States.[101]

[101] The Commission confirmed in 2017 that the Agreement and its safeguards and controls are properly implemented and that the findings of the previous joint review have been followed up by the US: https://ec.europa.eu/home-affairs/sites/homeaffairs/files/e-library/documents/policies/crisis-and-terrorism/19012017_tftp_report_en.pdf.

III. Organised crime

1. Organised Crime – General

Framework Decision 2008/841/JHA on the fight against organised crime

1. Legal framework

The legal basis of the Framework Decision was former **Article 29, 31(1)(e) and 34(2)(b) of the Treaty on European Union** (current Article 83(1) TFSU.

It was adopted in the framework of **the Hague Programme**[102] 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 its 2004 **Communication**[103], the Commission considered that the facilities available for combating organised crime in the EU needed to be strengthened and stated that it would draw up a Framework Decision to replace Joint Action 98/733/JHA[104].

2. Analysis

The objective of the Framework Decision is to approximate definitions and sanctions for offences of organised crime in the Member States. The main purpose was to encompassing offences typically committed in a criminal organisation in order to address the criminal association angle under which various criminal activities are carried out (instead of addressing those criminal activities separately).

Due to the fact that the outcome of the negotiations was less ambitious than the initial proposal, the Commission, supported by France and Italy, decided to issue a declaration[105] questioning the added value of the instrument from the point of view of achieving the necessary minimum degree of approximation.

It now stems from contacts with the practitioners (the law enforcement and judiciary authorities) and from the research[106] 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. **The Member States continue applying the measures they consider the most useful and suiting their**

---

[102] Communication from the Commission to the Council and the European Parliament of 10 May 2005 – The Hague Programme: ten priorities for the next five years. The Partnership for European renewal in the field of Freedom, Security and Justice (COM(2005) 184 final – OJ C 236 of 24/9/2005).

[103] Communication from the Commission to the Council and the European Parliament on measures to be taken to combat terrorism and other forms of serious crime, in particular to improve exchanges of information (COM/2004/0221 final).

[104] Joint Action 98/733/JHA making it a criminal offence to participate in a criminal organisation in the Member States of the European Union (OJ L 351 of 29/12/1998)

[105] "The Commission considers that the Framework Decision on the fight against organised crime fails to achieve the objective sought by the Commission in relation to Joint Action 98/733/JHA on making it a criminal offence to participate in a criminal organisation in the Member States of the European Union, and in relation to the United Nations Convention Against Transnational Organised Crime, adopted on 15 November 2000, to which the Community has been a party since 29 April 2004. The Framework Decision does not achieve the minimum degree of approximation of acts of directing or participating in a criminal organisation on the basis of a single concept of such an organisation, as proposed by the Commission and as already adopted in Framework Decision 2002/475/JHA on the fight against terrorism. Furthermore, the Framework Decision enables Member States not to introduce the concept of criminal organisation but to continue to apply existing national criminal law by having recourse to general rules on participation in and preparation of specific offences. The Commission is therefore obliged to note that the Framework Decision does not achieve the objective of the approximation of legislation on the fight against transnational organised crime as provided for in the Hague Programme." Council 2005/0003 (CNS).

[106] Study on organised crime carried out in 2015 (*http://bookshop.europa.eu/en/study-on-paving-the-way-for-future-policy-initiatives-in-the-field-of-fight-against-organised-crime-pbHR0614242/).*

purpose. In practice, they continue 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). The Framework Decision's legal standards, e.g. penalty thresholds, are quite low, it is also true that the corresponding provisions (mostly pre-existing) in the majority of the Member States are much more ambitious. For those reasons the research concluded that possible new legislation would not solve the existing problems. Instead, it was suggested that the EU should focus on various soft law measures assisting Member States in the way they apply the Framework Decision in practice.

In July 2016, the Commission issued a report on implementation of the Framework Decision.[107] It concludes that while the Framework Decision has 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 cover participation in a criminal organisation, while a few of them cover additionally the offence of conspiracy in organised crime. No Member States has opted for criminalisation of only the offence of conspiracy in organised crime. Some Member States make the national provisions broader and many provide for measures that are not covered at all by the Framework Decision, e.g. parallel offences tackling specific types of organised groups defined through their objective or *modus operandi*. Another example of national standards going beyond the Framework Decision is seen in basic penalty levels that are higher than envisaged by the Framework Decision.

The objective of enhancing cross-border cooperation through providing comparable minimum standards in relation to offence and sanctions for the offence of organised crime has already been addressed by the pre-existing legislation (the mentioned Joint Action 98/733/JHA and UNTOC[108]) which equipped the Member States with basic common standards. For this reason the **adoption of the Framework Decision had little impact on the national legislation** of the Member States. Overall, it needs to be underlined that none of the mentioned instruments, including the Framework Decision, changed the fact that **the Member States' transposition differs considerably being, at the same time, compatible with the Framework Decision (**due to the vague nature of the provisions of the instrument which allow a wide margin of transposition).

The Framework Decision, as a horizontal tool focusing on the association link, applies to a number of specific offences committed in practice (predicted offences) in line with the national legislation of a particular Member State.

Support to the policy implementation in the field of the fight against organised crime has also been provided by the security research programme, in both Framework Programme 7[109] and Horizon 2020[110]. Specifically, the FP7 projects CAPER ("Collaborative information, Acquisition, Processing, Exploitation and Reporting for the prevention of organised crime"), EKSISTENZ ("Harmonized framework allowing a sustainable and robust identity for European citizens") and HEMOLIA ("Hybrid Enhanced Money Laundering Intelligence, Investigation, Incrimination and Alerts") delivered sets of guidelines for the organised crime fighters.

---

[107] COM(2016)448 final.

[108] 2000 United Nations Convention against Transnational Organised Crime (UNTOC) (Council Decision 2004/579/EC, OJ L 261, 6.8.2004, p. 69).

[109] https://ec.europa.eu/research/fp7/index_en.cfm?pg=security.

[110] https://ec.europa.eu/programmes/horizon2020/en/h2020-section/secure-societies-%E2%80%93-protecting-freedom-and-security-europe-and-its-citizens.

The Framework Decision states in the Preamble that the obligation for the Member States to ensure that the types of conduct related to a criminal organisation as defined (offence of organised crime) in Article 2(a) should be without prejudice to Member States' freedom to classify other groups of persons as criminal organisations, for example, groups whose purpose is not financial or other material gain. The same applies to the Member States' freedom to interpret the term 'criminal activities' as implying the carrying out of material acts.

The Preamble also underlines that the Framework Decision respects the fundamental rights and principles recognised by the Charter of Fundamental Rights of the European Union (in particular Articles 6 and 49). It also states that it is not intended to reduce or restrict national rules relating to fundamental rights or freedoms such as due process, the right to strike, freedom of assembly, of association, of the press or of expression, including the right of everyone to form and to join trade unions with others for the protection of his or her interests and the related right to demonstrate.

The Framework Decision is applicable only to the territory of the EU Member States and there are no specific provisions extending its scope. At the same time, the Framework Decision was adopted in the context of UNTOC that covers a similar scope of criminalisation (*rationae materiae*) in relation to the offence of organised crime for all the signatory countries.

Mutual evaluation procedures foreseen by Joint Action 97/827/JHA of 5 December 1997

1. Legal framework

Joint Action 97/827/JHA of 5 December 1997[111] established a mechanism for evaluating the application and implementation at national level of Union and other international acts and instruments in criminal matters, of the resulting legislation and practices at national level and of international cooperation in the fight against organised crime.

2. Analysis

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.

According to Article 2 of Joint Action 97/827/JHA, the Presidency proposes to delegations in the General Evaluation Council Working Party ("GENVAL) a "specific subject of the evaluation as well as the order in which Member States are to be evaluated". Subsequently, the Member States design experts to be included in a list drawn-up by the Presidency and the programme of the on-the-spot visits is drawn.

The procedure has also been based on informal rules and practices developed over 18 years of experience in mutual evaluations, and on certain procedural arrangements and tentative deadlines endorsed by the GENVAL Working Party[112]. Each round takes usually from 1,5 to 2 years and it is based on detailed questionnaires. GENVAL also agreed to a 18-months

[111] Joint Action 97/827/JHA [111] establishing a mechanism for evaluating the application and implementation at national level of international undertakings in the fight against organized crime (OJ L 344 of 15 December 1997).
[112] Doc. 9154/1/13.

rendez-vous clause to inform on the follow-up to the recommendations, namely actions carried out after the report was adopted.

Currently the seventh round of mutual evaluations (*cybercrime*) is being finalised and the topic of the eight round (*environmental crime with a focus on illegal trafficking of waste and production and handling of dangerous materials*) has been agreed upon in 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) *Eurojust and EJN*.

The main added value of the reports is an overview of national practices which are useful to understand the functioning of the overall system. The discussions serve also as forum to exchange good practices and a political push for improving the way the Member States fight against organised crime.

The issue of fundamental rights has often been addressed in the course of mutual evaluations, depending on the topic of the evaluation.

The external dimension is addressed depending on the need required by the assessed topic.

Prevention of and fight against Crime (ISEC) 2007-2013

1. Legal framework

The legal base for the ISEC programme was Decision No 2007/125/JHA of the Council of 12 February 2007 establishing for the period 2007 to 2013, as part of General Programme on Security and Safeguarding Liberties, the Specific Programme 'Prevention of and Fight against Crime' ("ISEC Decision").

2. Analysis

ISEC had the following general objectives (article 2 of the ISEC Decision):

a) Contribute to a high level of security for citizens by preventing and combating crime, organised or otherwise, in particular terrorism, trafficking in persons and offences against children, illicit drug trafficking and illicit arms trafficking, corruption and fraud.

b) Contribute to the development of the policies of the Union and of the Community (without prejudice to the objectives and powers of the European Community).

Under these general objectives, the specific objectives of the ISEC (article 3(2) of ISEC Decision) were to stimulate, promote and develop:

(a) horizontal methods and tools necessary for strategically preventing and fighting crime and guaranteeing security and public order such as the work carried out in the European Union Crime Prevention Network, public-private partnerships, best practices in crime prevention, comparable statistics, applied criminology and an enhanced approach towards young offenders;

(b) coordination, cooperation and mutual understanding among law enforcement agencies, other national authorities and related Union bodies in respect of the priorities identified by the Council in particular as set out by the Europol's Organised Crime Threat Assessment;

(c) best practices for the protection and support witnesses; and

(d) best practices for the protection of crime victims.

The ISEC 2007-2013 financial allocation was 600 million EUR and was implemented under the direct management mode. Projects were supported by grants awarded by the Commission or via contracts for services concluded following the calls for tenders.

Within the ISEC Decision the following four financing themes were defined:

(a) crime prevention and criminology;

(b) law enforcement;

(c) protection and support to witnesses;

(d) protection of victims.

The following types of actions could be supported (article 4(1) of ISEC Decision):

(a) projects initiated and managed by the Commission with a European dimension;

(b) transnational projects, involving partners in at least two Member States, or at least one Member State and one other acceding or a candidate country;

(c) national projects within Member States, which:

(i) prepare transnational projects and/or Union actions (starter measures);

(ii) complement transnational projects and/or Union (complementary measures);

(iii) contribute to developing innovative methods and/or technologies with a potential for transferability to actions at Union level, at Member States level and/or acceding or a candidate country level.

(d) operating grants for non-governmental organisations pursuing on a non-profit basis objectives of the Programme on a European dimension.

A mid-term evaluation of CIPS was conducted in 2010[113]. An ex-post evaluation of CIPS is ongoing and the final report is expected by the end of 2017.

This legal base was repealed by Regulation (EU) No 513/2014 of the European Parliament and of the Council of 16 April 2014 establishing, as part of the Internal Security Fund, the instrument for financial support for police cooperation, preventing and combating crime, and crisis management.

Without prejudging the final key findings that the ex-post evaluation study should provide by end June 2017, the following preliminary observations can be made at this stage.

ISEC projects were primarily led by public bodies consisting of law enforcement agencies and national authorities, such as ministries of interior, followed by NGOs and universities/research institutes. Activities implemented as part actions grants were mostly focused on awareness-raising and dissemination activities (as a mandatory element of the project) and analytical activities (83%) followed closely by operation cooperation (70%), analytical and training activities (both 60%) and development and transfer of technology and methods (59%).

ISEC responded to an important need for transnational cooperation in the area of prevention and fight against crime. ISEC sought to fill in an important gap by providing funding for practical cooperation between EU Member States in support of EU priorities in the area of prevention and fight against crime, which would not have otherwise been financed by national or other funding. Consulted stakeholders were in agreement that in the context of the financial crisis during the Programme period, transnational cooperation would not have been financed through alternative sources of funding, such as national budgets. Strong EU added value was brought by the transnational partnerships allowing organisations to gain more knowledge and expertise on the subject that they were working on.

The basic acts establishing the Asylum, Migration and Integration Fund (AMIF) and the Internal Security Fund (ISF) for the programming period 2014-2020 contain various

[113] COM(2011)318.

provisions that refer to compliance with the Charter of Fundamental Rights of the European Union.

Regulation (EU) No 513/2014 of the European Parliament and of the Council of 16 April 2014 establishing, as part of the Internal Security Fund, the instrument for financial support for police cooperation, preventing and combating crime, and crisis management and repealing Council Decision 2007/125/JHA ('ISF Police Regulation') has the following provisions:

- Recital 19: "The Instrument should be implemented in full respect for the rights and principles enshrined in the Charter of Fundamental Rights of the European Union and for the Union's international obligations."
- Recital 20: "Pursuant to Article 3 of the Treaty on European Union (TEU), the Instrument should support activities which ensure the protection of children against violence, abuse, exploitation and neglect. The Instrument should also support safeguards and assistance for child witnesses and victims, in particular those who are unaccompanied or otherwise in need of guardianship."
- Article 3(5): "Actions funded under the Instrument shall be implemented in full respect for fundamental rights and human dignity. In particular, actions shall comply with the provisions of the Charter of Fundamental Rights of the European Union, Union data protection law and the European Convention for the Protection of Human Rights and Fundamental Freedoms (ECHR). In particular, wherever possible, special attention shall be given by Member States when implementing actions to the assistance and protection of vulnerable persons, in particular children and unaccompanied minors.

Council Decision 2002/348/JHA concerning security in connection with football matches with an international dimension as amended by Decision 2007/412/JHA of 12 June 2007

1. Legal framework

The Council Decision was issued at a time when it was felt that - as a result of various international and European competitions and large numbers of travelling supporters - football was becoming highly international in scale, and that international scale made it necessary to approach security in connection with football matches in a way extending beyond national borders. In particular, for the purposes of preventing and combating football-related violence, it was felt important to exchange information, so that the competent police authorities, and the authorities in the Member States, could make proper preparations and provide an appropriate response.

The legal basis of the Decision was Article 29, Article 30(1)(a) and (b) and Article 34(2)(c) of the Treaty on European Union.

2. Analysis

Council Decision 2002/348/JHA of 25 April 2002 requires that a National Football Information Point (NFIP) in each Member State is tasked with exchanging relevant information and developing cross-border police cooperation. Tactical, strategic and operational information can be used by the NFIP itself or is forwarded to the relevant authorities or police services. Contacts between the police services of the different countries involved in an event are coordinated and, if necessary, organised by the NFIP. A secured website for NFIPs (www.nfip.eu) disseminates information and advice on available legal and other options concerning safety and security in connection with football matches.

The NFIP coordinates the processing of information on high-risk supporters with a view to preparing and taking the appropriate measures to maintain law and order when a football event takes place. Such information includes, in particular, details of individuals actually or potentially posing a threat to law and order and security.

According to Council Decision 2007/412/JHA of 12 June 2007 amending Decision 2002/348/JHA, information should be exchanged on the forms contained in the appendix to the Football Handbook.

The Football Handbook is annexed to Council Resolution 2006/C 322/01 and provides examples of how the police should cooperate at international level in order to prevent and control violence and disturbances in connection with football matches. The content consists in particular of recommendations concerning: (i) information management by police forces; (ii) the organisation of cooperation between police forces; (iii) a checklist for media policy and communication strategy (police/authorities). The Football handbook, originally introduced in 1999 was updated by the Council Resolutions of 4 December 2006, 3 June 2010 and 29 November 2016 provides a template for this exchange of information.

In addition, Council resolution 2003/C 281/01 of 17 November 2003 on the use by Member States of bans on access to venues of football matches with an international dimension invites EU countries to consider banning individuals previously guilty of violence at football matches from football stadiums, including the possibility of bans extending to other EU countries, backed up by penalties for non-compliance.

In a 2014 Decision, the European Commission and the Union of European Football Associations (UEFA) agreed to strengthen cooperation and dialogue, including actions to step up efforts against violence at football stadiums. The two parties hold senior-level bilateral meetings at least yearly to review progress.

An informal expert network, the think tank on major sports events, follows and coordinates these issues as part of the Law Enforcement Working Party of the Council. It is understood anecdotally that the NFIPs are routinely used by the relevant Member State's authorities and that France, during the organisation of the EURO 2016 football cup tournament stressed at several occasions the importance of the NFIP network in order to exchange valuable security information between EU Member States. It would therefore appear that the objectives and instruments are still adapted to current needs.

The Commission contributed to the preparation of the EURO 2016 football tournament through explosive detection equipment trainings and tests.

As regards the personal data which can be exchanged in the scope of the Decision, "*with a view to preparing and taking the appropriate measures to maintain law and order when a football event takes place*", and considering that "*such exchange may in particular involve details of individuals actually or potentially posing a threat to law and order and security*", the Council Decision specifically refers to the Convention No 108 of the Council of Europe of 28 January 1981 for the protection of individuals with regard to automatic processing of personal data and to Recommendation No R (87)15 of the Committee of Ministers of the Council of Europe of 17 September 1987 regulating the use of personal data in the police sector (Article 3 paragraph 3).

Numerous bilateral contacts take place between third countries and EU Member States for the preparation of international tournaments or football matches and that lessons learnt are exchanged (e.g. for the FIFA World Cup in Brazil and the upcoming FIFA World Cup in Russia in 2018).

2. Money laundering, asset recovery and financial crime

Regulation (EC) No 1889/2005 on controls of cash entering or leaving the Community

1. Legal framework

Regulation (EC) No 1889/2005 of the European Parliament and the Council of 26 October 2005 on controls of cash entering or leaving the Community[114] (further: 'the Cash Control Regulation' or 'CCR') is based on Articles 33 (Customs cooperation) and 114 (internal market) TFEU.

2. Analysis

The CCR complements the existing anti-money laundering and anti-terrorist finance framework of the Union by laying down a system of controls on natural persons entering or leaving the Union. Natural persons carrying 10 000 Euro or more in currency or bearer-negotiable instruments are obliged to make a declaration with competent authorities of the Member State through which they are entering or leaving the Union.

The CCR has been the subject of extensive ex-post evaluations in 2010[115] and in 2015/2016[116]. Both evaluations concluded that, overall, the instrument performed satisfactorily but that, nevertheless, some weaknesses were detected and the passage of time and the evolution of international standards (Financial Action Task Force) and best practices in addition to Member State feedback made a comprehensive revision necessary. This revision process made use of an Impact Assessment[117] to formulate policy options and culminated on 21 December 2016 in the adoption of a Commission proposal for a new Regulation on controls on cash entering or leaving the Union[118]. The proposal aims to address identified weaknesses in the following areas: a) the definition of 'cash', which is proposed to also include precious commodities and prepaid cards; b) exchange of data between competent authorities, which is streamlined and harmonised; c) enabling controls on cash entering or leaving through other channels than carried by a natural person (e.g. in post of freight); and d) enabling competent authorities not only to register sub-threshold amounts of cash where there are indications of criminal activity but also to temporarily retain cash by administrative decision.

The CCR laid down a harmonised system of controls applicable to cash entering or leaving the Union. Its implementation gave rise to data exchange, a coordinated approach to the phenomenon and the organisation of controls, taking into account the specificities of the internal market and its freedoms. On an individual basis, Member States could not have sufficiently achieved such harmonised approach for cash crossing the external border. At the same time, they remain competent to organise intra-community controls provided these respect the provisions of Art. 63 TFEU.

The CCR (and the proposal which has been introduced) is in line with and contributes to other Union policies, notably:

- the *European Agenda on Security*[119], which emphasises the importance of the fight against terrorism and organised crime and highlights the importance of information-sharing between competent authorities, in particular FIUs;
- the *Action Plan for strengthening the fight against terrorist financing*, which lists a number of policy and legal initiatives (including this proposal) to be taken as part of a comprehensive approach in this area; and

[114] O.J. No L 309 of 25.11.2005.
[115] Report from the Commission to the European Parliament and the Council on the application of Regulation (EC) No 1889/2005 on controls of cash entering or leaving the Community pursuant to Art. 10 of that regulation. Cf. http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52010DC0429&from=EN
[116] See Annex 2 to the Impact Assessment accessible at https://ec.europa.eu/taxation_customs/sites/taxation/files/swd_2016_470_en.pdf.
[117] Cf. footnote 3.
[118] COM(2016) 825 final: https://ec.europa.eu/taxation_customs/sites/taxation/files/com_2016_825_en.pdf.
[119] C (2015) 185 final.

- the Commission's proposal for a Directive of the European Parliament and of the Council on combating terrorism and replacing Council Framework Decision 2002/475/JHA on combating terrorism[120], which includes provisions on criminal sanctions for people or entities who provide material support to terrorism.
- The principle of the free movement of capital, which prohibits restrictions on payments and capital movements between Member States and third countries without prejudice to non-discriminatory measures justified on grounds of public policy and public security.

The measures under the CCR potentially impact the rights which are enshrined in the following Articles of the Charter of Fundamental Rights of the EU (hereinafter: 'CFR'):

- respect for private life, home and family life (Article 7 CFR);
- the protection of personal data (Article 8 CFR);
- the freedom to conduct a business (Article 16 CFR); and
- the right to property (Article 17 CFR).

The measures laid down under the CCR strike a careful balance between the rights in question and the legitimate interests of society by taking an approach that is efficient (i.e. achieves the objective) but affects the rights as little as possible.

The CCR lays down provisions regarding the transfer of cash across the external border. The control policies in place have a potentially direct impact on security (in terms of the fight against AML/TF in third countries. Overall, the CCR implements the Financial Action Task Force's recommendation 32, which serves as a *de facto* global standard regarding controls on cross-border movements of cash.

The ARO Council Decision: cooperation between Asset Recovery Offices

1. Legal framework

Council Decision 2007/845/JHA of 6 December 2007 concerning cooperation between Asset Recovery Offices of the Member States in the field of tracing and identification of proceeds from, or other property related to crime[121].

2. Analysis

The Decision requires 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 and other crime related property, in view of their possible freezing and confiscation in the course of criminal or other (civil or administrative) proceedings. Member States may designate a maximum of two AROs;
- ensure that their AROs cooperate with each other by exchanging information and best practices, and that this cooperation is not hampered by the status of the AROs (which may be administrative, law enforcement or judicial authorities);
- upon request of another ARO, provide the requested information under the conditions and within the time limits indicated in Framework Decision 2006/960/JHA ("the Swedish initiative"). The Decision also enables an ARO to send relevant information spontaneously (i.e. without a prior request) to other AROs;

[120] COM (2015) 625 final.
[121] http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32007D0845&qid=1488381986786&from=EN.

- ensure that the information exchanged is treated according to the established rules of data protection (normally those of the receiving Member State).

The Decision initially aimed at providing 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). The deadline for transposition was 18 December 2008. Not all the Member States implemented the Council Decision swiftly. The Commission implementation report issued in 2011 emphasised that, two years after the expiry of the transposition deadline, five Member States still had not designated their ARO.

The 2011 Commission report notes that the Council Decision did not seem to present relevant shortcomings. However, it identified a number of challenges for the AROs, including limited resources, no access to all relevant databases, the lack of a secure information exchange system, little involvement in the management of frozen assets and limited access to judicial information on freezing and confiscation (e.g. information on whether assets were frozen in the cases where the AROs identified assets, or judicial statistics).

The situation has evolved over the years:

- Since 2015 all Member States have designated their AROs.
- SIENA has become the preferred secure information exchange system of the AROs (21 AROs connected).
- The operational exchanges between AROs have drastically increased (from 475 exchanges in SIENA in 2012 to over 3700 in 2016).
- The regular exchange of best practices in the meetings of the ARO Platform (co-chaired by the Commission and Europol) resulted in an enhanced awareness on how each ARO functions and what information it can (or cannot) provide.
- The development in the ARO Platform of common effectiveness indicators, their assessment through informal visits by peer experts and the subsequent discussions in the ARO Platform (the AROs in 10 Member States have been reviewed) brought along a shared vision on how AROs should ideally function to perform their tasks in an optimal way.
- New centralised databases have been established, or may soon be established, in accordance with the EU anti-money laundering requirements (centralised bank account and beneficial ownership registries).
- Asset Management Offices, in charge of managing the assets frozen in view of confiscation, are being set up in accordance with the confiscation Directive.
- The AROs are increasingly identified as the national central contact points, handling outgoing and incoming asset tracing requests, which facilitate, through their enhanced cooperation, the fastest possible EU-wide tracing of assets derived from crime.
- There is an increased awareness of the need for effective asset tracing as a necessary condition to increase the number and value of confiscated assets. For example, after establishing its ARO in 2013, Romania has frozen assets for an average of EUR 500 million per year over the last three years.
- The replies to the requests for information are increasingly detailed and comprehensive. It is estimated that in 2016 46% of the requests exchanged in the Union resulted in a positive identification of assets. The sharp increase in the exchanges and the enhanced accuracy of the intelligence information provided will likely result, in time, in more confiscations.

In light of these developments, stakeholders have called for enhancing the capabilities of the AROs to handle an increasing number of asset tracing requests and to consider granting

additional powers (e.g precautionary freezing powers in order to avoid the dissipation of the assets identified) and access to additional databases to the AROs. Better clarity is needed on the provisions on the exchange of information between AROs (including an obligation to exchange information through SIENA), as well as between AROs and other national authorities. Together with legal provisions, the EU financial support might be an important factor underpinning these developments. The EU financial support would allow funding projects to strengthen the effectiveness of the AROs (e.g. development of a new case management system, specialised training for ARO investigators, IT solutions to link up the ARO to databases).

The 2007 Council Decision provided added value by establishing national AROs and facilitating their cooperation. The ARO Platform helped establishing an integrated network of AROs by providing a regular forum for the exchange of best practices, strategic discussions and the development of effectiveness indicators. The EU funding programmes in the area of Home Affairs have financed several projects on strengthening national AROs and their practices, exchanging best practices, specialised training in asset recovery, a White Book on AROs, etc.

Almost all the designated AROs include the CARIN contact points in the Member States.

The Council Decision (Article 5) includes provisions on data protection, notably on the use of the data by the receiving Member State. The personal data processed in the context of the application of this Decision "shall be protected in accordance with the Council of Europe Convention of 28 January 1981 for the Protection of Individuals with regard to Automatic Processing of Personal Data, and, for those Member States which have ratified it, the Additional Protocol of 8 November 2001 to that Convention, regarding Supervisory Authorities and Transborder Data Flows. The principles of Recommendation No R(87) 15 of the Council of Europe Regulating the Use of Personal Data in the Police Sector should also be taken into account when law enforcement authorities handle personal data obtained under this Decision."

In terms of protection of fundamental right, the relevant legal framework to apply should be Framework Decision 2008/977/JHA on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters. However, there is no such reference in the Council Decision, since the Framework Decision 2008/977/JHA was adopted one year after the adoption of the Council Decision.

The Council Decision only covers the exchange of information between EU AROs. However, some representatives of non-EU authorities regularly attend the meetings of the ARO Platform. The AROs cooperate with asset recovery agencies outside the European Union on a bilateral basis, mostly through the contact points of the CARIN network of asset recovery practitioners (financially supported by the Commission), which can assist in the identification and tracing of assets in over 117 countries and jurisdictions.

Among possible avenues for improvement, the analysis identified a need to enhance the capabilities of the AROs to handle an increasing number of asset tracing requests. Granting them additional powers (e.g. precautionary freezing powers in order to avoid the dissipation of the assets identified) and access to additional databases to the AROs could be useful. More clarity seems to be needed on the provisions on the exchange of information between AROs (including an obligation to exchange information through SIENA), as well as between AROs and other national authorities.

The confiscation Directive: minimum rules on the freezing and confiscation of criminal assets

1. Legal framework

Directive 2014/42/EU on the freezing and confiscation of the instrumentalities and proceeds of crime in the European Union[122].

The Directive is based on Article 82(1) and 83(1) TFEU.

2. Analysis

The Directive aims at attacking the financial incentive which drives most serious and organised crime, at protecting the EU economy against infiltration and corruption by criminal groups, and at returning criminal assets to governments and citizens. In particular, the Directive:

- Lays down clearer and more efficient rules on confiscation of assets which are not directly linked to a specific crime, but which clearly result from similar criminal activities by the convicted person (extended confiscation).
- Strengthens rules on confiscation where assets have been transferred from the suspect to a third party who should have realised that it is a result of crime (third-party confiscation).
- Enables confiscation of criminal assets where a criminal conviction is not possible because the suspect is permanently ill or has fled (limited non-conviction based confiscation).
- Ensures that competent authorities, like prosecutors, can temporarily freeze assets that risk disappearing if no action is taken, subject to confirmation by a court (precautionary freezing).
- Allows financial investigations on a person's assets to be continued after a criminal conviction, where the relevant confiscation orders could not be fully executed (effective execution).
- Requires Member States to manage frozen assets so that they do not lose economic value before they are eventually confiscated (asset management).
- Ensures that actions taken to freeze and confiscate assets are backed by strong protections of fundamental rights (safeguards).

The deadline for transposition was 4 October 2016. Only 8 Member States notified to the Commission their legislation fully transposing the Directive by the deadline. Letters of formal notice were sent to 18 Member States in November 2016. By end February, 14 Member States notified to the Commission full transposition of the Directive.

The Directive was adopted recently, is still being transposed by the Member States and its provisions have not displayed their full effects yet.

According to the Directive (Article 13) the Commission shall issue by 4 October 2018 a report assessing the impact of existing national law on confiscation and asset recovery.

According to the Directive the freezing and confiscation of the proceeds of crime is generally based on a criminal conviction[123]. 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, illness or absconding 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, IE, IT, BG, SI, SK). When adopting the confiscation Directive, 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. Once the Commission delivers this report, it might

[122] http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32014L0042&rid=1.

[123] Except for the cases where a criminal conviction cannot be reached due to the illness or absconding of the suspect or accused person. In these cases the Directive enables confiscation even in the absence of a criminal conviction.

pave the way to the possible introduction of new EU measures on non-conviction based confiscation.

The Directive establishes a new legal EU framework for confiscation of the proceeds from serious and organised crime. It simplifies existing rules and fills gaps which have benefited persons convicted and suspected of crime until now. A higher level of harmonisation of the national freezing and confiscation measures will contribute to facilitate the mutual recognition of freezing and confiscation orders in the Union.

The Directive has been an opportunity for some Member States to substantially amend their criminal legislation, sometimes going beyond the provisions of the Directive. Several Member States have introduced provisions on non-conviction based confiscation, in addition to the cases already covered by the Directive.

The Directive also provided Member States with a strong incentive to strengthen their capacity to manage frozen assets in view of their confiscation. As a result, centralised Asset Management Offices have been set up in some Member States. The establishment of centralised Asset Management Offices is indicated in the Directive as one possible model.

Framework Decision 2005/212/JHA is entirely replaced by the Directive, except for the provision enabling confiscation for all offences punishable with imprisonment for at least one year. This provision could not be replaced due to the narrower scope of the Directive, which due to its legal basis cannot apply to all crimes, but applies only to the Eurocrimes listed in Art. 83 TFEU.

According to the Commission implementation report on Framework Decision 2005/212/JHA[124], all Member States that notified their legislation did enable confiscation for all offences punishable with imprisonment for at least one year. In some cases Member States enabled confiscation for all criminal offences (all crimes approach).

Except for this provision, Framework Decision 2005/212/JHA applies only to the Member States not participating in the Directive (Denmark and the United Kingdom). According to the Commission implementation report, Denmark complies almost fully with it (except for some minor provisions), while the United Kingdom had not notified to the Commission its transposing measures yet.

The Directive is also closely linked with the EU legislation on the mutual recognition of freezing and confiscation orders in the European Union (Framework Decisions 2003/577/JHA and 2006/783/JHA). In order to align such legislation with the provisions introduced by the Directive, the Commission proposed in December 2016 a Regulation on the mutual recognition of freezing and confiscation orders in the European Union. By enabling a swift execution of freezing and confiscation orders in other Member States without cumbersome formalities, the proposed Regulation will improve the fight against organised crime groups, which often acquire assets in several Member States.

The Directive (Article 8) includes extensive provisions on the safeguards which are necessary to protect fundamental rights such as the right to property and the right to a fair trial. Following a request by the European Parliament, the Fundamental Rights Agency (FRA) also issued an opinion on the Commission proposal in December 2012.

The Directive only applies to the Member States. Cooperation with third countries takes place under the mechanisms of specific conventions (eg Council of Europe, UN) and mutual legal assistance proceedings. In order to trace the relevant assets, informal networks of contact points such as CARIN play an important role. However, the Directive provisions are increasingly taken as a reference by neighbouring countries amending their legislation, such as those in the Western Balkans or Ukraine.

[124] COM(2007) 805 final of 17.12.2007.

It is too early to assess whether there is a need to amend the Directive. The Directive had to be implemented into national legislation by 4 October 2016, therefore the focus remains currently on its implementation.

Mutual Recognition of freezing and confiscation orders

1. Legal framework

The confiscation of assets generated by criminal activities is a very efficient tool in the fight against crime, as it deprives criminals from the proceeds of their crime. Freezing and confiscation of assets is also an important tool to combat terrorist financing as confiscation of assets disrupts the sources of revenue of terrorist organizations.

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. The proposed Regulation[125] on the mutual recognition of freezing and confiscation orders is part of this package.

The proposed Regulation, once adopted, will replace and complement the current legal framework for the recovery of criminal assets within the EU (Council FD 2003/577/JHA of 22.7.2003 and Council FD 2006/783/JHA of 6.10.2006) which does not respond effectively to the challenge of terrorists and criminals hiding their assets in other Member States.

2. Analysis

The proposed Regulation will:

- offer one single legal instrument for the recognition of both freezing and confiscation orders in other EU countries, simplifying the current legal framework. The Regulation would apply immediately in all Member States;
- widen the scope of the current rules on cross-border recognition. It would cover mutual recognition of all types of freezing and confiscation orders issued in the framework of criminal proceedings including confiscation of other persons' property, such as family members of a criminal and confiscation in cases where the criminal is not convicted e.g. due to escape or death.
- ensure a speedy and efficient execution of freezing and confiscation orders thanks to clear deadlines, standard forms and an obligation of competent authorities to communicate with each other;
- ensure that victims' rights to compensation and restitution are respected.

Discussions with Member States started in Council on 13 January 2017.

Directive 2014/62/EU on the protection of the Euro and other currencies against counterfeiting by criminal law (Euro Counterfeiting Directive)

1. Legal framework

Directive 2014/62/EU on the protection of the Euro and other currencies against counterfeiting by criminal law and replacing Framework Decision 2000/383/JHA.

This Directive replaced Framework Decision 2000/383/JHA following the introduction of the Euro. It supplements and facilitates the application of the Geneva Convention. The Geneva Convention is the International Convention for the Suppression of Counterfeitung Currency agreed on 20 April 1929 whereby states agree to criminalise acts of currency counterfeiting. It remains the principal international agreement on currency counterfeiting.

[125] COM(2016) 819 final.

The Directive was adopted on the legal basis for judicial cooperation in criminal matters, Article 83(1) (minimum rules for so-called euro-crimes).

The Commission Communication "Towards an EU Criminal Policy: Ensuring the effective implementation of EU policies through criminal law" is an important policy compass for criminal law instruments to be developed on the basis of the Lisbon Treaty. The Communication refers explicitly to the protection of the euro against counterfeiting through criminal law in order to strengthen the public's trust in the security of means of payment.[126]

2. Analysis

Since its introduction as a currency, the Euro has been targeted by organised crime groups active in money counterfeiting. Counterfeiting of the euro has caused financial damage of at least EUR 500 million and is apt to undermine the trust in the authenticity of the common currency. It is in the interests of the Union to take effective and coordinated measures to protect its currency (and other currencies) against counterfeiting.

The general objectives of the Directive are to prevent counterfeiting of the euro and other currencies by strengthening the criminal law protection and by strengthening cross-border judicial and law enforcement cooperation, in full compliance with the Charter of Fundamental Rights of the EU, and to keep and strengthen the trust in the genuine character of the single European currency and other currencies

More specifically, the Directive aims at

- To appropriately increase effectiveness and deterrence in relation to counterfeiting (production and distribution) and eliminate incentives for forum shopping in some Member States;
- To facilitate the proportionate application of the European Arrest Warrant in relation to currency counterfeiting (production and distribution);
- To facilitate cross-border investigations in relation to the counterfeiting offences and to reduce delays in processing cooperation requests;
- To strengthen the prevention of counterfeiting and circulation of counterfeit notes and coins by increasing the possibility of detecting notes and coins by a timely application of authentication procedures.

The measure is expected to achieve its objectives by a combination of the following elements:

- Common minimum rules on
  - definition of offences
  - sanctions (e.g. maximum penalty of at least eight years for distribution. (specific objective A and B)
  - liability of and sanctions for legal persons
- the possibility to use certain investigative tools in currency counterfeiting investigations(specific objective C)
- the possibility to transmit the seized euro counterfeits also during judicial proceedings to the National Analysis Centres(specific objective D)
- Collection of data on the number of counterfeiting offences, of the persons prosecuted and those convicted, and share these data with the Commission (statistics).

The transposition period of the Directive ended on 23 May 2016. The Commission is now in the process to perform the necessary transposition checks and, if need be, launch infringement procedures in accordance with the TFEU. Moreover, Member States are obliged – according

[126] COM(2011)573 final.

the Directive – to submit statistical data every two years to the Commission. It is therefore too early to assess the effectiveness of the new European law instrument.

The euro is the Union currency and as such essential to the financial interests of the Union. It needs to be protected in a coherent manner throughout Member States[127]. This European dimension requires that investigation cycles are not interrupted at national borders and that sanction levels are at the same level, wherever in the European Union the crime is committed. The added value of EU-action is particular palpable in the following areas:

- *Sufficient deterrence in all Member States;*
- *equal priority levels with law enforcement authorities in the MS;*
- *No forum shopping for criminals;*
- *Effective cross border investigations using the same investigation tools;*
- *Identifying counterfeits and preventing them from further circulation.*

The Directive is part of a larger legal framework consisting also of administrative[128] and training measures:
The Pericles 2020 programme was established by the Regulation 331/2014[129] (exchange, technical assistance and training cross-borders). for authorities, banks and others involved in combating euro counterfeiting – both in the euro area, in EU countries outside the euro area and in third countries. A mid-term-evaluation is being conducted by the Commission. The results of the first Pericles Programme can be found in the final report of the evaluation of the Pericles programme.

Support to policy implementation in the field of counterfeiting is also provided by the Horizon 2020 Research and Innovation Framework Programme. The project ANDRUPOS (Automatic non-destructive recognition of used printing techniques on substrates), which is foreseen to be launched in 2017, will explore the automated authentication of printing techniques, printers and paper sources, to improve the detection of counterfeiting and fraud.

---

[127] See Communication from the Commission of 26.5.2011 "On the protection of the financial interests of the European Union by criminal law and by administrative investigations - An integrated policy to safeguard taxpayers' money (COM(2011) 293 final), and the Proposal for a Directive of the European Parliament and of the Council on the fight against fraud to the Union's financial interests by means of criminal law, COM(2012) 363 final.

[128] Council Regulation (EC) No 974/98 of 3 May 1998 on the introduction of the euro, OJ L 139, 11.05.1998, pp 1-5, Article 12 of this regulation; obliges the Member States which have adopted the euro to ensure adequate sanctions against counterfeiting and falsification of euro notes and coins; Council Regulation (EC) No 1338/2001 of 28 June 2001 laying down measures necessary for the protection of the euro against counterfeiting, updated through Council Regulation 44/2009 of 18 December 2008. It regulates how euro notes and coins can be uttered in such a manner as to protect them against counterfeiting. Furthermore, issues such as gathering and accessing technical and statistical data relating to the counterfeit notes and coins, the examination of counterfeit notes and coins by the National Analysis Centres and obligations of credit institutions and centralisation of information at national level are addressed; OJ L 181, 4.7.2001, pp 6-10; Decision of the European Central Bank of 16 September 2010 on the authenticity and fitness checking and recirculation of euro notes (ECB/2010/14); OJ L 267, 9.10.2010, p. 1–20; Provisions of the decision were almost wholly replaced by decision of the Central Bank 2012/507/EU, OJ L 253, 20.9.2012, p. 19–31; Regulation (EU) No 1210/2010 of the European Parliament and of the Council of 15 December 2010 concerning authentication of euro coins and handling of euro coins unfit for circulation; Council Regulation (EC) No 2182/2004 of 6 December 2004 concerning medals and tokens similar to euro coins, amended by Council regulation (EC) No 46/2009 of 18 December 2008; , OJ L 339, 22.12.2010, p. 1–5

[129] Targeted actions for exchange, assistance and training of law enforcement agents to establish closer professional ties for a more efficient fight against euro counterfeiting are financed by the Union through the Pericles programme, which was established by Council Decision 2001/923/EC of 17 December 2001[129], and succeeded by Regulation (EU) No 331/2014 of the European Parliament and of the Council of 11 March 2014, OJ L 103, 5.4.2014, p. 1–9.

The Directive refers to the Charter of Fundamental rights and notably to the right to liberty and security, the respect for private and family life, the freedom to choose an occupation and the right to engage in work, the freedom to conduct a business, the right to property, the right to an effective remedy, and to a fair trial, the presumption of innocence and the right of defence, the principles of legality and proportionality of criminal offences and penalties, the right not to be tried or punished twice in criminal proceedings for the same offence (recital 27).

The Directive also refers to the effective but proportionate level of sanctions, to be provided for by the Member States. Currency counterfeiting is traditionally a crime subject to high sanctions in the Member States (recitals 15, 16 and 17). This is justified by the serious nature and the impact of the crime on citizens and society and businesses. In particular the euro is the single currency for 330 million people in the euro zone and the second most important international currency.

An impact assessment accompanied the proposal. It showed that dissuasive sanction levels and effective investigation tools in all Member States, as well as jurisdiction over the criminal offences contribute to protecting the fundamental rights of the victims of euro counterfeiting. This is balanced by the defence and procedural rights of the perpetrators, to be implemented and applied appropriately at Member State level.

Counterfeit Euro are produced in third countries to a considerable extent. Moreover, some third countries use the Euro as a currency. The Directive covers these external dimensions:

- Recital 26: the conclusion of agreements to protect the Euro with third countries using the Euro as currency should be pursued.
- Article 8: Member States shall take the necessary measures to establish their jurisdiction over offences committed outside its territory (subject to certain conditions).

In this context, it should be noted that by March 2016 the Geneva Convention of 1929 protecting currencies against counterfeiting has been signed by 83 parties and all EU Member States are contracting countries.

The Pericles Programme funds are also available to third countries.

Funds transfer regulation – FTR2 Regulation (EU) 2015/847 of the European Parliament and of the Council of 20 May 2015 on information accompanying transfers of funds and repealing Regulation (EC) No 1781/2006

1. Legal framework

Art 114 TFEU (internal market harmonisation).

The Regulation was to a large extent based on Special Recommendation VII on wire transfers adopted by the Financial Action Task Force (FATF) and aims to ensure that this international standard is transposed uniformly through the Union and, in particular, that there is no discrimination between national payments within a Member State and cross-border payments between Member States.

2. Analysis

The Funds Transfers Regulation lays down rules applicable to all transfer of money in the EU, requiring payment service providers to send information on the payer throughout the payment chain for the purposes of prevention, investigation and detection of money laundering and terrorist financing.

In order to enhance traceability, the Regulation imposes the following main requirements:

- include information on the payee;

- clarify that credit or debit cards, or mobile telephone or any other digital or IT device become subject to the provisions of the regulation if they are used to transfer funds person to person. In addition, clarify that below EUR 1 000, in the case of fund transfers outside the EU, a lighter regime of non-verified information on the payer and the payee applies (as opposed to possible exemptions from scope as in Regulation (EC) No 1781/2006);
- impose a requirement to verify the identity of the beneficiary (where not previously identified) for payments originating outside the EU and where the amount is more than EUR 1 000. With regard to the PSP of the payee and the intermediary payment service providers (PSP), an obligation to establish risk-based procedures for determining when to execute, reject or suspend a transfer of funds which lacks the required information and to determine appropriate follow-up action;
- with regard to data protection, align the requirements of record keeping of the information with the FATF standards;
- with regard to sanctions, reinforcement of sanctioning powers for competent authorities and a requirement to coordinate actions when dealing with cross-border cases; a requirement for sanctions imposed for breaches to be published; and a requirement to establish effective mechanisms to encourage reporting of breaches of the provisions of the Regulation.

The Regulation enters into force in June 2017. It repealed and replaced a similar act which needed updating to newer international standards. As such, the regulation can be considered adapted to current needs.

In line with new FATF Recommendation 16 on "wire transfers" and the accompanying Interpretative note, the changes implemented by the new act are aimed at addressing areas where gaps in transparency still remain.

A current problem in the passage from the FTR1 to FTR2 concerns a specific situation of transfers of funds between some Member States and their dependent territories, which do not form part of the territory of the European Union. In order to avoid treating these dependent territories as third countries, under FTR1 Member States could seek Commission authorisation to conclude agreements for such transfers of funds to be treated as transfers of funds within the Member States concerned. The Commission received three applications, respectively from the UK, Denmark and France on this matter, all solved positively. To keep the current situation and authorizations in place, those Member States have to request again authorisation, but have not done so yet.

The regulation is an essential element to ensure that harmonised rules allow effective coordination and a smooth procedure for an essential economic operation: transfer of monetary value. As such, it is an essential element of the internal market, but with a strong security component. It is also an ancillary act to the fourth Anti-Money Laundering Directive. As a consequence of the FTR2, intra-Union transfers of funds are assimilated to domestic/national transfers of funds.

Support to policy implementation in this area has also been provided by the security research programme. The project HEMOLIA[130] (Hybrid Enhanced Money Laundering Intelligence, Investigation, Incrimination and Alerts), which was funded under the 7th Research and Innovation Programme, specifically addressed money transfers and the detection of money laundering. The project developed an innovative anti-money laundering intelligent multi-agent alert and investigation system, which supports banks, law enforcement agencies and other relevant actors in the fight against money laundering, financial crime and fraud.

[130] http://www.hemolia.eu/.

The FTR2 seeks in particular to ensure protection of personal data (Article 8 of the Charter) as regards the collection, storage, transfer and access to personal data of the payer. The Preamble underlines that "personal data collected for the purpose of complying with this Regulation should not be further processed in a way that is incompatible with Directive 95/46/EC". It also strictly prohibits further processing of personal data for commercial purposes.

As regards transfer of personal data to a third country which would not ensure an adequate level of protection in accordance with Article 25 of Directive 95/46/EC, the Regulation provides that it should be permitted subject to the application of adequate safeguards in the jurisdictions located outside the Union.

In addition, recognising that it may not be possible in criminal investigations to identify the data required or the individuals involved in a transaction until many months, or even years, after the original transfer of funds, the Regulation provides that it "is appropriate to require payment service providers to keep records of information on the payer and the payee for a period of time for the purposes of preventing, detecting and investigating money laundering and terrorist financing." However, safeguards are foreseen; "That period should be limited to five years, after which all personal data should be deleted unless national law provides otherwise."

If necessary for the purposes of preventing, detecting or investigating money laundering or terrorist financing, Member States should be able to allow or require retention of records for a further period of no more than five years, without prejudice to national criminal law on evidence applicable to ongoing criminal investigations and legal proceedings "after carrying out an assessment of the necessity and proportionality of the measure".

Under the FTR2, international transfers of funds, i.e. either from third countries into the Community or from the Community to third countries, have to be accompanied by complete information on the payer. By contrast, transfers of funds within the Union shall only be required to be accompanied by the account number of the payer (or a unique identifier to be traced back to the payer). This simplified regime amounts to assimilating intra-Union transfers of funds to domestic/national transfers of funds.

High-risk third countries: delegated act Commission Delegated Regulation (EU) 2016/1675 of 14 July 2016 supplementing Directive (EU) 2015/849 of the European Parliament and of the Council by identifying high-risk third countries with strategic deficiencies

1. Legal framework

The legal basis is Article 9(2) of the 4th anti-money laundering directive (AMLD), Directive (EU) 2015/849.

2. Analysis

The delegated act sets out the list of third-country jurisdictions which have strategic deficiencies in their anti-money laundering and countering the financing of terrorism regimes that pose significant threats to the financial system of the Union.

Based on this list, obliged entities have to apply enhanced customer due diligence measures when establishing business relationships or carrying out transactions with natural persons or legal entities established in the listed countries.

This represents the first delegated act adopted in the field. It entered into force in September 2016.

The EU list basically replicates the list on high-risk countries adopted by the Financial Action Task Force (FATF). The European Parliament (EP) agreed to the first delegated act but

invited the Commission to consider a more ambitious approach, not limited to a mere copying of the FATF lists.

On 24 November 2016, the Commission adopted a new Delegated Regulation in line with the latest assessments from FATF by removing one country (Guyana) from the list. On 19 January 2017, the European Parliament objected to the Commission delegated regulation of 24 November and called on the Commission to submit a new delegated act which takes account of its concerns that an assessment should be conducted and to avoid relying solely on external information sources. Consequently the second Delegated Regulation cannot enter into force at this stage. The Commission is now reflecting on ways to address the current situation.

The EU approach towards high risk third countries cannot be disconnected however from what is done within international fora, such as FATF. On the other hand EU key concerns should be duly taken into account in the existing FATF listing process. Further effort is needed so that issues like the beneficial ownership transparency is considered more accurately when drawing FATF lists and should be included as a criterion in the FATF methodology.

The act is an essential element to ensure that harmonised rules allow undertakings to have sufficient legal clarity on what is required of them in respect of conducting business with partners established in high-risk third countries. As such, it is an essential element of the internal market, but with a strong security component. It is also an ancillary act to the 4AMLD.

The act may be considered to affect the freedom to conduct a business (Article 16 of the Charter). However, the requirements imposed to obliged entities are necessary, proportionate and justified, derive directly from Union law and only impose a number of requirement as to conducting customer due diligence, clearly defined by the 4AMLD.

The external dimension is inbuilt in the act, as it deals with establishing a single regime for conducting business with entities established or located in specific third countries.

3. Trafficking of Firearms

Firearms Directive – Directive (EU) 2017/853 amending Council Directive 91/477/EEC on control of the acquisition and possession of weapons

1. Legal framework

The proposal for revising the Firearms Directive (Directive 91/477/EEC as amended by Directive 2008/51/EC) is based on Article 114 TFSU.

In October 2013 the European Commission Communication “Firearms and the internal security of the EU: protecting citizens and disrupting illegal trafficking" proposed measures to increase the level of security of EU citizens in relation to firearms and to safeguard their licit market. In February 2015, at the informal European Council meeting, Heads of State and Government requested that all competent authorities increase the level of cooperation in the fight against illicit trafficking of firearms, including through the swift review of relevant legislation. The 2015 European Agenda on Security called for a review of the existing legislation on firearms in 2016 to improve various aspects of the Directive. Following the tragic events of 13 November 2015 in Paris, the Commission decided to advance the review of the Firearms Directive. In light of this, a proposal was adopted by the Commission on 18 November 2015.

2. Analysis

The aim of the review of the Firearms Directive was to address certain loopholes which were identified based on a number of studies that the European Commission had conducted evaluating all the provisions of the Firearms Directive[131].

In particular, the Evaluation of the Firearms Directive study highlighted some remaining obstacles in the current Directive which could undermine its functioning and highlighted the main issues that needed to be addressed. These were namely (a) the issue of convertibility of blank firing weapons (such as alarm weapons) into real firearms; (b) the need to clarify requirements for the marking of firearms (allowing their traceability); (c) the need for common and stringent guidelines for the deactivation of firearms; (d) the need to clarify definitions; (e) the need to consider internet selling arrangements; (f) the need to streamline and improve the national data exchange systems and explore the possibilities for interoperability; and (g) the need to strengthen data collection activities related to civilian firearms and related criminal offences to support appropriate future decision making processes at EU level.

Moreover, as highlighted in the 2015 European Agenda on Security, the Commission was asked to revised the Directive to improve the sharing of information (e.g. by uploading information on seized firearms in Europol's information system), to reinforce traceability, to standardise marking, and to establish common standards for neutralising firearms.

The revised Firearms Directive has amended the Directive to take into account these issues.

Threats of serious and organised crime and terrorism and the potential huge social and economic costs of violent actions are inherently characterised through their transnational nature, affecting more than one Member State at the same time. In this sense, they cannot be dealt with in a fully satisfactory manner by the individual Member States.

Only an EU-wide system can bring about the co-operation needed between Member States to control and track the civil use of firearms taking place within the EU.

The security issues tackled by the Firearms Directive are of cross-border nature. Therefore, vulnerabilities of a Member State to criminal activity affect the European Union as a whole.

As such, differences in national legislation, classification of firearms, and administrative procedures undermine the uniform application of the Directive. As underlined in the evaluation study on the Firearms Directive, effective action to ensure a high level of security and regulate the cross-border movement of firearms can only be taken at EU level. The Firearms Directive establishes a common regulatory framework that would not have been achieved through national or bilateral action alone.

The revised Firearms Directive complies with the proportionality principle. Proportionality is ensured by limiting the content of the proposed changes to those with the most important impact on security, according to the main conclusions of the studies carried out in the preparatory phase. On the whole, this proposal does not go beyond what is necessary to achieve the objective of ensuring the security of EU citizens without unnecessarily restricting the internal market.

Besides standard provisions of a commercial policy nature, in order to take into account the concerns and comments of private stakeholders the proposal is aimed at improving security

[131] Study to support an Impact Assessment on Options for Combatting Illicit Firearms Trafficking in the EU CSES, July 2014: https://ec.europa.eu/home-affairs/sites/homeaffairs/files/e-library/documents/policies/organized-crime-and-human-trafficking/general/docs/dg_home_-_illicit_fireams_trafficking_final_en.pdf.
Study to support an Impact Assessment on a possible initiative related to improving rules on deactivation, destruction and marking procedures of firearms in the EU, as well as on alarm weapons and replicas, June 2014: http://www.sipri.org/research/security/europe/publications/study-on-firearms.
Evaluation of the Firearms Directive, Dec 2014: http://ec.europa.eu/DocsRoom/documents/8385?locale=en.

standards and reducing inconsistencies with the UN Firearms Protocol, in particular those related to the definitions.

Regulation 258/2012 on export, import and transit licensing or authorization systems of firearms, their parts and components

1. Legal framework

The Regulation (EU) 258/2012 of the European Parliament and of the Council was adopted on 14 March 2012 to implement the Article 10 of the United Nations' Protocol against the illicit manufacturing of and trafficking in firearms, their parts and components and ammunition, supplementing the United Nations Convention against Transnational organised Crime and establishing export authorisation, and import and transit measures for firearms, their parts and components and ammunition.

2. Analysis

This Regulation is part of an overall legal and operational framework aiming at preventing, detecting, investigating and prosecuting firearms trafficking.

The Regulation applies only to firearms, their parts and essential components and ammunition for civilian use and not to those intended specifically for military purposes. Furthermore, it only addresses trade with and transfers from or to third countries.

The main scope of Regulation 258/2012 is the traceability of legal international trade of firearms for civilian use. It is based on the principle that firearms and related items should not be transferred between states without the knowledge and consent of all states involved. It lays down procedural rules for export, and import - as well as for transit of firearms, their parts and components and ammunition.

Exports of firearms are subject to export authorisations, containing the necessary information to trace them, including the country of origin, the country of export, the final recipient and a description of the quantity of the firearms and related items.

Member States have the obligation to verify that the importing third country has issued an import authorisation before issuing an authorisation to the export. In the case of transit of weapons and related items through third countries, each transit country must give notice in writing that it has no objection. Member States must refuse to grant an export authorisation if the person applying has any previous record concerning illicit trafficking or other serious crime.

The traceability of weapons represents an overarching objective in the fight against illegal trafficking in firearms. Improving firearms tracing - from manufacturer to last legal purchaser - is a key prevention objective of a comprehensive legislation aiming at reducing the risk of criminal diversion of rules and help law enforcement agencies to tackle the illegal trafficking in firearms.

Pursuant to its Article 21(3), the implementation of Regulation is currently being evaluated. This evaluation will consider the EU policy on security and firearms latest developments to lead to a common understanding of whether the current procedures and provisions put in place by the Regulation have delivered the intended results, and whether those results have been achieved in the most efficient manner, leading, where appropriate, to a set of recommendations for possible amendments notably in light of the Firearms legal package of 18 November 2015.

Before the adoption of the Regulation the national legislations in place did not fully comply with the provisions of Article 10 of the UNFP. At that time most but not all EU Member States required an import licence or authorisation before issuing an export licence (as requested by Article 10 UNFP). The Member States as whole did not have a harmonised procedure regarding the previous authorisation of transit of firearms.

The regulation of imports and exports of firearms has ensured a unified action in order to avoid regulatory heterogeneity and lack of administrative cooperation, which would have prevented proper law enforcement encouraged diversions into the black market.

A coordination group of experts chaired by the Commission meets regularly and ensure uniform application of the Regulation.

Mostly by enabling control of exports of firearms, the Regulation hinders trade by organised criminal groups to third countries, which can have a destabilising effect outside of the EU (with eventual repercussion inside it), and which would strengthen criminality inside the EU. The Regulation prevents shady exporters from trying their luck in various countries after having had their request for an export licence turned down in their own.

This Regulation governs mostly exports of firearms and is *per se* focussed on the external dimension of internal security. Having adopted strong rules on transfers of firearms both within and outside the Union, the EU has hereby ratified the UN firearms protocol. The conclusion of the UN firearms protocol by the European Union sent an important signal that the EU is serious about tackling the risk of criminal use of firearms, and encouraged those countries that have not yet done so to ratify and implement the protocol.

According to the assessment, avenues for further work could include:

- Ensuring that the definitions and categories are in line with the revised Directive on acquisition and possession of firearms (Directive 91/477)
- Improving the exchange of information between national authorities, if possible by linking it with the system to be put in place for intra-EU transfers under Directive 91/477
- Adapting and modernising export and import procedures

An evaluation is currently ongoing and its outcome will be presented by the end of 2017.

Action Plan on trafficking in firearms and explosives

1. Legal framework

The 2015 European Agenda on Security identified the fight against the trafficking in firearms as one of its priority actions. It called upon reviewing the legal framework and reinforcing the fight against firearms trafficking. Conscious of the priority to be given to the trafficking in firearms, in the 8 October 2015 Council Conclusions on firearms trafficking, Ministers of Interior called on the Member States, the Commission, Europol and Interpol to deliver on a series of actions for that purpose.

The European Commission adopted on 2 December 2015 an Action Plan to better prevent, detect, investigate and seize firearms, explosives and explosives precursors to be used for criminal and terrorist purposes as part of a Security Package. It complemented the legal initiatives adopted on 18 November 2015[132] proposing stricter rules in the legal use of firearms and common firearms deactivation standards.

2. Analysis

The illicit trafficking of firearms is part of the core business of organised crime groups as a source of revenues, because it makes possible other forms of crime and they are used for intimidation, coercion and gang violence. Above all, the series of terrorist attacks this year have shown the imperative to cut off access to both firearms and explosives.

With the 2015 Action Plan, the Commission is primarily looking into how in practice the fight against trafficking in firearms but also explosives can be stepped up and be rendered more

[132] See IP/15/6110.

effective. This string of measures is built around four priorities: restricting access to illegal firearms and explosives, enhancing operational cooperation, full use of information exchange tools and international cooperation.

The objective has been to intensify operational cooperation between Member States, police and customs and other law enforcement, involving Europol in particular but also key third countries and international organisations such as Interpol.

Special focus has been given to new threats and their links with other crime is crucial for targeting effectively the illicit trafficking in and the use of firearms and explosives.

The Commission has carefully considered a proper coordination with actions related to the Policy Cycle within the EMPACT priority on Firearms and to the European Firearms Expert group. Special attention has been given to actions in those fields which have not been fully exploited yet.

The role of Europol has been crucial, namely through a rapid and comprehensive implementation of the Europol Analysis System and through the Firearms Focal Point, assisting Member States and supporting efforts to improve systematic monitoring of firearms.

The need for strong coordination inside Member States still exist and that therefore the requirement of the Action Plan to set up national focal point is relevant and appropriate so far only ten Member States have set up national focal point on firearms in their administrations and three have planned to do it.

In the area of explosives precursors, the number of Member States compliant with Regulation (EU) 98/2013 has increased from 14 in October 2015 to 23 in February 2017. The Commission adopted a Report on application in February 2017 [COM(2017) 103 final].

The Action Plan has been very important to build a better intelligence picture on the trafficking of firearms and the use of explosives, and on diversion from legal markets, and to improve existing statistical and analytical tools at EU and national level.

Operational Actions have been in the core business of the EU action such as Operation plans. MARS, a coordinated transnational investigation based on a modus operandi of converted/reactivated firearms and joint actions in Western Balkans which have recently allowed seizing 48 firearms and arresting 58 individuals.

The Commission has promoted some researches such as Project EFFECT and project FIRE to improve knowledge on the illicit trafficking of firearms covering inter alia online trafficking and the diversion of legal trade. Europol has organised special training on how to tackle the illicit trade of firearms in the Internet and the Darknet. A Manual on Investigation drafted by Europol is also in the pipeline.

In 2016, under the Internal Security Funds the Commission has granted about 3 M€ to fund 5 projects by national stakeholders in this field and it has provided 1.5 M€ financial support over two years to the United Nations Office on Drugs and Crime (UNODC), 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. The Commission aims to carry out a regular collection of firearms trafficking data at EU level as part of the Eurostat annual data collection exercise.

In the area of explosives precursors, the number of Member States compliant with Regulation (EU) 98/2013 has increased from 14 in October 2015 to 23 in February 2017. In addition, an expert group bringing Member States and the supply chain together meets quarterly to promote good and harmonised precursors, and a series of regional workshops have been organised to support implementation. Most recently, the Commission added three additional threat substances to Annex II in November 2016 and adopted a report on the application in February 2017 [COM(2017) 103 final].

Article 6 of the Charter of Fundamental Rights of the European Union provides that "Everyone has the right to liberty and security of person." The very purpose of EU policy in the fight against firearms trafficking is to protect the security of EU citizens. All actions that enable better cooperation between enforcement authorities and fight cross-border crime contribute to enhanced security.

The illicit trafficking and use of firearms and explosives has been systematically **integrated into EU's security dialogues** with key partner countries and organisations. These dialogues are leading to specific joint action plans on firearms and where possible also explosives, including EU agencies such as Europol, Eurojust and CEPOL as well as relevant international organisations such as the UN and INTERPOL. EU financial assistance has been also envisaged in certain cases (such as confiscated/decommissioned firearms), e.g. under the Instrument contributing to Stability and Peace, other EU assistance programmes or the CFSP budget.

The activities under the Action Plan on the illicit trafficking of firearms between the EU and the South East Europe Region for the years 2015-2019 have been rapidly stepped up to further reduce the illicit flow of firearms to the EU. The EU has already a well advanced dialogue with MENA countries to enhance EU-MENA 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 assessment shows that further activities in the context of the implementation of the Action Plan could include:

- Ensure systematic harmonised data collection on firearms seizures for all EU Member States in order to better assess trafficking routes and improve threat assessments and quantitative evidence-base.
- Set up an EU-wide Ballistic Information System (or ensure interoperability between national systems).
- Set up an EU-wide information system to exchange information on authorisations (or refusals) to possess, acquire or transfer firearms.
- Step up international cooperation with third countries, following the model of the cooperation with the Western Balkans..
- Explore legislative action to enable cross-border controlled deliveries of firearms.

Action Plan on illicit trafficking in firearms between the EU and the South East Europe region (2015-2019)

1. Legal framework

The EU and countries in South East Europe have a shared interest in enhancing their cooperation to address common threats posed by illicit trafficking in firearms, an interest which is underpinned by the shared vision of these countries' accession to the EU.

On 5-6 November 2012, the Ministers of South East Europe acknowledged the need to enhance efforts to counteract the illicit trafficking and accumulation of firearms, their parts and essential components and ammunition in South East Europe, as well as their wish to work together with EU partners towards a joint solution for the whole region.[133]

Consequently, one year later, Ministers decided to set up a network of experts in firearms trafficking in the region. This led in October 2014 to the adoption of an Action Plan on firearms trafficking between the EU and South East European countries for 2015-2019.[134] It

[133] Council document 15897/12.

[134] Bosnia and Herzegovina, Macedonia, Kosovo*, Montenegro and Serbia. (*this designation is without prejudice to positions on status, and is in line with UNSCR 1244 and the ICJ Opinion on the Kosovo Declaration of Independence).

was formally adopted in December 2014 by both the Council[135] and the EU-Western Balkans Ministerial Forum on Justice and Home Affairs.

The need to carry on cooperation in the Western Balkans and the EU was last confirmed by the 2015 EU Action Plan against illicit trafficking of firearms.[136] On 15-16 December 2016, the EU-Western Balkans Ministerial Forum on Justice and Home Affairs reaffirmed the commitment to implement a number of specific actions to implement the Action Plan.

2. Analysis

The action plan foresees the following actions:

- Enhancing the exchange of information at regional level and with Member States
- Enhancing operational law enforcement co-operation at regional level
- Improving the collection and exchange of statistics on production, stockpiling and trafficking of firearms and ammunition;
- Promoting networking at all levels, the exchange of best practices and joint training;
- Harmonising national legislation on firearms in line with EU and international standards.

The 2015 European Agenda on Security recognises that trafficking of firearms has a critical external dimension, given that many illegal firearms in the EU have been trafficked from neighbouring countries where large stockpiles of military weapons remain. The dialogue with the region is regularly assessed and updated upon relevance.

The EU has for a long time been involved in various forms of technical cooperation within the context of the Common Foreign & Security Policy and the European Neighbourhood Policy, aiming at blocking trafficking routes, improving the management of firearms stocks, and preventing the diversion of firearms from the legal market, notably in the Western Balkan region.

At the meeting of 29 January 2016, the EU and Western Balkans experts decided to enlarge the scope of the Joint Action Plan to illicit explosives. They recommended to increase the insertion of information on firearms into Interpol's Illicit Arms Records and tracing Management System (iARMS) and they decided to call for regular meetings between the Secretariats of the South East Europe Firearms Expert Group (SEEFEG) and the South Eastern and Eastern Europe Clearinghouse for the Control of the Small Arms and Light Weapons (SEESAC) to discuss the way of working and initiatives to improve mutual cooperation, such as the follow up of Threat Assessment questionnaire on illicit firearms trafficking.

They also decided to carry out at least two joint actions focused on the illicit trafficking in firearms, components and ammunition and explosives with a regional approach and to organise dedicated common training actions to improve awareness about the fight against illicit trafficking in firearms, updated trends and best practices to tackle it. The first Joint Action helped establish good coordination and helped identify shortcomings to be addressed in the future (such as the quality of operational information, the time of information delivery or legal obstacles).

On 30th November 2016, the Commission called the first joint meeting EFE/WB experts. The experts favourably considered the support of EU Members States under EU Policy cycle Firearms Priority (EMPACT). They agreed to continue their efforts in the fight against illicit trafficking in firearms to, inter alia, continue enhancing cooperation in investigations of trans-border crimes, coherently with the initiatives aiming at enhancing operational law enforcement cooperation, promoted within the Integrative Internal Security Governance (IISG). They also decided to enhance the exchange of information at regional level and with

[135] Council document 15516/14.
[136] Commission Communication of 2/12/2015, "EU action plan against illicit trafficking in and use of firearms and explosives ", COM(2015) 624 final.

Member States involving different organisations including Europol on the production and stockpiling and trafficking in firearms and ammunition aiming also to develop more effective investigative and intelligence standards.

The EU measures are adding value in supporting and facilitating cooperation in this field, by hosting joint EU-WB meetings, financing several activities, spurring regulatory convergence, financing research and sharing of information. The latter has been recalled by the participants of the EU-Western Balkans Ministerial Forum on Justice and Home Affairs in Brdo on 15-16 December 2016, who acknowledged the pressing need to counter the illicit trafficking and accumulation of firearms and reaffirmed their strong commitment to work together towards joint solutions.

The Action Plan aims to provide a coherent framework for cooperation between the European Union and the South East Europe region. Through this Action Plan between the EU and South East Europe region, the EU intends to intensify the cooperation with the countries of the region according to their specific needs, requirements and performance. In line with the EU Firearms Strategy, this Action Plan has a comprehensive and multidisciplinary character. It is based on the respect for international law, encouraging the respect for and observance of human rights and fundamental freedoms

Besides, the EU and WB countries cooperate intensely with the UNDP, through SEESAC (The South Eastern and Eastern Europe Clearinghouse for the Control of Small Arms and Light Weapons), in the framework of the UN PoA (UN Program of Action) on small arms and light weapons and the ATT (Arms Trade Treaty). Cooperation with OSCE also takes place, based on the 2000 OSCE Document on Small Arms and Light Weapons by which States agreed to norms, principles, and measures to control each stage in a weapon's life: production, transfer, storage, collection or seizure, and destruction.

The assessment shows that further activities in the context of the implementation of the Action Plan could include:

- Regularly update the action plan by keeping on organising joint meetings between the European Union and the South Eastern Europe Firearms experts (including by ensure Western Balkans participation in EMPACT Firearms and CEPOL activities);
- Step up operational cooperation by promoting increased exchange of information with Europol and European Union Member States prior to joint operations ("intelligence-led") and after the operations (follow-up investigations);
- Encourage Member States to depart from purely bilateral approach in their cooperation with Western Balkan countries and engage in multilateral action (such as joint actions under EMPACT Firearms);
- Promote a better use of the means available to participating countries such as Europol Mobile Office and the funds available for investigations and operations ("red envelope")
- Encourage systematic data collection on seizures in the Western Balkan;
- Carry out a feasibility study on voluntary surrenders (buy-back programmes).

Commission Implementing Regulation on Deactivation of Firearms and its subsequent revision

1. Legal framework

Commission Implementing Regulation (EU) 2015/2403 of 15 December 2015 is establishing common guidelines on deactivation standards and techniques for ensuring that deactivated firearms are rendered irreversibly inoperable.

During the informal European Council meeting of 12 February 2015, the Heads of State and Government requested that all competent authorities increase the level of cooperation in the

fight against illicit trafficking of firearms, including through the swift review of relevant legislation.

The European Commission Communication "Firearms and the internal security of the EU: protecting citizens and disrupting illegal trafficking"[137], launched in October 2013 proposed measures to increase the level of security of EU citizens in relation to firearms and to safeguard their licit market.

The 2015 European Agenda on Security called for a review of the existing legislation on firearms in 2016 to improve various aspects of the Directive. Following the tragic events of 13 November 2015 in Paris, the Commission decided to advance the review of the Firearms Directive. In light of this, a proposal was adopted by the Commission on 18 November 2015.

2. Analysis

The Evaluation of the Firearms Directive study[138] highlighted some remaining obstacles in the current Firearms Directive which could undermine its functioning. It also highlighted the main issues that needed to be addressed in the Firearms Directive. One of these issues related to the need for common and stringent guidelines for the deactivation of firearms.

In fact, in the past, there were instances where deactivated firearms were reactivated and used for criminal purposes.

In an effort to tackle this problem, an implementing regulation on deactivation of firearms was agreed. The regulation was agreed in November 2015 following a two-year discussion with EU experts. It became applicable as from April 2016.

The implementing regulation proposes stringent minimum common guidelines regarding the deactivation of firearms which will render reactivation much more difficult.

These implementing regulation are in line the relevant UN protocol which states that all essential parts of a deactivated firearm are to be rendered incapable of removal (e.g. though welding).

However, during the discussion of the revised Firearms Directive in 2016, the co-legislators decided that implementing regulation should be re-discussed, not due to lack of security of the current regulation, but to allow Member States to be able to deactivate also in another way (not necessarily through welding). That is the rationale behind the revision of the implementing regulation on deactivation.

Threats of serious and organised crime and terrorism and the potential huge social and economic costs of violent actions are inherently characterised through their transnational nature, affecting more than one Member State at the same time. In this sense, they cannot be dealt with in a fully satisfactory manner by the individual Member States. Only an EU-wide system can bring about the co-operation needed between Member States to control reactivation of deactivated weapons.

The EU has also provided added value through the setting up of an expert working group on deactivation. Since not all EU Member States are part of the CIP (Commission Internationale Permanente pour l'épreuve des armes a feu portatives), it provides a fora for experts to meet and discuss practices in relation to deactivation.

4. Trafficking in Human Beings

1. Legal framework

[137] COM(2013) 716 final, Communication from the Commission to the Council and the European Parliament, Firearms and the internal security of the EU: protecting citizens and disrupting illegal trafficking.
[138] Evaluation of the Firearms Directive, Dec 2014: http://ec.europa.eu/DocsRoom/documents/8385?locale=en.

Trafficking in human beings is a complex phenomenon with cross-cutting links to several policy areas, including security and organised crime, development, justice, gender, employment, and foreign policies of the Union. It is both a violation of fundamental rights, explicitly prohibited under Article 5 of the EU Charter of Fundamental Rights, and a serious form of organised crime ("Eurocrime") explicitly enshrined in Art. 83 TFEU and linked to illegal migration, Article 79 TFEU.

The EU has established a comprehensive legal and policy framework to address trafficking in human beings, namely the Anti-Trafficking 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.

The Directive 2011/36/EU adopts a comprehensive, integrated approach that focuses on human rights and on the victims and is gender-specific and child sensitive. It equally focuses on the law enforcement aspects as it aims to prevent crime and ensure that victims of trafficking are given an opportunity to recover and to reintegrate into society. The Commission has been proactively monitoring the transposition of the Directive 2011/36/EU and will continue ensuring full compliance and implementation of this milestone piece of EU legislation in the area of THB. Based on Article 20 of the Directive, the EU Anti-trafficking Coordinator ensures consistency 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 Commission has delivered on the vast majority of actions envisaged in the 2012-2016 Strategy.

2. Analysis

Having a clear policy framework in this area to guide the work has been crucial to ensure a coherent approach, proper budget planning and coordinated funding activities. The EU Anti-trafficking Coordinator has had the responsibility over the past five years to monitor the implementation of the 2012-2016 EU Strategy which has provided a coherent basis and direction for the EU policy in this area. Member States have followed the implementation of the Strategy with National Action plans and key stakeholders have endorsed and welcomed the policy steer from the Commission. The policy framework has led amongst others to the creation of networks and platforms fostering coordination between Member States, the EU Institutions and JHA Agencies. The 2012-2016 Strategy succeeded in putting together a number of processes that result in a coordinated and more coherent approach at the EU level to tackle the crime, which has been clearly recognised in Council Conclusions and European Parliament[139] resolutions.

With the expiration of the 2012-2016 Strategy, a reflection has started on a new policy framework in order to guide the work of the Commission and all relevant actors across the EU in a consistent manner. Based on the targeted discussion with Member States (via the Network of National Rapporteurs or equivalent mechanisms), JHA agencies, EU Civil Society Platform against THB, international organisations, inter-service group on Trafficking in human beings, the Commission is currently in the process of developing a post 2016 policy framework to bring together all the different policy areas and define deliverables to achieve the various objectives in a coherent and efficient manner.

Having completed numerous reports and studies, as well as based on various consultations with all relevant stakeholders and taking into account the coordination efforts at EU level, it

[139] In the European Parliament resolution of 12 May 2016 on implementation of the Directive 2011/36/EU of 5 April 2011 on preventing and combating trafficking in human beings and protecting its victims from a gender perspective; European Parliament resolution of 5 July 2016 on the fight against trafficking in human beings in the EU's external relations; Council Conclusions on addressing trafficking in human beings (THB) for labour exploitation.

appears that both the Directive and the Strategy have contributed towards addressing the key challenges in the area of trafficking in human beings.

At the same time, given that the Directive is still a relatively recent instrument and further to the changing socio-political context[140] it is clear that much remains to be done in the areas of prosecution, protection and prevention as well as in other areas.

In this context, ensuring full implementation of the Directive and the continuation of the efforts as per the renewed post-2016 policy framework is crucial.

All Member States have officially notified the Commission of the transposition of the Directive 2011/36/EU, upon which the Commission has issued the Report assessing the extent to which Member States have taken the necessary measures in order to comply based on Article 23.1 of the latter. Substantial efforts have been taken by the Member States to transpose this comprehensive instrument. Nevertheless, there still remains significant room for improvement in particular as regards: specific child protection measures, presumption of childhood and child age assessment, the protection before and during criminal proceedings, access to unconditional assistance, compensation, non-punishment, assistance and support to the family member of a child victim as well as prevention.

Furthermore, over the past five years a lot has been achieved in delivering actions (indicative guidelines, manuals, reference documents[141], studies[142] below) laid down in the 2012-2016 Strategy and fulfilling legal reporting requirements under the Directive.[143] The EU Strategy has provided a coherent basis and direction for the EU policy in this area. Of note some EU Member States have designed their national strategies mirroring the EU 2012-2016 Strategy. The 2012-2016 Strategy succeeded in putting together a number of processes that result in a coordinated and more coherent approach at the EU level to tackle the crime, which has been clearly recognised by the Council and European Parliament resolutions. In this context, it is important to highlight that trafficking in human beings is constantly evolving, while trafficking for various forms of exploitation is expected to increase in the current migration crisis occurring in North Africa and the Middle East.

[140] The financial crisis, migration challenges and increased transnational security threats concerns, have all had an important impact on the complex phenomenon of trafficking in human beings, increasing vulnerability of the victims. There are reports of a high incidence of trafficking in human beings in the Central Mediterranean Route. The modus operandi and the forms of trafficking change, for example with indications on increase to trafficking for sexual exploitation.

[141] 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.

[142] 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).

[143] Report on the progress made in the fight against trafficking in human beings (2016) as required under Article 20 of Directive 2011/36/EU on preventing and combating trafficking in human beings and protecting its victims, Brussels, 19.5.2016 COM(2016) 267 final and the Accompanying Commission Staff Working Document (Brussels, 19.5.2016 SWD(2016) 159 final); 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; 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 COM(2016) 719. Although not a legal obligation, Commission Staff Working Document, Mid-term report on the implementation of the EU strategy towards the eradication of trafficking in human beings (Brussels, 17.10.2014, SWD(2014) 318 final) was also published.

There are new threats and challenges which must be addressed with adequate and targeted actions at EU level[144]. More specifically both the modus operandi and the forms of trafficking change, for example with indications on increase to child trafficking and trafficking for sexual exploitation. There are reports of a high incidence of trafficking in human beings in the Central Mediterranean Route, while the migration and refugee crisis is expected to lead to more trafficking of asylum seekers arriving from Syria. Europol informs that traffickers are already abusing gaps in the asylum systems. In this context, the link of unaccompanied minors and trafficking need to be further addressed.

The links of trafficking in human beings and other forms of crime, such as falsification of documents, drug trafficking, cybercrime, child pornography, terrorism and terrorism financing migrant smuggling benefit fraud need further examination and targeted action. Also, as related activities, Member States mention money-laundering, or the means for implementing that, such as by falsifications, lesions or threats. There is a pertinent need to protect and assist the most vulnerable while at the same time targeting the perpetrators of this serious form of criminality.

Against this, the Commission can continue to have a leading role in this area as well as and further build on the work successfully completed by presenting a cross cutting, comprehensive policy framework which addresses current trends, challenges and gaps identified in order to guide and coordinate the efforts in this area. This would also contribute to supporting the Member States in: the full implementation of the EU law against trafficking; prosecuting the perpetrators; protecting the victims; and, preventing the phenomenon from happening in the first place.

Having completed numerous reports and studies, as well as from all consultations with all relevant stakeholders, it can be concluded that both the Directive and the Strategy have contributed towards addressing the key challenges in the area of trafficking in human beings. In addition, the Directive, the Strategy as well as all coordination efforts, offered a real added value by supporting or facilitating European cooperation by improving national capabilities or by complementing, stimulating or leveraging Member States and EU action[145]. The Directive provided for a harmonised definition of the criminal offence of THB. In this context, also the coordination work across services (within the Commission and with other EU institutions and bodies), with Member States (via the EU Network of National Rapporteurs or equivalent mechanisms composed of senior officials as well as independent Rapporteurs), with JHA agencies (via the THB Contact Points JHA agencies coordination group) and civil society organisations (EU Civil Society Platform against THB gathering 100 NGOs from EU Member States and selected neighbouring priority countries), have further contributed to

[144] Report on the progress made in the fight against trafficking in human beings (2016) as required under Article 20 of Directive 2011/36/EU on preventing and combating trafficking in human beings and protecting its victims, Brussels, 19.5.2016 COM(2016) 267 final and the Accompanying Commission Staff Working Document (Brussels, 19.5.2016 SWD(2016) 159 final); Europol, Situation Report, Trafficking in human beings in the EU(2016), Europol, EU SOCTA 2017, delivering a set of recommendations based on an in depth analysis of the major crime threats facing the EU, including THB.

[145] Strengthening child protection systems to ensure safe return and prevent re-trafficking; establishment of national, multidisciplinary law-enforcement units on THB; proactive financial investigations of THB cases and cooperation with EU agencies; analysis of information received form Member States on financial investigation in THB cases (Europol); joint investigation teams; full use of EU agencies; Implementation of Eurojust Action Plan against THB (February 2017); regional cooperation on THB along routes from east to the EU; Coordination and monitoring of the implementation of the Joint Statement signed by EU JHA agencies; strengthening the EU-wide coordination mechanism to support the Network of National rapporteurs and/or equivalent Mechanisms; establishment of cooperation mechanisms in EU delegations in priority third countries and regions ; strengthening and formalisation partnerships with international organizations; inclusion of human rights clauses; funding of projects on THB in EU and third countries and regions; establishment of EU platform of civil society organisations and service providers; strengthening and training targeting judiciary and cross-border law enforcement officials, increased policy coherence through training programmes, setting up inter-service group on THB within Commission, etc.

addressing trafficking in human beings and facilitating cooperation at EU and national levels. A number of JITs and Joint Operations were concluded.

The statistical working papers on THB (2013 and 2015 editions) published by Eurostat demonstrate encouraging progress in terms of availability of data[146]. These are results of the coordination efforts between Commissions services and Member States authorities and civil society, with clear EU added value pointing to the need for further improvements on THB data for better conclusions on the phenomenon and for the policy at national and EU level. Due to the improved availability of THB data across EU Member States, as a result of these robust data collections, in 2016, Eurostat launched a pilot data collection for developing THB data as part of its official annual crime/criminal justice statistics.

To implement this comprehensive legal and policy framework, the EU provides extensive funding under a number of thematic and geographical instruments and projects, a database of which is available on the EU anti-trafficking website. THB has been addressed in several topics of the security and Social Sciences and Humanities[147] research programme in Framework Program 7[148], Societal Challenge 6 (Inclusive, Innovative and Reflective societies) and Societal Challenge 7 (Secure Societies) in Horizon 2020[149].

Trafficking in human beings is explicitly prohibited by the Charter of Fundamental Rights. Directive 2011/36/EU, adopts a human rights approach and this is further reflected in the EU Strategy. The Directive sets forth a series of provisions for victims for safeguarding their fundamental rights and ensuring access to and implementation of their rights as victims.

This approach is also considered in a number of deliverables of the EU Strategy including the Commission's Guidelines on the identification of victims of trafficking in human beings in particular for consular services and border guards, the Study on high-risk groups for trafficking in human beings (2015) and the Study on the gender dimension of trafficking in human beings (2016).

The external dimension of trafficking in human beings 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, both as a human rights issue as well as a cross-border illegal activity, involving countries of origin and transit outside the EU. The EU Strategy addressed the importance of increasing cooperation 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 planned post-2016 EU policy framework will take stock of these experiences, ensuring coherence and continuity, and follow up and build on the key EU policy instruments that systematically addressed THB in a radically changed political environment, reflecting a strong focus on the external dimension of the EU anti-trafficking policy.

The basic framework has been set in the 2009 the Action Oriented Paper on strengthening the EU external dimension against trafficking in human beings (AOP) and in the Global Approach to Migration and Mobility (GAMM). Following up to the AOP a list of priority countries and regions was adopted by the Council. EU Delegations in third priority countries appointed contact points on THB, to strengthen coherence, exchange of information, monitoring EU-funded projects on THB. In line with the GAMM, THB is systematically covered in all dialogues and cooperation frameworks with non-EU countries, such as the Mobility Partnerships, the Common Agendas on Migration and Mobility and visa liberalisation dialogues. THB is included in the Stabilization and Association Agreements

[146] Eurostat Statistical Working Paper Trafficking in Human Beings 2013 edition and 2015 edition.
[147] http://ec.europa.eu/research/social-sciences/index.cfm?pg=policies&policyname=justice-stability
[148] https://ec.europa.eu/research/fp7/index_en.cfm?pg=security.
[149] https://ec.europa.eu/programmes/horizon2020/en/h2020-section/secure-societies-%E2%80%93-protecting-freedom-and-security-europe-and-its-citizens.

between the EU and the Western Balkans countries and addressed in the action plans with the Neighbourhood countries and progress is reported in the Neighbourhood Policy annual reports. THB is also addressed in the new Global Strategy for the European Union's Foreign and Security Policy.

While THB existed prior to the migration crisis, it is being exacerbated by the recent migration challenges. The Report on the progress made in the fight against trafficking in human beings highlights that there is evidence that the migration crisis has been exploited by traffickers to target the most vulnerable, in particular women and children. Europol's February 2016 Situation Report on trafficking in human beings in the EU suggests that current trends in sexual and labour exploitation are expected to increase and the migration crisis will have a major impact on THB. Europol SOCTA 2017 highlights that the migration crisis has resulted in an increase in the number of potential victims of THB (vulnerable adults, unaccompanied minors, irregular migrants and asylum seekers) and that the increasing reports of sham marriages are likely related to the migration crisis.

In a radically changed socio-political environment, the external dimension of THB is explicitly addressed in multiple EU policy areas and instruments: 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 (EUGS), the new Action Plan on Human Rights and Democracy 2015-2019, the new framework for the EU's activities on gender equality and women's empowerment in EU's external relations for 2016-2020, the Strategic Engagement on Gender Equality, the EU Strategy on Corporate Social Responsibility (CSR) and the new European Consensus on Development, the new Partnership Framework, the Joint communication Migration on the Central Mediterranean route Managing flows, saving lives. The recently appointed European Migration Liaison officers (EMLO), are tasked to include information on the situation on THB in their periodical reports. Eurojust increased the number of contact points in third countries, encouraging the referral of THB cases.

THB also forms part of the Khartoum and Rabat Processes, it is included in the priority domains of the Joint Valletta Action Plan, and the need to enhance efforts to address THB is reflected in the Joint Conclusions presented in the context of the February 2017 Valletta Summit on Migration.

5. Drugs Trafficking

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

1. Legal framework

Framework Decision 2004/757/JHA is based on the predecessors of Article 83(1) TFEU, Article 31(e) and Article 34(2)(b) ex-TEU.

The need for legislative action to tackle illicit drug trafficking had at the time of the adoption of the Framework Decision been recognised in particular in the action of the Council and the Commission on how best to implement the provisions of the Amsterdam Treaty on the area of freedom, security and justice adopted in 1998, the conclusions of the Tampere European Council of 15 and 16 October 1999, the EU Drug Strategy (2000-2004) and the EU Action Plan on Drugs (2000-2004).

2. Analysis

The objective of the Framework Decision is to establish minimum rules relating to the definition of offences of illicit trafficking in drugs and precursors and to establish minimum-maximum levels of sanctions for those offences.

The European Agenda on Security stresses that the market for illicit drugs remains the most dynamic of criminal markets, with a recent trend being the proliferation of new psychoactive substances (NPS). The current EU Drugs Strategy (2013-2020) also aims at reducing intra-EU and cross-border production, smuggling, trafficking, distribution and sale of illicit drugs. There is still a current need for an EU common approach to tackle illicit drug trafficking.

The main added value of the Framework Decision is that it establishes a common approach on EU level to fight against trafficking in drugs and precursors. The Framework Decision focusses only on the most serious types of drug offences and excludes offences related to personal consumption of drugs from its scope. Further, Member States have to ensure that the offences defined are punishable by effective, proportionate and dissuasive criminal penalties.

The implementation of the Framework Decision by Member States is not completely satisfactory. In 2009, the Commission adopted a report on the implementation of the Framework Decision (COM (2009)669 final) which found that the provisions of the Framework Decision were not implemented by all Member States to the full extent. A report on the evaluation of the transposition and impact of Framework Decision 2004/757/JHA on drug trafficking published by the Commission in 2013 concluded that in general, the laws of most Member States were already consistent with the Framework Decision when it was adopted since the Member States had already implemented the UN Drug Control Conventions when the Framework Decision was adopted (1961 UN Single Convention on Narcotic Drugs, 1971 UN Convention on Psychotropic Substances, 1988 UN Convention against Illicit Traffic in Narcotic Drugs and Psychotropic Substances). Therefore, the perception of practitioners in the Member States is that the Framework Decision had no significant impact on the practice of prosecutions, convictions and sentencing. However, the study found the legislation of only 5 Member States (DE, ES, FI, EL, LV) was in full compliance with all provisions of the Framework Decision.

The Framework Decision will be amended in order to deal with the new trend of the growing numbers of NPS in the context of the new legal framework on NPS currently under negotiation. The political agreement was found on 29 May 2017. [150]

Besides the amendments related to NPS, it has to be noted that the Framework Decision dates from 2004 and is based on a legal basis that has in the meantime been replaced by the Lisbon Treaty. The Framework Decision also does not provide for any prevention measures which are an important part of drug supply reduction and also does not address new developments such as the online markets for drugs. Therefore, a modernisation of the Framework Decision could be considered.

As to its external reach, the Framework Decision is applicable only to the EU Member States. However, it defines drugs by reference to the Schedules of the 1961 UN Single Convention on Narcotic Drugs and the 1971 UN Convention on Psychotropic Substances and precursors by reference to the Schedules of the 1988 UN Convention against Illicit Traffic in Narcotic Drugs and Psychotropic Substances. Therefore, the scope of its application is linked to the area of international scheduling of substances, where the EU has an exclusive external competence. In March 2017, the EU adopted for the first time an EU common position on the scheduling of 10 new substances under the 1961 and 1971 Conventions and on the scheduling of 2 precursors under the 1988 UN Convention.

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

1. Legal framework

[150] See Council of the European Union, Brussels, 9 June 2017 (OR. en) 9955/17.

Council Decision 2005/387/JHA is based on the predecessors of Articles 67 and 83(1) TFEU, Article 29, 31(e) and Article 34(2)(b) ex-TEU. It repealed (and replaced) Joint Action 97/396/JHA concerning the information exchange, risk assessment and the control of new synthetic drugs.

2. Analysis

The aim of the Council Decision is to establish a mechanism for exchange of information on new psychoactive substances (NPS), to provide for an assessment of the risks associated with these new substances to be carried out by the European Monitoring Centre for Drugs and Drug Addiction (EMCDDA), and to set out a procedure on EU level for bringing specific NPS under control.

Where the Council, based on a Commission proposal that follows a risk assessment of a new substance, decides to submit a NPS to control measures, it adopts an implementing Decision in relation to that substance and Member States have to make certain conducts linked to that substance punishable under criminal law.

The Council Decision is not any more adapted to the rapid emerge of NPS in the last years as procedures are hardly adapted to the speed of this phenomenon. An impact assessment conducted by the Commission in 2013 concluded that the capacity to rapidly identify and assess NPS needs to be improved. Therefore, the Commission proposed in 2013 a package of two legal acts for a new legislative framework on NPS (a Regulation on NPS, and a Directive amending Framework Decision 2004/757/JHA). The objective of the proposals was to reduce the availability of NPS that pose risk through swifter, more effective action on EU level.

Negotiations on the package have been ongoing for more than three years. At the end of August 2016, the Commission adopted a proposal amending the EMCDDA Regulation. The Council agreed on a general approach on the NPS package on 8 December 2016. Beginning of 2017, trilogues started and the political agreement was found end May 2017

The Council Decision includes a recital (recital 15) stressing that it respects fundamental rights and observes the principles recognised by Article 6 of the Treaty and reflected in the Charter of Fundamental Rights of the EU. A similar recital can be found in the EMCDDA Regulation (recital 21) that will be amended once the new legislative framework on NPS is adopted.

The European Agenda on Security points to the urgency of the adoption of the new legislative framework on NPS. Awareness raising of the risks and consequences associated with the use of NPS, the challenge of their misuse, the challenge of having them sold online, as well as measures to address their emergence, use and rapid spread are also part of the EU Action Plan on Drugs 2013-2016. The evaluation of the EU Drugs Strategy 2013-20 and the EU Action Plan 2013-16 further concludes that the rapid adoption of the legislative package on NPS and its swift implementation are priorities for the coming years.

The adoption of the new legislative framework on NPS is also in line with the outcome document adopted at the UN General Assembly at the Special Session on the world drug problem (UNGASS, 19-21 April 2016). A specific section of this document deals with addressing emerging and persistent challenges and threats including NPS and calls for strengthening action to address the challenge of NPS as well as for enhancing information-sharing and early warning networks.

The Council Decision (and the future new legislative framework on NPS) applies only to the Member States. However, the EU-system, in particular early warning system and risk assessment have become a reference for other countries worldwide and for the UN system (World Health Organisation (WHO), United Nations Office on Drugs and Crime (UNODC)).

European Monitoring Centre for Drugs and Drug Addiction – EMCDDA

1. Legal framework

EMCDDA was set up in 1993 by a Regulation, substantially amended several times and finally recast in 2006[151]. The Centre relies on the European Information Network on Drugs and Drug Addiction (Reitox) for the majority of its data. This network, composed of focal points in each of the EU Member States, Norway and Turkey, contributes to the Centre's core business of collecting and reporting qualitative and standardised information on the drug phenomenon across Europe. These data feed the European and global analyses performed by the EMCDDA, thereby forming the basis of its world-renowned knowledge and its reputation as a centre of excellence on drugs in Europe.

The EMCDDA founding regulation is currently being amended in order to include provisions on information exchange and early warning system on new psychoactive substances as well as on the risk assessment procedure, currently part of Council Decision 2005/387/JHA[152], among the tasks of the Centre. The aim is to strengthen the system and to streamline procedures in order to ensure more effective and swifter action at EU level to put these harmful substances under control.

2. Analysis

The main objective of the Centre is to provide the EU and its Member States with sound and comparable information on drugs, drug addiction and their consequences in Europe, thus helping policymakers to design informed drug laws and strategies.

In order to achieve its main objective the Centre performs the following tasks:

a) monitoring the state of the drugs problem and emerging trends; b) monitoring the solutions applied to drug-related problems; c) providing information on best practices in the Member States and facilitating information exchange among them; d) assessing the risks of new psychoactive substances and maintaining a rapid information system; e) developing tools and instruments to help Member States to monitor and evaluate their national policies, and the European Commission to monitor and evaluate EU policies.

The EMCDDA publishes three main products: the European Drug Report, which presents an overview of the drug phenomenon in Europe, covering drug supply, use and public health problems as well as drug policy and responses; the European Drugs Market Report, which assesses the impact of the drug market, for each drug, on society and the factors driving it; and the European Drug Reponses Report, which aims at providing an overview of the responses to drug use across the EU and their effectiveness as well as recommendations for action. While the first one is a yearly publication, the other two are meant to be issued every three years but not simultaneously.

The Centre will be subject to an external evaluation to be initiated by the Commission, as foreseen in Article 23 of the EMCDDA founding Regulation, in order to assess: a) the last two 3-year work programmes of the Centre (2013-2015 and 2016-2018), as well as the Reitox system; and b) if the provisions of the founding regulation are still adapted to current needs.
The final report of such evaluation will be sent once ready to the European Parliament, to the Council and to the Centre's Management Board.

The last external evaluation of the Centre was initiated by the Commission in mid-2011 and concluded in mid-2012; it covered the 2007-2009 and 2010-2012 work programmes; the final report was sent, as foreseen by Article 23 of the founding Regulation, to the European Parliament, to the Council and to the Centre's Management Board on 26 July 2012.

[151] Regulation (EC) No 1920/2006 of the European Parliament and of the Council of 12 December 2006, OJ L 376 of 27.12.2006.
[152] Council Decision 2005/387/JHA of 10 May 2005 on the information exchange, risk assessment and control of new psychoactive substances, OJ L 127, 10.5.2005.

On the basis of the evaluation to be conducted, the Commission might decide further amendments of EMCDDA founding regulation. The result of the evaluation could also feed the preparation of the new EU Drugs Strategy, given that the current one expires in 2020.

Council Regulation (EC) No 111/2005 of 22 December 2004 laying down rules for the monitoring of trade between the Union and third countries in drug precursors as amended by Regulation 1259/2013 and Regulation (EC) No 273/2004 of the European Parliament and of the Council of 11 February 2004 on drug precursors as amended by Regulation 1258/2013

1. Legal framework

Council Decision 90/611/EEC of 22 October 1990 concerning the conclusion, on behalf of the European Economic Community, of the United Nations Convention against Illicit Traffic in Narcotic Drugs and Psychotropic Substances (OJ L 326, 24.11.1990, p. 56).

Council Regulation (EC) No 111/2005 is based on Article 207 (Common Commercial policy) of the TFEU.

Regulation (EC) No 273/2004 is based on Article 114 (Common rules on Competition, Taxation and Approximation of laws) of the TFEU.

The need for legislative action to tackle diversion of drug precursors directly follows from the fact that the EU is a Party to the United Nations Convention against Illicit Traffic in Narcotic Drugs and Psychotropic Substances of 1988 for issues which are dealt with under Article 12 of that Convention.

2. Analysis

The objective of Regulation 273/2004 is to establish a control and monitoring system at EU level for intra-EU trade in drug precursors, with the same objectives as Regulation 111/2005. The two Regulations jointly implement the provisions of Article 12 of the United Nations Convention against Illicit Traffic in Narcotic Drugs and Psychotropic Substances of 1988.

The 2015 European Agenda on Security stresses that the market for illicit drugs remains the most dynamic of criminal markets. Additionally, the EU is a major producing area of synthetic drugs such as MDMA and amphetamines. The current EU Drugs Strategy (2013-2020) therefore aims, among others, at reducing the production, smuggling, trafficking, distribution and sale of illicit drugs.

Both Regulations have been amended in 2013 in order to address the rapid emergence of non-scheduled substances and the diversion of medicinal products containing drug precursors at export. Also, to ensure a better system for the collection and exchange of information between the national competent authorities and the Commission, a new mandatory EU Database on Drug Precursors was introduced with the revision of the Regulations. The amendments were proposed on the basis of the recommendations contained in a report adopted by the Commission on 7 January 2010 on the implementation and functioning of the Community legislation on monitoring and control of trade in drug precursors. In its Conclusions of 25 May 2010 concerning the report, the Council invited the Commission to propose legislative amendments to the two Regulations on drug precursors.

At the end of 2019 the Commission shall submit a report to the European Parliament and to the Council on the implementation and functioning of these Regulations, and in particular on the possible need for additional action to monitor and control suspicious transactions with non-scheduled substances.

The main added value of the two Regulations on drug precursors is that they establishe a clear and common framework on EU level to prevent the diversion of drug precursors.

Drug supply reduction is one of the two main policy areas covered by the EU Drugs Strategy (2013-2020) and EU Action Plan on Drugs (2013-2016).

The Regulation is also relevant in the context of the EU Policy Cycle (2013-2017) which includes *inter alia* priorities on synthetic drugs, cocaine and heroin trafficking.

The measures under the Regulations potentially impact the rights which are enshrined in the following Articles of the Charter of fundamental Rights of the EU (hereinafter: 'CFR'):

- the protection of personal data (Article 8 CFR);
- the freedom to conduct a business (Article 16 CFR).

The measures laid down under the Regulations strike a careful balance between the rights in question and the legitimate interests of society by taking an approach that is efficient (achieves the objective) but affects the rights as little as possible. Specific provisions on the treatment of personal data collected by the national competent authorities for the enforcement of the Regulations have been introduced during the revision of the Regulations in 2013, following the advice provided by the European Data Protection Supervisor.

The two Regulations jointly implement Article 12 of the 1988 UN Convention against Illicit Traffic in Narcotic Drugs and Psychotropic Substances in the EU. Adherence to this Convention is almost universal.

In the regard the Regulations are part of a global control and monitoring system for drug precursors under the umbrella of the United Nations.

EU Drugs Strategy (2013-2020) and EU Action Plan on Drugs (2013-2016 and 2017-2020)

1. Legal framework

The European Agenda on Security stresses that the market for illicit drugs remains the most dynamic of criminal markets. It states that the EU should continue to support Member States' activities in fighting illicit drugs

The EU Drugs Strategy provides the overarching political framework and priorities for EU drugs policy, identified by Member States and EU institutions, for the period 2013-20. 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, the second one covering 2017-2020[153].

2. Analysis

The EU Drugs Strategy and Action Plan articulate a consensus among Member States as to the key features of an effective drugs policy. They identify the relevant actors who play a role in a holistic and multidisciplinary approach to drugs policy. The Strategy is based on a five pillar structure consisting of two main policy areas, the reduction of the drug demand and the reduction of drug supply, and three cross-cutting themes: coordination, international cooperation and information research, monitoring and evaluation.

The Communication on the evaluation of the EU Drugs Strategy 2013-2020 and Action Plan 2013-16 which includes a proposal for a new Action Plan on Drugs for 2017-20 based on the findings of the evaluation was adopted by the Commission on 15 March 2017.[154]

The Strategy and Action Plan are structured around two policy areas: drug demand reduction and drug supply reduction and aim at protecting the security and the health of EU citizens.

[153] Adopted by the Council of the EU on 20 June 2017.
[154] COM (2017) 195 final.

The Strategy requires the Commission to initiate and external midterm assessment of the Strategy by 2016, in view of preparing a second Action Plan for the period of 2017-20. According to the evaluation,[155] the Strategy and the Action Plan continue to address adequately the current needs in relation to drugs policy at EU, national and international levels. All areas tackled in the Strategy and Action Plan 2013-16 remain relevant for addressing all aspects of the drugs phenomenon.

The evaluation found that there was widespread agreement of stakeholders that there is a continued need for an Action Plan. They considered it necessary to continue setting out precise priorities and actions relating to each objective, to assign responsibly and to formulate specific measurable indicators. The Strategy and Action Plan provided added value to individual Member States (and other non-state actors) and their strategies by establishing a common EU-wide strategic framework and by institutionalising a process of consensus building for increasingly complex and international issues. None of them imposes legal obligations, but the evaluation found that they have been successful in broadly directing collective action in the field of drugs and promoting a shared model with a culture of defining priorities, objectives, actions and indicators for measuring performance. The priorities and actions of the EU Drugs Strategy and Action Plan have, according to the above mentioned evaluation, been found coherent with most other EU relevant polices and strategies, such as the European Agenda on Security and the European Development Consensus, while more synergies need to be built with the EU Health Strategy. The evaluation also found that the EU added value appears more pronounced in terms of demand reduction activities and emerging challenges.

The evaluation pointed to the need for a greater level of focus on the use of new communication technologies in illicit drug production and trafficking and the role of internet in drug prevention. The evaluation also showed that the omission of a discussion on recent trends in cannabis policy was noted by a wide range of stakeholders and represented one of the most frequent items raised when exploring whether there are any issues not covered by the Strategy. The evaluation also indicated that there is room for improvement in implementation and access to risk and harm reduction measures across various Member States. Finally, it also found that a future Action Plan should continue to include actions to monitor new psychoactive substances, to reduce demand for and supply of them, and to reduce harms associated with their use.

The Strategy and Drugs Action Plan frames the EU external policy in the field of drugs. The Strategy and Action Plan adds value to what Member States are doing in terms of enhancing the "voice" of the EU in international fora, providing guidance for candidate and neighbouring countries and a framework for regional bilateral cooperation with third countries. In particular it provided the basis for the EU's longstanding dialogue and cooperation with the CELAC countries and ENP partners and key actors such as the US and Russia. It has provided the framework for the EU candidate countries to work on the alignment of their legislation and the institutional set up, including through cooperation with the EMCDDA to enhance their monitoring of the drugs phenomenon.

Four EU financial programmes provide funding for drug-related projects between 2014-2020, to help implement the objectives set by the EU Drugs Strategy 2013-2020 and to foster cross-border cooperation and research on drug issues:

- The Justice Programme 2014-2020;
- The Internal Security Fund 2014-2020;
- The Health Programme 2014-2020;

[155] https://ec.europa.eu/home-affairs/sites/homeaffairs/files/what-we-do/policies/organized-crime-and-human-trafficking/drug-control/eu-response-to-drugs/20161215_final_report_annexes_en.pdf.

- Horizon 2020.

Support to the implementation of the EU Drugs Strategy 2013-2020 has been provided by the security and Social Sciences and Humanities research programmes in Framework Programme 7 and Challenge 6 (Inclusive, Innovative and Reflective societies) and Challenge 7 (Secure Societies) in Horizon 2020. Several research projects aimed at drug supply reduction have been funded, such as for example: LOTUS[156] (Localization of threat substances in urban societies), CUSTOM (Drugs and precursor sensing by complementing low cost multiple techniques) and DIRAC (Rapid screening and identification of illegal drugs by IR absorption spectroscopy and gas chromatography). The project ALICE RAP[157] looks at addictions and the business of addictions, and the projects funded under the ERA-NET ERANID (European Research Area Network on Illicit Drugs)[158] focus on understanding drug use pathways and society responses to drug use.

Maritime Analysis and Operations Centre (Narcotics) – MAOC (N)

1. Legal framework

MAOC (N) is a treaty-based organisation outside EU law created in 2007: seven EU Member States, France, Ireland, Italy, Spain, Netherlands, Portugal and the United Kingdom established the Centre by an international treaty. MAOC (N) is however mostly funded by the Internal Security Fund of the European Union. MAOC (N) currently benefits from a three year EU grant agreement which ends on 30 September 2018 and provides a budget of € 2.8 million for that period of 36 months, which represents 95% of the eligible costs of MAOC (N). The UK has also provided additional funding. All in all, the UK annual contribution amounts to around € 90k.

2. Analysis

MAOC (N) provides a forum for multi-lateral cooperation to suppress illicit drug trafficking by sea and air. The focus is on cocaine and cannabis trafficking in the Atlantic and the Western Mediterranean.

MAOC (N) again developed well in 2016 with a 52% increase in intelligence exchange managed by the Centre. So far, MAOC (N) has contributed to the seizure of over 122 tons of cocaine and over 377 tons cannabis for a retail value of over 12 billion euros in the EU. MAOC (N) also contributed to the arrest of 913 persons from 63 countries. 11 countries deploy assets in the fight against drug trafficking coordinated by MAOC (N).

Next to MAOC (N) Member States, the US has deployed two liaison officers to MAOC (N) (from the Drug Enforcement Agency under the Ministry of Justice and the US military's Southern Command in Key West/Florida).

Key added value, unique feature and unlike e.g. Europol, MAOC (N) receives and shares law enforcement and military intelligence and also military assets are being deployed, acting on intelligence shared via MAOC (N).

The Centre will celebrate its tenth anniversary in October 2017 with a high level event. This event will not only provide the opportunity to take stock of MAOC (N)'s successes so far but also to look ahead.

From an EU perspective, while preserving its key features, the development and possibly deepening of future cooperation with relevant EU agencies such as Europol, Eurojust, the European Border and Coast Guard Agency, the EMCDDA[159], ESA[160], EMSA[161], the EFCA[162]

[156] http://www.lotusfp7.eu/.
[157] http://www.alicerap.eu/
[158] http://www.eranid.eu/projects/
[159] European Monitoring Centre for Drugs and Drug Addiction.

as well as Interpol comes to mind. In general, MAOC-(N)'s anniversary provides the occasion to evaluate its core business and look ahead, e.g. at expanding more from the maritime domain to trafficking by air, adding further commodities to be controlled, widening the geographical scope of action, admitting more members – or to remain more focused in scope and membership.

Council Decision 2001/419/JHA on the transmission of samples of controlled substances

1. Legal framework

Council Decision 2001/419/JHA is based on Article 30, 31 and 34(2)(c)ex-TEU. Whilst Article 34(2)(c) was repealed by the Lisbon Treaty, Article 30 and 31 were partly replaced by Art. 81, 83 and 87 TFEU. The Council Decision was adopted following an initiative of Sweden.

2. Analysis

The objective of the Council Decision is to establish a system for the lawful transmission between Member States of samples of seized illicit drugs. The facilitation of such exchanges between Member States has the objective to increase the effectiveness of the fight against the illicit production and trafficking of drugs.

Each Member State must designate a national contact point which is the sole body competent for the transmission of samples. The contacts points have to be communicated to the Council Secretariat which publishes the list in the Official Journal.

There is still a need for an EU system for exchanging of samples of seized illicit drugs. The last list of contact points was published by the Council Secretariat end of 2016.

In 2007, the Council evaluated the Council Decision on the basis of a questionnaire sent to the Member States. The evaluation shows, according to summaries of discussions in the Council published in the Council Registry that the United Kingdom, Sweden and Germany were at the time the greatest contributors in the transmission of samples.

The Council Decision is a decision based on a former third-pillar legal basis which excludes any approximation of the laws of the Member States and which is binding without any direct effect (Art. 34(c) ex-TEU).

The Council Decision may serve as a framework for EU candidate countries.

6. Environmental Crime

Directive 2008/99/EC on Environmental Crime (ECD)

1. Legal framework

The Environmental Crime (ECD) was adopted in 2008[163], on the legal basis for environmental policy (ex-Article 175 TEC).

2. Analysis

The ECD is the most important EU legal instrument in relation to environmental crime. It is a complex piece of legislation which criminalises under certain conditions violations of obligations stemming from more than 60 legal instruments (listed in its annexes). The ECD obliges Member States to criminalise unlawful conducts committed intentionally or with at

[160] European Space Agency.
[161] European Maritime Safety Agency.
[162] European Fisheries Control Agency.
[163] Directive 2008/99/EC of the European Parliament and of the Council of 19 November 2008 on the protection of the environment through criminal law (OJ L 328/28, 6.12.2008).

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.

The main objective of the ECD is to protect the environment more effectively[164]. The effects of environmental offences are indeed often extending beyond the borders of the States in which the offences are committed. The availability of criminal penalties demonstrates a social disapproval of a qualitatively different nature compared to administrative penalties or a compensation mechanism under civil law aims. Common rules on criminal offences also make it possible to use effective methods of criminal investigation and assistance within and between Member States. The directive therefore also aims at strengthening compliance with the EU environmental policy. Finally, a secondary objective of the ECD is to ensure a level-playing field for individuals and businesses and to avoid safe-havens for criminals in the EU.

The monitoring of the Member States' transposition of the ECD is coming to an end. Among the main problems detected in the context of the transposition process were the coverage of offences committed by serious negligence, as well as the liability of legal persons and the sanctions imposed on them under national law. Generally speaking, 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, little information is available on its practical implementation and the effectiveness of criminal enforcement in this area. In the context of the Agenda on Security, the European Commission has started reviewing 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.

On 20 October 2016, the European Commission notably organised a first workshop[165] focused on two specific environmental crimes which have a strong organised crime dimension i.e. wildlife trafficking and waste trafficking. The discussion confirmed that the two crimes have a clear organised crime dimension due to their "low risk-high profit ratio" and that they are often associated to other crimes such as corruption, financial crime and forgery of documents. Nonetheless, their detection rate remains rather low and the number of prosecutions or convictions limited, mainly due to the lack of prioritisation, resources and specialization.

This expertise gathering process is being pursued in 2017. A workshop with the four specialised networks of environmental professionals (prosecutors, judges, inspectors and police) was organised in March 2017 by the European Commission in the context of the envisaged Commission initiative on Environmental Compliance Assurance[166].

On the basis of the information collected, a progress report may be produced by the end of 2017. 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.

[164] See in particular recitals 3 and 4 of the Directive.

[165] The workshop was widely attended: 23 Member States, Europol and Eurojust, four specialised networks (ENPE (prosecutors), IMPEL (inspectors), EnviCrimeNet (police) and EUFJE (judges), as well as several NGOs (TRAFFIC, WWF, WCS, IFAW, EFFACE project). The Commission was also present.

[166] http://ec.europa.eu/smart-regulation/roadmaps/docs/2015_env_066_environmental_compliance_assurance_en.pdf.

Having common rules on criminal offences facilitates cooperation between Member States. The above mentioned progress report would notably assess whether and to what extent the ECD has improved European cooperation in the fight against environmental crime.

The review process of the ECD is referred to in the Commission Action Plan on Wildlife Trafficking adopted in February 2016[167]. It is also closely related to the Commission initiative on Environmental Compliance Assurance.

Support to the policy implementation in the field of environmental crime has also been provided by the security research programme in both Framework Programme 7[168] and Horizon 2020.[169] Specifically, the project CWIT "Countering WEEE Illegal Trade" was linked to Directive 2012/19/EU on waste electrical and electronic equipment (WEEE). This project was coordinated by INTERPOL and delivered a market analysis, legal analysis, crime analysis as well as a recommendations roadmap on the trade of illegal electronic waste in the EU.

The EU criminal law policy is based on several pillars: strengthening mutual trust between judicial systems, approximating national laws where necessary, and adopting minimum standards for procedural rights in criminal proceedings, thereby ensuring that fundamental rights are safeguarded. The ECD is an instrument which approximates national laws by imposing on Member States to criminalize certain environmental offenses under certain conditions. Those conditions, including the focus on serious offences, ensure that the principle of proportionality is respected.

The ECD requires Member States to criminalise, inter alia, illegal wildlife trafficking and illegal waste shipments, which often have a trans-boundary dimension.

[167] http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52016DC0087&from=EN.
[168] See: https://ec.europa.eu/research/fp7/index_en.cfm?pg=security .
[169] The full list of security research projects can be found here: https://ec.europa.eu/home-affairs/financing/fundings/research-for-security_en.

IV. Cyber

1. Cyber Crime

Council Framework Decision of 28 May 2001 combating fraud and counterfeiting of non-cash means of payment (2001/413/JHA)

1. Legal framework

The Framework Decision is based on Art 34.2(b) TUE. At the time the Framework Decision was adopted, the Council referred to the political mandate provided by the Action Plan to combat organised crime, approved by the Amsterdam European Council (16 and 17 June 1997), as well as to the Action Plan of the Council and the Commission on how to implement the provisions of the Treaty of Amsterdam on an area of freedom, security and justice, approved by the Vienna European Council on 11 and 12 December 1998.

2. Analysis

The stated objectives of the Framework Decision (rec. 4) are 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, given the international dimension of those offences.

The specific objectives of the Framework Decision are:

- to provide a description of the different forms of behaviour requiring criminalisation in relation to fraud and counterfeiting of non-cash means of payment, covering the whole range of activities that together constitute the menace of organised crime in this regard.

Articles 2 to 5 of the Framework Decision define offences related to payment instruments, to computers and to specifically adapted devices

- to make sure that the above mentioned forms of behaviour are classified as criminal offences in all Member States, and that effective, proportionate and dissuasive sanctions be provided for natural and legal persons having committed, or being liable for, such offences.

Articles 6, 7 and 8 set out provisions related to these objectives

- to provide for the widest measure of mutual assistance between Member States and enhance cooperation.

Articles 9 (on jurisdiction), 10 (on extradition and prosecution) and 11 (on cooperation) define rules to this aim.

The Commission produced two complementary reports on the implementation of the Framework Decision (in 2004 and 2006 respectively), which show how Member States used the margins of discretion left by the Framework Decision (e.g. by setting very different levels of penalties for the same offence).

In the meanwhile, technological developments and new emerging criminal activities (as identified by Europol in its Internet Organised Crime Threat Assessment[170]) have brought the Commission to outline plans for future initiatives and actions in its European Agenda on Security, recognising the need to look into renewing common rules at EU level to combat fraud and counterfeiting of non-cash means of payment.

The protection of citizens against such crimes and their investigation and prosecution has proven difficult for a number of reasons:

[170] https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment-iocta-2016.

- Certain behaviours, while harmful to society, are not criminalized as they constitute a new modus operandi not yet covered by present-day rules.
- Current EU rules on fraud and counterfeiting of non-cash means of payment are insufficiently technology neutral: for example, they only cover physical (corporeal) payment instruments, i.e. a plastic card or a cheque.
- Furthermore, investigations are often limited to the acts committed within the country, if not for legal, then for practical reasons. Even where criminality could be established, non-cash payment fraud offenses now frequently go at least partially unsanctioned, leading to low overall criminal sanctions and a swift release of the perpetrators – and therefore low deterrence.
- Law enforcement is limited in its use of investigative tools. One driver of this problem lies in lower levels of sanctions as use of investigative tools is often restricted to crimes of a certain severity, as reflected in sanctions applied.
- The fight against non-cash payment fraud is not a priority in many Member States. This is in part due to its nature as a high-volume, low individual impact crime as criminals often defraud many victims of smaller sums, and in part due to low sanction levels which have a strong influence on national priority setting.
- Cooperation between law enforcement agencies of different Member States can be challenging, due to the divergence in national laws as certain behaviour may be criminalized in one Member State but not in another, or may be sanctioned at very different levels.
- Victims may suffer from long-term impacts of identity theft, such as negative entries in their credit history. The underlying cause is the lack of well-established victims' rights when faced with identity theft.
- There is little reliable and detailed information both on individual cases and on the overall scale and impact of non-cash payment fraud available to law enforcement. The private sector plays a key role here because close to all infrastructure affected by the crimes is privately owned; cooperation, incentives and well-established reporting channels are therefore of the essence.
- Moreover, the knowledge about the size and nature of criminal activities related to fraud and counterfeiting of non-cash means of payment and the effectiveness of the law enforcement response is still partial and fragmented, in the absence of comparable statistics.

The Commission published an Inception Impact Assessment[171] in May 2016, where it 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.

Non-cash payment frauds affect the trust of the public in digital services and undermine the strengthening of the digital single market. Fraudsters manage to adapt rapidly their modi

[171] http://ec.europa.eu/smart-regulation/roadmaps/docs/2016_home_077_non_cash_payment_en.pdf.

operandi to evolving technologies and exploit legal loopholes and discrepancies, setting up transnational criminal networks, posing challenges to law enforcement.

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). However, the Policy Cycle has also contributed to identify gaps that still exist and challenges (e.g. on coordinated action against "carding websites" selling bundles of compromised credit card credentials online).

EU-funded projects have also created synergies and stimulated public-private cooperation, with the aims of improving law enforcement capacity (for instance through the RAMSES project,[172] funded under the Secure Societies strand of Horizon 2020), assisting victims (for example through the PROTEUS project[173]) and enhancing reporting of fraudulent transactions by financial institutions (as in the case of the OF2CEN project,[174] funded under the ISEC programme and its successor, EU OF2CEN, funded under the Internal Security Fund - Police). Again, this allowed identifying some shortcomings in the current framework (e.g. capacity of sharing valuable information across borders).

Support to the policy implementation in the field of combating fraud and counterfeiting of non-cash means of payment has also been provided by the security research programme in both Framework Programme 7[175] and Horizon 2020[176]. For example, the FP7 project E-CRIME ("The economic impacts of cybercrime") delivered a set of reports and guidelines regarding economic impacts of cybercrime and anti-cybercrime measures. Furthermore, the recently signed Horizon 2020 project TITANIUM ("Tools for the Investigation of Transactions in Underground Markets") is required to develop methods and technical solutions for investigating and mitigating illegitimate activities involving virtual currencies and/or underground market transactions.

In relation to fundamental rights, the following considerations, linked to a possible future initiative, should be taken into account:

A) *Penalties*: the definition of common minimum maximum levels of penalties for different offences may facilitate law enforcement cooperation. The level of sanctions needs to be effective, proportionate and dissuasive.

B) *Protection of personal data*: by its own nature, non-cash payment fraud is based on identity theft. Effective enforcement of clear rules on data theft and trade and proportionate criminal sanctions may complement the security and data breach rules to create better data protection. The deterrent effect of more successful investigations and proportionate sanctions could further enhance the prevention of identity theft and protection of personal data. At the same time information gathering and sharing (e.g. in public-private cooperation) required to fight crime can also affect the privacy rights of the victims or third parties where their personal data is concerned.

C) *Victims' rights*: measures to strengthen victims' rights such as procedural safeguards for the rectification of negative entries in victims' credit history may be considered.

Operational law enforcement cooperation spans to countries where organised crime groups active in Europe conduct parts of their activities (e.g. cashing out in Central America or

[172] http://ramses2020.eu/project/.
[173] http://www.apav.pt/proteus/index.php/en/.
[174] http://www.poliziadistato.it/articolo/30663.
[175] https://ec.europa.eu/research/fp7/index_en.cfm?pg=security.
[176] https://ec.europa.eu/programmes/horizon2020/en/h2020-section/secure-societies-%E2%80%93-protecting-freedom-and-security-europe-and-its-citizens.

South-East Asia countries). Discussions on prevention of non-cash payment fraud also took place in 2016 in the framework of the G7 Roma-Lyon Group.[177]

Directive 2011/93/EU on combatting the sexual abuse and sexual exploitation of children and child pornography

1. Legal framework

Sexual abuse and sexual exploitation of children are particularly serious forms of crime with a cross border dimension, as listed in Art. 83 TFSU. 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 stated in Article 24 of the Charter of Fundamental Rights of the European Union.

Online child sexual abuse is a nefarious crime with long-term consequences for its victims. Harm is caused not only when abuse is actually recorded or photographed, but also every time the images and videos are posted, circulated and viewed. For the victims, the realisation that the images and videos in which they are abused are 'out there' and that they could even encounter someone who has seen the material is a major source of trauma and additional suffering.

A major step in the EU action to address these phenomena was the adoption of Directive 2011/93/EU on combating the sexual abuse and sexual exploitation of children and child pornography (the Directive), which replaced the Council Framework Decision 2004/68/JHA of 22 December 2003 on combating the sexual exploitation of children and child pornography.

While the Commission reported that almost all of the Member States had ensured a high level of protection of children from sexual exploitation and abuse, and had adopted the necessary criminal law measures, including an appropriate level of penalties, there were a number of issues that the Framework Decision was not dealing with.[178] 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 as highly necessary for effectively combatting the sexual abuse of children. Benefitting from the new treaty environment ensured by the Treaty of Lisbon and seeking to extend the scope of the Framework Decision, the Commission tabled its new legislative proposal in 2009[179], which resulted into the Directive.[180]

The Directive takes numerous elements from the 2007 Council of Europe Convention on Protection of Children against Sexual Exploitation and Sexual Abuse (Lanzarote Convention), which has been ratified to date by 42 countries, including 26 EU Member States (all except UK and IE).

2. Analysis

The Directive is a comprehensive legal instrument that sets out minimum standards to be applied throughout the European Union. It follows a holistic approach to tackle these crimes

[177] The G7 Roma/Lyon Group (R/L) is a working group that was first set up under the Italian presidency of the then G8 in 2001. It debates and develops issues and strategies relating to public security in an effort to combat terrorism and transnational crime.
[178] 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 Brussels, 16.11.2007 COM(2007) 716 final.
[179] Proposal for a Directive of the European Parliament and of the Council on combating the sexual abuse, sexual exploitation of children and child pornography, repealing Framework Decision 2004/68/JHA COM/2010/0094 final - COD 2010/0064.
[180] Combating Child Sexual Abuse Online, Study for the LIBE Committee, European Parliament, 2015.

effectively, incorporating provisions covering investigation and prosecution of offences, assistance and protection of victims, and prevention.

Specifically, to effectively **investigate and prosecute offences**, the Directive notably includes criminalisation of a wide range of situations of child sexual abuse and exploitation, online and offline. These include new phenomena such as online grooming and webcam sexual abuse and online viewing of child abuse images without downloading them.

With regard to **assistance to and protection of child victims**, the Directive notably includes provisions requiring extensive assistance, support and protection measures, in particular to prevent child victims from suffering additional trauma through their involvement in criminal investigations and proceedings, inter alia by setting specific standards for interviews with child victims.

Finally, **to prevent these crimes**, the Directive notably includes mechanisms to enable excluding convicted offenders from professional activities involving direct and regular contact with children and a requirement that Member States make intervention programmes or measures such as treatment available to convicted offenders and others who fear they could offend.

The Commission is currently monitoring the implementation of the Directive and there is still considerable scope for the Directive to reach its full potential. Given the comprehensive nature of the Directive, the first priority is to ensure that children benefit from the full added value of the Directive through its complete and correct implementation by Member States, before proposing amendments or any complementary legislation.

The European Parliament, in its 2015 Study for the LIBE Committee on Combatting Child Sexual Abuse, found that "[The Directive] is up-to date, sufficiently nuanced and comprehensive to combat online child sexual abuse."[181]

There are, however, a number of issues not covered in the Directive which could be the object of future EU legislation or policy, after the Directive is fully implemented. For example:

- Mandatory background checks for employment and volunteering relating to children.
- 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).
- Better management of travel by convicted child sex offenders and exchange of information on individuals posing a risk for children.
- Allow hotlines to search child sexual abuse material proactively (like IWF in the UK).
- Enlarging the investigation tools, in view of new challenges, especially in the technological field, such as anonymization, darknet, P2P networks and live streaming.

The fight against child sexual abuse is directly influenced by common issues affecting the fight against cybercrime, including encryption, jurisdiction issues on access to digital evidence and data retention.

As identified in the impact assessment study, the broader approach of the Directive compared to the Framework Decision it replaces, including the combination of legislative and non-legislative instruments enables Member States to better achieve the different objectives mentioned above, since the obligation to establish a legal framework for certain measures is complemented by guidance based on best practice and other tools to improve its implementation through cooperation at the EU level.

[181] Combating Child Sexual Abuse Online, Study for the LIBE Committee, European Parliament, 2015, p12.

To facilitate the implementation of the Directive and the achievement of its objectives, the Commission has funded several initiatives:

- To combat the distribution of material depicting child sexual abuse online, the Commission co-funds the INHOPE network of hotlines that work in partnership with law enforcement and the internet industries.
- The Commission has also funded projects targeting the online exchange of child abuse images and facilitation of live abuse, such as the European Financial Coalition.
- The Commission also co-funds EU-wide awareness raising to empower children and their parents and educators, such as the Better Internet for Kids initiative under the Connecting Europe Facility programme (and formerly under the Safer Internet Programmes established in Decision No 1351/2008/EC of the European Parliament and of the Council of 16 December 2008 establishing a multiannual Community programme on protecting children using the Internet and other communication technologies).
- In addition, the Commission continues supporting INTERPOL in enhancing global law enforcement cooperation in this area, in particular with regard to identification of child victims depicted in child sexual abuse material (e.g. through grants totalling 3.6M Euros invested in the development and continuous improvement of the International Child Sexual Exploitation image database, a key tool to identify child victims globally).
- Furthermore, the Commission also funds research to combat child sexual abuse and help identify victims more effectively, for example through the ASGARD and EVIDENCE projects under Horizon 2020.

Support to the policy implementation in the field of cross-border access to electronic evidence and the role of encryption in criminal investigations has also been provided by the security research programme in both Framework Programme 7[182] and Horizon 2020[183]. Specifically, the on-going Horizon 2020 project ASGARD ("Analysis System for Gathered Raw Data") is joining forces with Europol, with regard to the research of possible tools that could be used in the identification of victims of child sexual abuse. Outcomes of the project will be provided to policy makers.

The Directive includes several provisions that relate to the protection of Fundamental Rights:

- Use the best interest of the child as a primary consideration in all actions related to children (Article 24(2) of the Charter of Fundamental Rights of the EU).
- Optional blocking measures to be implemented taking account of the rights of the end users and complying with existing legal and judicial procedures and the European Convention for the Protection of Human Rights and Fundamental Freedoms and the Charter of Fundamental Rights of the European Union.

The preliminary conformity assessment of the transposition measures taken by Member States to implement the Directive has identified a number of possible non-conformities in the safeguards concerning the blocking measures in a number of Member States. Bilateral dialogues with Member States will take place to address these issues, before Commission enforcement powers under the Treaties may be used where needed.

Child sexual abuse and child sexual exploitation are unfortunately global phenomena. International cooperation to fight against these crimes is therefore critical.

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

[182] https://ec.europa.eu/research/fp7/index_en.cfm?pg=security.
[183] https://ec.europa.eu/programmes/horizon2020/en/h2020-section/secure-societies-%E2%80%93-protecting-freedom-and-security-europe-and-its-citizens.

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 will include more than 70 countries, along with major international organisations, technology companies, and leading civil society organisations.

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

The ongoing work within the Commission with regard to cross-border access to digital evidence as well as encryption 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 of the Directive concerned include those on jurisdiction, offences concerning child pornography and solicitation of children for sexual purposes.

Directive 2013/40/EU on attacks against information systems and replacing Council Framework Decision 2005/222/JHA

1. Legal framework

The legal basis of the Directive is Article 83(1) of the TFEU. The Directive replaced Council Framework Decision 2005/222/JHA. The Council Conclusions of 27 to 28 November 2008 indicated that a new strategy should be developed with the Member states and the Commission.

2. Analysis

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 approximates criminal law of the Member States in the area of attacks against information systems by establishing minimum rules concerning the definition of criminal offences and the relevant sanctions, and to improve cooperation by competent authorities by obliging Member States to establish a network of national operational points of contact. This obligation strengthens the importance of the networks that have been 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.

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 should be considered to also take into account procedural elements relating to cross-border access to electronic evidence and the role of encryption in criminal investigations, which are currently subject of ongoing policy development processes of the Commission following Council Conclusions on improving criminal justice in cyberspace[184] and the outcome of the debate of the Council on the role of encryption in criminal investigations.[185].

The Commission is currently assessing the conformity of the transposition of the Directive by Member States by means of a study of Member States' legislation that was notified for that purpose. According to Article 17 of the Directive, the Commission shall submit in September

[184] 9 June 2016 Conclusions of the Council of the European Union on improving criminal justice in cyberspace, doc. 10007/16.
[185] Outcome of the Council meeting of 8 and 9 December 2016, doc. 15391/16.

2017 a report to the European Parliament and the Council, assessing the transposition of the Directive by Member States and "accompanied, if necessary, by legislative proposals".

Subject to the ongoing assessment of the conformity of the transposition by Member States[186], it appears that the use of approximated definitions of criminal offences and the relevant sanctions have improved operational cooperation between Member States' authorities on specific investigations, notably as the use of procedural measures is often dependent on a certain minimum level of sanctions. In addition, the obligation for Member States to establish a network of national operational points of contact has been facilitating operational cooperation between Member States' authorities in specific investigations, e.g. for the exchange of information. It is not likely these objectives could have been reached at Member State level only, as Member States' definitions of offences and levels of sanctions initially diverged. Similarly, the organisation and functioning of operational points of contact differed per Member State. A further harmonisation of these elements could not have been reached at Member State level only, and might actually have been aggravated by separated national developments without coordination at European Union level.

Support to the policy implementation in the field of cross-border access to electronic evidence and the role of encryption in criminal investigations has also been provided by the security research programme in both Framework Programme 7[187] and Horizon 2020[188]. Specifically, the FP7 project EVIDENCE ("European Informatics Data Exchange Framework for Courts and Evidence")[189] addresses creation of a Common European framework for the correct and harmonised handling of electronic evidence during its entire lifecycle: collection, preservation, use and – in particular – exchange of electronic evidence. The project is providing useful inputs to EU policy makers regarding cross-border access to electronic evidence.

The Directive respects fundamental rights recognised in particular by the Charter of Fundamental Rights of the European Union. No provisions of the Directive have a particular effect on fundamental rights. Cybercrime is a global phenomenon, and the Directive takes account of that by including a broad scope for the exercise of jurisdiction by Member States over the offences covered, e.g. when the effect of a cyberattack takes place in a Member State. It also provides for optional grounds for jurisdiction, the transposition of which by Member States are currently being assessed.

As to the external dimension, the ongoing policy development processes of the Commission on cross-border access to electronic evidence and on the role of encryption in criminal investigations will provide further input in support of the external dimension of the Directive. Increasingly, authorities involved in cybercrime investigations encounter obstacles relating to cross-border access to electronic evidence or encryption, in particular when those investigations have a cross-border element.

The main multilateral framework for the fight against cybercrime is the 2001 Council of Europe Budapest Convention on Cybercrime.[190] The European Union is not a party to the Convention, but currently 26 EU Member States have signed and ratified the Convention. Ireland and Sweden have signed but not yet ratified. The Directive builds on the Convention and provides for measures to ensure a conform transposition by European Union Member States. The Budapest Convention also covers additional elements, including on procedural law providing for cross-border access to electronic evidence, which are currently not yet covered by European Union legislation.

---

[186] Overall report on the transposition of Directive 2013/40/EU, December 2016 (not published).
[187] https://ec.europa.eu/research/fp7/index_en.cfm?pg=security.
[188] https://ec.europa.eu/programmes/horizon2020/en/h2020-section/secure-societies-%E2%80%93-protecting-freedom-and-security-europe-and-its-citizens.
[189] European Informatics Data Exchange Framework for Courts and Evidence, http://www.evidenceproject.eu/
[190] Council of Europe Convention on Cybercrime (ETS No. 185).

2. Cyber Security

Regulation (EU) 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 carrying out a full evaluation of ENISA, as requested by art.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, expected in autumn 2017 will be then presented to the European Parliament and the Council. The text below therefore represents only a very preliminary assessment by the Commission services.

1. Legal framework

The Regulation concerning the European Union Agency for Network and Information Security (ENISA) was established on the basis of the Art. 114 of TFEU (internal market). The internal market legal basis supported as well the previous founding regulation of ENISA Regulation 460/2004.

2. Analysis

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.

This general mission translates into specific objectives as it follows:

- Developing and maintaining a high level of expertise of EU actors.
- Assisting Member States and the EU institutions in developing policies necessary to meet the legal and regulatory requirements in the network and information security field.
- Assisting Member States and the Commission in enhancing capacity building throughout the EU.
- Stimulate cooperation both between Member States of the EU and between related NIS communities.

ENISA carries out its activities according to an annual and multiannual work programme. It has been 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.

A preliminary remark on this area is that, despite some limitations (in particular linked to the limited resources granted to the agency), ENISA did provide an important contribution in the following areas:

- Cooperation between Member States and NIS stakeholders.
- Community building across Member States.
- Cooperation between CERTs/CSIRTs.

- Capacity building in Member States (in particular in the smaller MSs).

According to article 3.f) of ENISA's regulation, the agency should contribute to the Union's efforts to cooperate with third countries and international organisations to promote international cooperation on network and information security issues.

ENISA's international activities have so far been limited. The agency advises on international matters when requested to do so by the EU institutions, it engages as observer in the organisation of international cyber-exercises and contributes to conferences and events with an external dimensions. However, due to the small size of the agency and the need to prioritize its activities on the internal affairs, the international dimension of its work has not been very developed.

Directive on Security of Network and Information Systems (NIS-Directive)

1. Legal framework

The NIS-Directive[191] is based on Article 114 TFEU. The legal act constitutes an important element of the implementation of the 2013 EU Cybersecurity Strategy[192].

2. Analysis

The objective of the NIS Directive is to achieve a high common level of security of network and information systems within the EU. This means improving the security of the Internet and the private network and information systems underpinning the functioning of our society and economy. In particular this should be achieved by:

- improving national cybersecurity capabilities, which are currently uneven across the EU;
- enhancing EU-level cooperation in cybersecurity, which takes place in small and closed circles
- ensuring risk management and incident reporting for operators of essential services and digital service providers.

More specifically, the directive aims at ensuring **Member States preparedness** by requiring them to be appropriately equipped, notably by having in place a Computer *Security Incident* Response Team (CSIRT), a competent national *NIS authority and national NIS strategy*. Furthermore, the legal act aims at enhancing **cooperation** among all the Member States, by setting up a 'Cooperation Group', in order to support and facilitate strategic cooperation and the exchange of information among Member States, and a 'CSIRT Network', in order to promote swift and effective operational cooperation on specific cybersecurity incidents and sharing information about risks. And finally, the directive requires businesses in sectors with an important role for society and economy such as transport, energy, water and banking sectors that are identified by the Member States as operators of essential services under the directive to take appropriate security measures and to notify serious incidents to the relevant national authority. Also providers of key digital services (i.e. search engines, cloud computing services and online marketplaces) will need to comply with security and notification requirements. This measure pursues the objective to establish a culture of security across sectors which are vital for our economy and society and moreover rely heavily on information and communications technologies (ICT).

[191] Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union, OJ L 195, 19.7.2016, p.1.
[192] JOIN(2013) 1 final.

The NIS Directive is a new legal act which entered into force in August 2016 and is currently subject to transposition into national law by Member States. The deadline for transposition is 9 May 2018.

For the time being, the Member States have very different levels of capabilities and preparedness, leading 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 will 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.

The measure has a strong positive impact for the effective protection of fundamental rights, and specifically the rights to the protection of personal rights and privacy. In this context, Recital 75 of the directive states that the legal act respects fundamental rights and principles enshrined in the Charter of Fundamental Rights of the European Union, in particular the right to respect for private life and communications, the protection of personal data, the freedom to conduct a business, the right to property, the right to an effective remedy before a court and the right to be heard. Moreover, the recital stipulates that those fundamental rights should also be respected by the implementation of the directive. With regard to the processing of personal data for the purposes of the Directive, Article 2 explicitly refers to Directive 95/46/EC and Regulation (EC) No 45/2001.

In the context of international cooperation, Article 13 of the directive states that international agreements concluded by the Union in accordance with Article 218 TFEU may allow and organise the participation of third countries or international organisations in some activities of the Cooperation Group.

Contractual Public Private Partnership on Cybersecurity

1. Legal framework

This contractual Public Private Partnership on cybersecurity (cPPP) is one of the 16 initiatives put forward in the Commission's Digital Single Market Strategy.[193] 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[194] and constitutes an important element of the implementation of the 2013 EU Cybersecurity Strategy.[195] The contract between the European Commission and the industry represented by the European Cybersecurity Organisation (ECSO) was signed on 5 July 2016.

2. Analysis

Even though the whole value chain of digital technologies may not be mastered in Europe, there is a need to at least retain and develop certain essential capacities and ensure that European citizens, enterprises (including SMEs), public administrations have access to the latest digital security technology developments, which are interoperable, competitive, trustworthy and based on European rules and values.

A more joined-up approach can help step up the supply of more secure solutions by industry in Europe and stimulate their take-up by enterprises, public authorities, and citizens. In this context, the cPPP gathers industrial and public resources to deliver excellence in research and

[193] COM(2015) 192 final.
[194] COM(2016) 410 final.
[195] JOIN(2013) 1 final.

innovation and maximise the use of available funds through greater coordination with Member States and regions.

The cPPP should help achieve the above goal by stimulating cybersecurity industry through:

- **building trust among Member States and industrial actors** by encouraging cooperation at early-stage research;
- **aligning the demand and supply sectors for cybersecurity products and services** - allowing the cybersecurity industry to understand better the requirements of end-users and customers of cybersecurity solutions (e.g. energy, health, transport, finance);
- **developing common, sector-neutral and replicable building blocks** to help ensure compatibility of solutions across borders, while allowing flexibility for products to be further adapted to the needs of specific markets or customers.

The Commission's experience with the existing digital Public-Private Partnerships shows that they enable the partners to develop a long-term, strategic approach to research and innovation and reduce uncertainties by allowing for long-term commitments.

For the purpose of this Partnership the industry has prepared a Strategic Research and Innovation Agenda, which offers a vision and defines priorities for cybersecurity research and innovation for Europe. The cPPP partners remain in continuous dialogue with the European Commission to advise on the Work Programme under Horizon 2020.

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.

The European cybersecurity industry has been very fragmented. Historically, industrial development in this area has been stimulated by governmental purchase and some highly innovative European companies in this sector are still largely dependent on public procurement in their home country. A side effect of this situation is limited willingness for cross-border purchasing, which is a barrier to the development of a common cybersecurity market. At the same time smaller, newer players while initiating their business in limited, country markets, struggle with making international expansion as buying behaviours can be biased towards established (often global) brands that can leverage strong market presence and marketing budgets to protect their market share from new entrants.

Until recently, whereas some initiatives across a few Member States aimed to bring together the competencies and industrial players in this area, potentially helping European companies to join forces and expand across a number of European countries, the fragmentation has been still considerable: the industry was nowhere near some more structured segments of the ICT industry, such as microelectronics, where well-established regional cluster of excellence and ecosystems can be identified, leveraging academia, industrial, institutional and customers/users capacities, and enabling this industry to compete on a global scale.

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. ECSO is a fully self-financed non-for-profit association (ASBL) under Belgian law. ECSO became a legal counterpart for the contractual cPPP signed with the Commission in July 2016. Since its launch the organisation was joined by more than 180 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.

Under EU research and innovation programme Horizon 2020, the EU will invest €450 million in calls for proposals related to this partnership. There is a continuous dialogue between the

cPPP partners and the European Commission in order to provide advices on the Work Programme under Horizon 2020.

The measure has potentially a strong positive impact on the effective protection of fundamental rights (including protection of personal data and privacy) if it results in research and innovation projects that can help better protect citizens and businesses against cybersecurity and privacy threats.

At the moment the initiative focuses on strengthening cybersecurity industrial capacity in Europe. However, as cybersecurity is a global challenge a dialogue with global partners is also taking place and a number of global players in cybersecurity have also decided to join the initiative.

V. Information exchange and operational cooperation

1. Information Systems and Interoperability

Schengen Information System (SIS)

1. Legal framework

The current legal framework for the second generation of SIS is based upon a former third pillar instrument: Council Decision 2007/533/JHA[196] and a former first pillar instrument: Regulation (EC) No 1986/2006[197]. Additional provisions allowing national services responsible for issuing vehicle registration certificates to access SIS are contained in Regulation (EC) No 1986/2006[198]. Transitional provisions moving from the first generation of SIS to the second are laid out in Commission Decision 2009/724/JHA[199] and the requirements relating to the security plan for the Central SIS and its communication infrastructure are set out in Commission Decision 2010/261/EC[200].

2. Analysis

The Schengen Information System (SIS) 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. 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. This included assessing the most effective way for Europe-wide information sharing and legal assistance for the carrying out of national law enforcement, immigration and judicial decisions. It was clear that these could no longer be achieved with traditional bilateral agreements and mutual legal assistance requests, due to the rapid movement of criminals and the need to act promptly. SIS allowed 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) was introduced, entering into operation on 9 April 2013 and providing Member States with enhanced functionalities and new object categories.

Effective information exchange amongst Member States, and between Member States and the relevant EU agencies, is essential to providing a robust response to the challenges of migration management, integrated border management of the EU's external borders and the fight against terrorism and cross-border crime, and to building an effective and genuine Security Union.

Competent authorities in the Member States such as police, border guards and customs officers need to have access to high quality information about the persons or objects they are checking, with clear instructions about what needs to be done in each case. SIS is at the very

[196] Council Decision 2007/533/JHA of 12 June 2007 on the establishment, operation and use of the second generation Schengen Information System (SIS II) (OJ L 205, 7.8.2007, p. 63).
[197] Regulation (EC) 1986/2006 of the European Parliament and of the Council of 20 December 2006 regarding access to the Second Generation Schengen Information System (SIS II) by the services in the Member States responsible for issuing vehicle registration certificates (OJ L 381, 28.12.2006, p. 1).
[198] Regulation (EC) No 1986/2006 of the European Parliament and of the Council of 20 December 2006 regarding access to the Second Generation Schengen Information System (SIS II) by the services in the Member States responsible for issuing vehicle registration certificates.
[199] Commission Decision 2009/724/JHA of 17 September 2009 laying down the date for the completion of migration from the Schengen Information System (SIS 1+) to the second generation Schengen Information System (SIS II).
[200] Commission Decision 2010/261/EC of May 2010 on the Security Plan for Central SIS II and the communication infrastructure.

heart of Schengen cooperation and plays a crucial role in facilitating the free movement of people within the Schengen area. It enables competent authorities to enter and consult data on wanted persons, persons who may not have the right to enter or stay in the EU, missing persons – in particular children – and objects that may have been stolen, misappropriated or lost. The system not only contains information about a particular person or object but also clear instructions for the competent authorities on what to do with that person or object once found.

The Commission carried out a comprehensive evaluation[201] of the functioning of the second generation of SIS in 2016, 3 years after its entry into operation. This evaluation showed that SIS is functioning effectively and is a genuine operational success. SIS is the most successful tool for the effective cooperation of immigration, police, customs and judicial authorities in the EU and the Schengen associated countries. It is the most widely used information-sharing tool in Europe, with approximately 72 million records. In 2016, it was consulted almost 4 billion times by about 2 million end-users throughout 29 European countries.

Notwithstanding the successes of the system, the evaluation noted a number of areas where operational and technical improvements could be made. Some of these changes require legislative change and, to that end, the Commission adopted proposals for three Regulations on 21 December 2016[202].

The evaluation[203] examined this issue in detail, providing a comprehensive assessment of the added value provided by the EU. It found that the EU adds significant value through the creation and maintenance of SIS. In particular, the system provides significant EU added value as the key compensatory measure for the removal of internal borders between the Member States, in a way that could not be achieved without a pan-European approach. Furthermore, the level of information exchange between Member States through SIS cannot be achieved via decentralised, national solutions. The system provides for easier, more effective and more efficient information exchange between Member States on issues where time is often of the essence, leading to more effective and efficient law enforcement and stronger, more secure external borders.

The new SIS legal proposals, adopted by the Commission on 21 December 2016 are closely linked with and complement other Union policies, namely:

- **Internal security** as underlined in the European Agenda on Security[204] and the Commission's work towards an effective and genuine Security Union[205], to prevent,

[201] COM(2016) 880 - Report from the Commission to the European Parliament and the Council on the evaluation of the second generation Schengen Information System (SIS II) in accordance with art. 24 (5), 43 (3) and 50 (5) of Regulation (EC) No 1987/2006 and art. 59 (3) and 66 (5) of Decision 2007/533/JHA; and SWD(2016) 450 - Commission Staff Working Document accompanying the Report from the Commission to the European Parliament and the Council on the evaluation of the second generation Schengen Information System (SIS II) in accordance with articles 24 (5), 43 (3) and 50 (5) of Regulation (EC) No 1987/2006 and articles 59 (3) and 66 (5) of Decision 2007/533/JHA.

[202] COM(2016)0883 final - 2016/0409 (COD) - Proposal for a Regulation of the European Parliament and of the Council on the establishment, operation and use of the Schengen Information System (SIS) in the field of police cooperation and judicial cooperation in criminal matters, amending Regulation (EU) No 515/2014 and repealing Regulation (EC) No 1986/2006, Council Decision 2007/533/JHA and Commission Decision 2010/261/EU; COM/2016/0882 final - 2016/0408 (COD) - Proposal for a Regulation of the European Parliament and of the Council on the establishment, operation and use of the Schengen Information System (SIS) in the field of border checks, amending Regulation (EU) No 515/2014 and repealing Regulation (EC) No 1987/2006; COM/2016/0881 final - 2016/0407 (COD) - Proposal for a Regulation of the European Parliament and of the Council on the use of the Schengen Information System for the return of illegally staying third-country nationals.

[203] SWD(2016) 450 - Commission Staff Working Document accompanying the Report from the Commission to the European Parliament and the Council on the evaluation of the second generation Schengen Information System (SIS II) in accordance with articles 24 (5), 43 (3) and 50 (5) of Regulation (EC) No 1987/2006 and articles 59 (3) and 66 (5) of Decision 2007/533/JHA.

[204] COM(2015) 185 final.

detect, investigate and prosecute terrorist offences and other serious crime by enabling law enforcement authorities to process personal data of persons suspected to be involved in acts of terrorism or serious crimes.
- **Data protection** insofar as the new proposals provide safeguards aimed at limiting the impact on fundamental rights of individuals whose personal data is processed in SIS.

The new proposals are also closely linked with and complement existing Union legislation, namely:

- **European Border and Coast Guard** as regards their access to SIS for the purposes of the proposed European Travel Information and Authorisation System (ETIAS)[206], as well as for providing a technical interface for SIS access to European Border and Coast Guard Teams, teams of staff involved in return-related tasks and members of the migration management support team to, within their mandate, have the right to access and search data entered in SIS.
- **Europol** insofar as the new proposals grant Europol additional rights to access and search of data, within its mandate, that have been entered in SIS.
- **Prüm** insofar as the developments in the new proposals to enable the identification of individuals on the basis of fingerprints (as well as facial images and DNA profiles) complement the existing Prüm provisions[207] on mutual cross-border online access to designated national DNA databases and automated fingerprint identification systems.

The new SIS proposals are also closely linked with and complement future Union legislation, namely:

- **Management of external borders** insofar as the new proposals complement the new principle in the Schengen Borders Code of systematic checks against relevant databases of all travellers, including EU nationals, upon entry and exit to the Schengen area, as established in response to the foreign terrorist fighter phenomenon.
- **Entry/Exit System** as the new proposals seek to reflect the proposed use of a combination of fingerprint and facial image as biometric identifiers for the operation of the Entry/Exit System (EES).
- **ETIAS** insofar as the new proposals take into account the proposed ETIAS which provides for a thorough security assessment, including a check in SIS, of third-country nationals who intend to travel in the EU.

In accordance with data protection principles, all individuals whose data are processed in SIS II have the following specific rights under Article 41 of the SIS II Regulation and Article 58 of the SIS II Decision:

- the right of access to data relating to them stored in the SIS II.;
- the right to correct inaccurate data or have data deleted, if they have been stored unlawfully; and
- the right to bring proceedings before the courts or competent authorities to correct or delete data or to obtain compensation.

Anyone exercising these rights can apply to the competent authorities in the Schengen State of his/her choice. This is possible because all copies of data in the national databases are identical to the central system database. Therefore, these rights can be exercised in any Schengen country, regardless of who issued the alert. When an individual exercises his/her

[205] COM(2016) 230 final.
[206] COM(2016) 731 final.
[207] Council Decision 2008/615/JHA of 23 June 2008 on the stepping up of cross-border cooperation, particularly in combating terrorism and cross-border crime (OJ L 210, 6.8.2008, p.1); and Council Decision 2008/616/JHA of 23 June 2008 on the implementation of Decision 2008/615/JHA on the stepping up of cross-border cooperation, particularly in combating terrorism and cross-border crime (OJ L 210, 6.8.2008, p. 12).

rights of access, correction of inaccurate data and deletion of unlawfully stored data, competent authorities must reply within a strict deadline. The individual must receive a reply as soon as possible and, in any event, not later than 60 days from the date on which he/she applies for access, or sooner if national law so provides. The individual must also be informed as soon as possible of action taken to correct or delete data as requested, and in any event not later than three months from the date on which he/she applies for correction or deletion, or sooner if national law so provides.

A specific evaluation is carried out of each Member State under the Schengen evaluation mechanism, exploring how each country protects personal data, including personal data stored and processed in SIS. Data protection was also a specific consideration in the Commission's overall evaluation of the system. The SIS legislative instruments give the European Data Protection Supervisor an explicit oversight role, ensuring that all personal data processing activities carried out by eu-LISA are in accordance with the law, and these must be audited regularly.

SIS also supports the rights of the child, helping to locate and protect missing children, including children who have been abducted or trafficked. Alerts for missing children can require law enforcement officials and border guards to take them into protective custody once found, in line with the best interests of the child, ensuring that they are safe and well. This protection is extended and improved in the December SIS proposals, which introduce further measures to protect children, including children at risk of parental abduction.

SIS only applies to those countries that participate in the Schengen acquis. As a result, it is not applicable externally and does not have specific external relations objectives. However, it does have an external dimension to the extent to which SIS provides support for effective border management by ensuring that border guards at the EU's external borders have access to up-to-date information on individuals who are of interest in criminal cases, including terrorism, and on those who should be refused entry or stay in EU territory. This aspect has been strengthened by the Commission's recent proposals (adopted in December 2016) with particular provisions to support EU return policy by increasing the visibility of return decisions through SIS, and clarifying procedures relating to refusal of entry or stay.

Law enforcement access to Visa Information System

1. Legal framework

Council Decision 2008/633/JHA of 23 June 2008 concerning access for consultation of the Visa Information System (VIS) by 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[208].

The Decision was adopted following the Council conclusions of March 2005, stating that ‘in order to achieve fully the aim of improving internal security and the fight against terrorism’, Member State authorities responsible for internal security should be guaranteed access to the VIS, ‘in the course of their duties in relation to the prevention, detection and investigation of criminal offences, including terrorist acts and threats’, ‘subject to strict compliance with the rules governing the protection of personal data’.

The legal base is a pre-Lisbon instrument. In case the VIS is subject to recast, a new legislation based on Article 87 TFEU should be adopted.

The Decision became applicable in September 2013.

2. Analysis

[208] OJ L 218, 13.8.2008, p. 129.

The objective of the Decision was to provide the legal basis under which Member State authorities responsible for internal security and the Europol may access and consult the VIS for the purposes of preventing, detecting and investigating terrorist offences and of other serious criminal offences.

The Decision also lays down the conditions and procedures under which they may do so.

The law enforcement access to VIS is a recently implemented instrument; VIS law enforcement access Decision became applicable only in September 2013. Given that the VIS contains a growing number of data of visa applicants, there is a growing interest for law enforcement to benefit from access to these data, in particular to the biometric data.

The Decision allowed the law enforcement to access an EU database. Without the Decision such access would not be possible.

The evaluation of VIS conducted in 2016 showed that while access to the VIS for law enforcement purposes currently remains quite fragmented and limited among Member States, the high level of satisfaction and real or expected benefits from VIS access indicate that the number of users and requests should only increase in the future.

The added value of the EU legislation in this field is only increasing. The recent calls by the Council of Ministers of the EU in the field of justice and home affairs to step up checks at external borders are a strong appeal to more systematic and wider use of the VIS and to making it more interoperable with existing and possibly new EU databases.

The Decision introduces an access to a large scale "administrative" database of data of unsuspected persons. Access to such database by law enforcement has an impact on the right to privacy and the right to data protection of the persons concerned.

The Decision provides for guarantees and safeguards regarding data protection, in particular regarding the access procedure[209] and rights of data subjects[210].

Law enforcement access to Eurodac

1. Legal framework

Regulation (EU) 603/2013 of 26 June 2013 on the establishment of Eurodac for the comparison of fingerprints for the effective application of Regulation (EU) No 604/2013 establishing the criteria and mechanisms for determining the Member State responsible for examining an application for international protection lodged in one of the Member States by a third-country national or a stateless person and on requests for the comparison with Eurodac data by Member States' law enforcement authorities and Europol for law enforcement purposes, and amending Regulation (EU) No 1077/2011 establishing a European Agency for the operational management of large-scale IT systems in the area of freedom, security and justice (recast)[211].

The Regulation was adopted following the Commission Communication to the Council and the European Parliament of 24 November 2005 on improved effectiveness, enhanced interoperability and synergies among European databases in the area of Justice and Home Affairs outlining that authorities responsible for internal security could have access to Eurodac in well-defined cases, when there is a substantiated suspicion that the perpetrator of a terrorist or other serious criminal offence has applied for international protection. In that Communication the Commission also found that the proportionality principle requires that Eurodac be queried for such purposes only if there is an overriding public security concern, that is, if the act committed by the criminal or terrorist to be identified is so reprehensible that

[209] Articles 4 to 7.
[210] Article 8.
[211] OJ L 180, 29.6.2013, p. 1.

it justifies querying a database that registers persons with a clean criminal record, and it concluded that the threshold for authorities responsible for internal security to query Eurodac must therefore always be significantly higher than the threshold for querying criminal databases.

Regarding the law enforcement access to Eurodac, the Regulation has become applicable in July 2015.

The Regulation is currently subject to recast. The Commission proposal of 4 May 2016 did not cover the law enforcement access to the database[212]. However, the partial general approach adopted by the Council in December 2016 provides for substantive amendments to the conditions and procedures for law enforcement access[213] and the subsequent discussions in the Council focus on further simplification of the law enforcement access regime[214].

2. Analysis

The objective of the Regulation was to provide the legal basis under which Member State law enforcement authorities and the Europol may compare the fingerprints with the fingerprints registered in Eurodac for the purposes of preventing, detecting and investigating terrorist offences and of other serious criminal offences.

The Regulation also lays down the conditions and procedures under which they may do so.

The law enforcement access to Eurodac is a recently implemented instrument; Eurodac Regulation became applicable only in July 2015. There is a growing awareness of the law enforcement authorities about the potential of the law enforcement access to Eurodac, but for the time being the access to the database is very limited.

The Eurodac Regulation allowed the law enforcement to access an EU database. Without the Regulation such access would not be possible.

Currently, Eurodac contains very limited alphanumeric data. The added value for the law enforcement is therefore limited to the comparison of the fingerprints.

The added value of the EU legislation in this field is only increasing. The access to Eurodac allows the Member States authorities to identify persons which may not be identifiable via other existing databases.

The Regulation introduces an access to a large scale "administrative" database of data of unsuspected persons. Access to such database by law enforcement has an impact on the right to privacy and the right to data protection of the persons concerned.

The Regulation provides for comprehensive guaranties and safeguards regarding data protection, in particular regarding the access procedure[215] and rights of data subjects[216].

Regarding the necessity and proportionality of the measure, it should be noted that Eurodac Regulation provides for much stricter access conditions and procedures then the Council Decision 2008/633/JHA concerning law enforcement access to the Visa Information System (VIS) 217.

The current Regulation provides for rather high level of protection of fundamental rights, even in light of the recent case law of the Court[218]

---

[212] COM(2016) 272 final.
[213] Council document 15119/16.
[214] Council document 8502/17.
[215] Articles 19 to 21.
[216] Articles 30 and 31.
[217] OJ L 218, 13.8.2008, p. 129 .
[218] *Digital Rights Ireland and Others* (C-293/12 and C-594/12), *Schrems* (C-362/14), *Tele2 Sverige and Others* (C‑203/15 and C‑698/15).

Directive 2016/681 of 27 April 2016 on the use of passenger name record (PNR) data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime

1. Legal framework

Article 82(1) and point (a) of Article 87(2) TFEU.

An EU policy on PNR was considered to be necessary to ensure common standards across the Member States. The proposal for a PNR Directive aimed at harmonising the transmission of data by carriers to PIU, as well as the technical requirements for the transfer of PNR data by air carriers. The proposal for a PNR Directive also aimed to ensure that all Member States collect and use PNR data in order to be able identify previously unknown persons of interest and effectively exchange the results of PNR processing at EU level. It contains data protection safeguards, in particular relating to access to data by law enforcement.

2. Analysis

Directive 2016/681 (the PNR Directive) provides for the transfer by air carriers of passenger data to the Member States, in view of their processing for the fight against terrorism and serious crime.

The processing of passenger data against law enforcement databases and risk-based predetermined criteria can provide valuable information on persons that might be involved in criminal activities, notably by allowing to identify persons of interest that were previously not known to law enforcement authorities.

The PNR Directive was adopted on 27 April 2016 and has to be transposed by Member States until 25 May 2018. The Directive has not yet started to deploy its effects. Its objectives appear to be still adapted to the need to fight in a more efficient way terrorism serious crime.

The PNR Directive provides for a review of all its elements, to be conducted by 25 May 2020.

After its transposition by Member States, the PNR Directive will ensure that the collection and processing of PNR data are conducted in a harmonised way at EU level and that the relevant results of this processing are exchanged between the Member States.

The EU has been providing financial support to Member States to assist them in the process of implementing the PNR Directive. The Commission presented in November 2016 an Implementation Plan for the PNR Directive outlining the main steps in the implementation process and the support measures provided by the Commission to ensure the timely transposition of the Directive.

The collection and processing of PNR data for law enforcement purposes entail an interference with the fundamental rights to the protection of private life and to the protection of personal data, as enshrined in Articles 7 and 8 of the Charter on Fundamental Rights of the European Union. Consequently, the PNR Directive embeds strong safeguards aimed at ensuring that the interference is compliant with the requirements set forth in Article 52 of the Charter. Notably, the PNR Directive defines purpose for processing the data, clearly defines the types of processing of PNR data and the categories of persons that have access to the data, provides for a maximum period of retention of five years and for the masking out of the data after six months and prohibits the processing of sensitive data. The PNR Directive also provides for the rights of individuals to information, access, rectification, erasure and blocking and requires that the processing of any personal data is appropriately secured. Equally, the supervision of the application of these rules by the data protection officers and by the independent data protection supervisory authorities in Member States is an essential component of the protection of individuals with regard to the processing of personal data.

The PNR Directive provides for the collection and processing by Member State of PNR data for flights to and from the EU, as well as of intra-EU flights. As such it allows to identify

persons of interest that might be involved in terrorism and serious crime and that are flying to or from the EU.

The PNR Directive provides for the possibility to exchange PNR data or the result of processing PNR data with third countries, thus reinforcing the external dimension of internal security.

The operation of the PNR Directive will also trigger an increase in the number of requests for PNR data from third countries. A comprehensive approach needs therefore to be adopted between the internal and the external policy concerning the collection and processing of PNR data.

Agreement between the European Community and the Government of Canada on the processing of Advance Passenger Information and Passenger Name Record data

1. Legal framework

Article 95 EC Treaty (old). It aims to ensure respect for fundamental rights and freedoms, notably the right to privacy, while supporting the fight against terrorism and serious transnational crime.

To be noted that the envisaged new (2015) EU-Canada PNR Agreement, negotiated following the entry into force of the Lisbon Treaty, is based on Article 82(1)(d) TFEU on judicial cooperation in criminal matters, Article 87(2(a) TFEU on police cooperation in criminal matters in conjunction with Article 218(6)(a) TFEU – procedure to negotiate international agreements. Such police and judicial cooperation brings major security gains, to counter phenomena like foreign terrorist fighters travelling to conflict zones for terrorist training, drugs trafficking or travelling sex offenders.

This new Agreement has not yet entered into force, as it was sent to the European Court of Justice by the European Parliament, asking, inter alia, whether the Agreement should also be based on Article 16 TFEU (data protection).

2. Analysis

The objective of the 2006 PNR Canada Agreement is to ensure that API/PNR data of passengers is provided to Canada in full respect of fundamental rights and freedoms, in particular the right to privacy.

This international Agreement was linked to:

(i) commitments by the Canada Border Service Agency to the EU on the handling of API/PNR data– which provide for detailed data protection safeguards which the Canadian authorities undertook to apply when processing PNR data obtained from flights arriving from Europe and,

(ii) an Adequacy Decision of the Commission (Decision 2006/253/EC), based on Article 25(2) of Directive 95/46/EC which acknowledges that the processing of PNR data by the competent Canadian authority in accordance with the aforementioned Commitments respects EU law (OJ L 91, 29.3.2006, p. 49).

According to Article 5(2) of the 2006 EU-Canada PNR Agreement, the obligation of air carriers to process PNR data "*shall only apply for as long as the [Adequacy] Decision is applicable, ceasing to have effect on the date that the Decision is repealed, suspended or expires without being renewed*".

The Commitments and the Adequacy Decision expired on 22 September 2009. Therefore, in spite of the fact that the Agreement itself does not have an expiry date and has never been terminated by any of the Parties, it can no longer produce its legal effectas regards the obligation for air carriers to transfer PNR data to the Canadian authorities, pursuant to Article 5 of the Agreement.

However, it should be noted that during the interim period between the 2006 arrangements and the conclusion of a new Agreement, the data protection guarantees embedded in the commitments continue to be acknowledged by Canada, which undertook to confirm to EU Institutions and Member States that the original Commitments are still in full force and effect. In addition, some of the data protection guarantees contained in the Commitments are in any event recognised by the general provisions of national Canadian legislation.

This situation was meant to be temporary, pending the adoption of a new Agreement, negotiated following the entry into force of the Treaty of Lisbon.

A new EU–Canada PNR Agreement was signed on the 25 June 2014 in Brussels and sent to the European Parliament, which however voted to seek an opinion from the European Court of Justice on its compatibility with the Treaties and the Charter of Fundamental Rights and the adequacy of the legal basis used. This envisaged new Agreement is therefore currently *sub judice* and the Court's opinion is scheduled to be released on 26 July 2017.

In terms of **supporting European cooperation**, the old (2006) Canada PNR Agreement in principle only provided for the collection and processing by Canada of PNR data for flights to and from the EU. However, it did also contain a commitment from Canada to provide information to foreign States concerning persons on board to such flights where the laws of that State so required. It also committed to provide European authorities with access to API and PNR for persons whose itinerary includes a flight to the EU in case the EU would decide to pass legislation and to adopt an airline identification system.

The envisaged new Canada PNR Agreement (based on the current Treaty regime), in order to foster international police and judicial cooperation, does provide for the sharing by the Canadian authorities of information containing PNR data obtained under the Agreement with Europol, Eurojust or the police and judicial authorities of the Member States. The envisaged agreement establishes the transfer of PNR data and analytical information by Canada at its own initiative and lays down an obligation for Canada to transfer data or information at the request of police authorities in Member States or of Europol, or of judicial authorities in Member States or Eurojust. A reciprocity clause was also included in the new Agreement with a view to the (at that time) forthcoming EU PNR regime. This clause would allow for future amendments potentially entailing obligations to provide Member States authorities with access to PNR data of flights from Canada to the European Union after the establishment of an EU PNR regime, thereby further improving police and judicial cooperation between Member States.

The external dimension of the internal security is reinforced by allowing Canada to identify persons of interest that might be involved in terrorism and serious crime and that are flying to or from the EU. With the adoption of the EU PNR Directive, passenger data will now also be transferred from third countries (including Canada) to the EU. There is therefore a need to ensure that the EU future external PNR policy reflects appropriately its internal PNR policy in future agreements, in line with the requirements potentially defined by the European Court of Justice in its opinion.

Agreement on the processing and transfer of Passenger Name Record (PNR) data by air carriers to the Australian Customs and Border Protection Service (entry into force 1.6.2012)

1. Legal framework

Article 82(1)(d) TFEU on judicial cooperation in criminal matters, Article 87(2(a) TFEU on police cooperation in criminal matters in conjunction with Article 218(6)(a) TFEU – procedure to negotiate international agreements. Such police and judicial cooperation is believed to bring major security gains, in areas like foreign terrorist fighters travelling to conflict zones for terrorist training, drugs trafficking or travelling sex offenders (see main objectives below under point 2).

2. Analysis

The main purpose of the Agreement is to ensure the transfer of Passenger Name Record (PNR) data to the Australian Customs and Border Protection Service (ACBPS) pursuant to which this service assesses the risk a passenger may pose to Australian security with the aim of preventing, detecting, investigating and prosecuting terrorist offences or serious transnational crime. The Agreement also fosters international police and judicial cooperation through the transfer of PNR data or relevant and appropriate analytical information obtained from PNR data from Australia to the competent Member States authorities as well as Europol and Eurojust within their respective competences.

The first (2013) joint review of this Agreement has shown, on the basis of a preliminary assessment of the question of whether PNR serves the purpose of supporting the fight against terrorism and other serious crimes that are transnational in nature, that the processing of PNR data provided ACBPS with the possibility of carrying out effective pre-departure risk assessments of all passengers up to 72 hours before departure. The early identification of passengers who may pose a high risk enables ACBPS to prepare the necessary responses upon arrival and better target their interventions, while facilitating the travel of legitimate travellers due to minimal interventions.

The upcoming joint evaluation of the EU-Australia PNR Agreement scheduled for the second half of 2017 will explore the wider functioning, operational value and necessity of the Agreement.

In terms of supporting European cooperation, this international Agreement provides in principle only for the collection and processing by Australia of PNR data for flights to and from the EU (i.e. not to or between Member States).

However, in order to foster international police and judicial cooperation, the envisaged Agreement provides for the sharing by the Australian authorities of information containing PNR data obtained under the Agreement with Europol, Eurojust or the police and judicial authorities of the Member States. The agreement establishes the transfer of PNR data and analytical information by Australia at its own initiative and lays down an obligation for Australia to transfer data or information at the request of police authorities in Member States or of Europol, or of judicial authorities in Member States or Eurojust.

A reciprocity clause was also included in the Agreement with a view to the (at that time) forthcoming EU PNR regime. This clause allows for future amendments potentially entailing obligations to provide Member States authorities with access to PNR data of flights from Australia to the European Union after the establishment of an EU PNR regime, thereby further improving police and judicial cooperation between Member States.

In terms of safeguarding fundamental rights, the EU-Australia PNR Agreement embeds safeguards concerning the protection of fundamental rights, and especially the right to private life and to the protection of personal data as guaranteed by Articles 8 and 7 of the Charter of Fundamental rights.

The compliance of the draft EU-Canada PNR Agreement (and the data protection safeguards contained therein) with the Charter of Fundamental rights is subject of the forthcoming Court's opinion. It may also be relevant for other PNR Agreements, including the one with Australia. This will also need to be taken on board in the joint review and evaluation of the EU-Australia PNR Agreement scheduled for the second half of 2017.

The EU-Australia Agreement reinforces the external dimension of internal security by allowing Australia to identify persons of interest that might be involved in terrorism and serious crime and that are flying to or from the EU. The Agreement also provides for the possibility to exchange PNR data or the result of processing PNR data with Member States, Europol and Eurojust, thus reinforcing the external dimension of internal security.

With the adoption of the EU PNR Directive, there is a need to ensure that the EU future external PNR policy reflects appropriately its internal PNR policy. This might require possible adjustments also to the EU-Australia PNR Agreement, as already foreseen in Article 24 paragraph 6 thereof. This will also be taken on board in the upcoming joint review and evaluation.

EU-US agreement on the use and transfer of PNR to the US Department of Homeland Security (entry into force on 1.7.2012)

1. Legal framework

The EU-US agreement on the use and transfer of PNR to the US Department of Homeland Security is based on Article 82(1)(d) TFEU on judicial cooperation in criminal matters, Article 87(2(a) TFEU on police cooperation in criminal matters in conjunction with Article 218(6)(a) TFEU – procedure to negotiate international agreements. Such police and judicial cooperation is believed to bring major security gains, in areas like foreign terrorist fighters travelling to conflict zones for terrorist training, drugs trafficking or travelling sex offenders (see main objectives below under point 2).

2. Analysis

The main purpose of the Agreement is to ensure the transfer of Passenger Name Record (PNR) data with the US Department of Homeland Security (DHS) pursuant to which this service assesses the risk a passenger may pose to security with the aim of preventing, detecting, investigating and prosecuting terrorist offences or serious crime. The Agreement also fosters international police and judicial cooperation through the transfer of PNR data or relevant and appropriate analytical information obtained from PNR data from the U.S. to the competent Member States authorities as well as Europol and Eurojust within their respective competences.

The (2013) review of this Agreement has shown, on the basis of a preliminary assessment of the question whether PNR serves the purpose of supporting the fight against terrorism and other crimes that are transnational in nature, that PNR provides DHS with the possibility of carrying out pre-departure assessments of all passengers up to 96 hours which gives DHS sufficient time to carry out all the background checks before the arrival of a passenger and prepare its response. It also provides DHS with the opportunity to perform risk assessments on the basis of scenario-based targeting rules in order to identify the 'unknown' potential high-risk individuals. PNR further provides the possibility to make associations between passengers and identify criminals who belong to the same organised crime group. According to DHS PNR is also successfully used for identifying trends of how criminals tend to behave when they travel, for example by understanding which routes they use.

In terms of supporting European cooperation this international Agreement in principle only provides for the collection and processing by the US of PNR data for flights to and from the EU *(i.e. not to or between Member States).*

However, in order to foster international police and judicial cooperation, the envisaged Agreement provides for the sharing by the US authorities of information containing PNR data obtained under the Agreement with Europol, Eurojust or the police and judicial authorities of the Member States. The agreement establishes the transfer of PNR data and analytical information by the US at its own initiative and lays down an obligation for the US to transfer data or information at the request of police authorities in Member States or of Europol, or of judicial authorities in Member States or Eurojust.

A reciprocity clause was also included in the Agreement with a view to the (at that time) forthcoming EU PNR regime. This clause allows for future amendments potentially entailing obligations to provide Member States authorities with access to PNR data of flights from the

US to the European Union after the establishment of an EU PNR regime, thereby further improving police and judicial cooperation between Member States.

In terms of safeguarding fundamental rights, the EU-US PNR Agreement embeds safeguards concerning the protection of fundamental rights, and especially the right to private life and to the protection of personal data.

The compliance of the draft EU-Canada PNR Agreement (and the data protection safeguards contained therein) with the Charter of Fundamental rights, which is the subject of a forthcoming European Court of Justice opinion, may also be relevant for other PNR Agreements, including the one with the US.

The EU-US Agreement reinforces the external dimension of internal security, by allowing the US to identify persons of interest that might be involved in terrorism and serious crime and that are flying to or from the EU. The Agreement also provides for the possibility to exchange PNR data or the result of processing PNR data with Member States, Europol and Eurojust, thus reinforcing the external dimension of internal security.

With the adoption of the EU PNR Directive, passenger data will now also be transferred from third countries (including the US) to the EU. There is therefore a need to ensure that the EU future external PNR policy reflects appropriately its internal PNR policy. This might require possible future adjustments also to the EU-US PNR Agreement, as already foreseen in Article 20 paragraph 2 thereof.

Council Framework Decision 2009/315/JHA on the organisation and content of the exchange of information extracted from the criminal records between Member States

Council Decision 2009/316/JHA on the establishment of the European Criminal Records Information System (ECRIS) in application of Article 11 of Framework Decision 2009/315/JHA

1. Legal framework

The ECRIS framework was adopted in 2009 on the legal basis of Article 31 and 34(2)(b) and (c) of the Treaty on European Union. The revision of ECRIS, as proposed with the Commission proposal for an amending Directive as regards the exchange of information on third country nationals, would be based on Article 82(1) TFEU, the Chapter on judicial cooperation in criminal matters.

The need to improve the exchange of information on convictions was prioritised in the European Council Declaration on Combating Terrorism of 25 and 26 March 2004 and was subsequently reiterated in the Hague Programme of 4-5 November 2004 and in the Action Plan of 2- 3 June 2005 on its implementation. Furthermore, the computerised interconnection of criminal records at European Union level was recognised as a political priority by the European Council in its Conclusions of 21 and 22 June 2007.

ECRIS forms a key part of the Commission's priority of a common area of justice and fundamental rights, as well as the European Agenda on Security, which calls explicitly for the inclusion of non-EU nationals within ECRIS to improve the fight against cross-border crime and terrorism. Also the Joint Declaration on the EU's legislative priorities for 2017 mentions especially inclusion of third country nationals in ECRIS.

2. Analysis

The main objective is to improve the exchange of information on convictions between the EU Member States. The Framework Decision 2009/315 establishes the principles of information exchange and lays down the framework for a computerised conviction-information exchange system that would allow information to be exchanged in a uniform, electronic and easily machine-translatable way, based on the use of a “standardised European format”. This system, called European Criminal Records Information System (ECRIS), was established by

the Council Decision 2009/316. By improving information exchange in criminal matters, the instruments are to contribute to reducing crime and fostering crime prevention and thus to improve the functioning of a common area of security and justice.

The main policy objective is to develop a cost-efficient EU-wide solution to improve cross border exchange of information on persons convicted in the EU in full respect of fundamental rights in the context of cooperation between Member States in criminal matters. The general objectives are to improve the functioning of a common area of security and justice by improving information exchange in criminal matters; and to reduce crime and foster crime prevention (also with regard to terrorism).

The ECRIS system allows for an efficient, electronic, decentralised information exchange between Member States regarding criminal convictions of European citizens in the EU.

However, the current ECRIS was not designed for **third country nationals (TCN)** as it does not contain a mechanism to identify Member State(s) holding criminal record information on TCN. Member States wishing to receive such information have to send 'blanket' requests to all Member States, including (the majority of) the Member States not holding the requested information. The administrative burden caused by having to respond to 'blanket' requests has been identified as the most costly element (estimated at up to € 78 million) of the ECRIS workflow, if Member States were to systematically send such requests. As ECRIS is inefficient with regard to TCN, in practice, Member States do not use the full potential of ECRIS with regard to TCN. Thus, complete information on the criminal history of convicted TCN is not always available to courts, law enforcement authorities, and other administrative authorities according to national law. Other equally or more efficient information exchange channels do not exist.

For this reasons, in January 2016, the Commission presented a legislative proposal for a Directive amending the Framework Decision 2009/315 as regards the exchange of information on third country nationals, and replacing the Decision 2009/316. This proposal was complemented by a second one on 29 June 2017.

As far as the exchange of information for **other purposes than criminal proceedings** is concerned, the ECRIS system seems to be significantly underused, with only 21% of requests for these purposes. It might be caused by the fact that Framework Decision 2009/315 gives a lot of discretion to the Member States in respect to replies to requests for information for other purposes, to the extent that, in accordance with national law, the information might even not be transmitted at all. The Member States should consider revising their national law as such as allowing an effective exchange of information for other purposes, e.g. employment, naturalisation, authorisation to carry weapons, etc. Alternatively, the revision of the relevant Framework Decision provisions could be considered.

Since 1 January 2017 all 28 Member States exchange information using the ECRIS system. The yearly volume of exchange is nearly 2 million messages (including notifications, request and responses to requests). The average of request is over 30.000 per month, with over 30% of requests leading to a 'positive hit' (response containing one or more convictions).

The Commission offered to the Member States the Reference Implementation software enabling connection of the national criminal records databases to the common communication infrastructure, which is being used by 24 Member States. It also supported the Member States financially in the process of preparation of their national criminal records systems by numerous grants, specifically between 2009 and 2012. With the help of this funding, some Member States managed to modify their national systems significantly in order to meet the requirements of the European legislation.

The Report on the implementation of the Framework Decision 2009/315 of 2016 notes that significant progress has been made in the exchange of criminal records information between the EU Member States. It is worth mentioning that the most vital provisions have been

implemented satisfactorily by all 22 Member States who notified their national measures, while some other provisions are unevenly transposed.

Framework Decision 2009/315 contains several provisions designed to ensure a high and satisfactory level of **protection for personal data** transmitted by the convicting Member State to the Member State of the person's nationality. It limits the use the requesting Member State can make of information asked for (Article 9). It also lays down specific rules applying where the Member State of the person's nationality forwards information transmitted to it by the convicting Member State, making a distinction between requests involving criminal proceedings and other requests (Article 7). If the request is not related to criminal proceedings, only the convicting Member State will be able to assess, on the basis of the purpose of the request, whether or not full information on convictions should be transmitted. The Member State of the person's nationality should therefore check with the convicting Member State to what extent it may transmit such information to the requesting Member State. The same applies for requests from third countries, with a view to ensuring that the Member State of the person's nationality does not give them more information than to a Member State.

The instruments comply with the **proportionality principle** as the rules they lay down governing the organisation and content of information exchanges are confined to what is necessary in order to achieve the above objectives. For example, the Framework Decision requires Member States to store information transmitted to it, but leaves it to each Member State to decide how and where such information is stored. It also does not interfere in the internal use of this information, but concentrates on the storage for the purpose of retransmission.

As described above, the ECRIS system allows, in its current form, for exchanges of information on **convictions of third country nationals**, but it does not work efficiently in this respect. The aim of the Commission proposal of 29 June 2017 is to fill-in this gap.

As far as the **exchange of information with third countries on convicted EU-nationals** is concerned, it can take place on the basis of existing bilateral agreement between that country and a certain Member State. The Framework Decision 2009/315 contains a few provisions which ensure that in cases where criminal records information is provided to third States, this is done in accordance in respect of the limits set by the convicting Member State (Article 7(3)) and in accordance with the purpose limitation (Article 9(4)).

Council Common Position 2005/69/JHA of 24 January 2005 on exchanging certain data with INTERPOL

1. Legal framework

The European Council of 25 March 2004, in its Declaration on combating terrorism, instructed the Council to take forward work on the creation by end 2005 of an integrated system for the exchange of information on stolen and lost passports having recourse to the Schengen Information System (SIS) and the Interpol database. The Council Common Position 2005/69/JHA of 24 January 2005 aimed to be a first response to that request that should be followed-up by the setting up of the technical functionality in the SIS to achieve that aim.

2. Analysis

The Council Common Position 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 the SIS, as regards the Member States participating in it.

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* […]".

Article 4 "Monitoring and evaluation" of the Common Position provides that "*On the basis of information provided by the Member States, the Commission shall, by December 2005, submit a report to the Council on the operation of this Common Position. The Council shall assess the extent to which Member States comply with this Common Position and take the appropriate action*".

The European Council of 25 March 2004, in its Declaration on combating terrorism, instructed the Council to take forward work on the creation by end 2005 of an integrated system for the exchange of information on stolen and lost passports having recourse to the Schengen Information System (SIS) and the Interpol database. This Common Position was a first response to that request that should be followed-up by the setting up of the technical functionality in the SIS to achieve that aim.

As required by Article 4, 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.

In March 2014, at the occasion of the Malaysia Airlines flight 370 incident the then-Secretary General of Interpol noted that very few countries systematically query the SLTD database for the purposes of verifying whether a travel document has been reported as lost or stolen.

This issue was discussed at a JHA Senior Officials EU - Interpol meeting in June 2014, where the Commission reported on a number of practical problems raised by certain EU Member States, leading them to conduct only a limited number of searches on Interpol's SLTD.

The JHA Council recalled in its October 2014 conclusions the obligations made to EU Member States in its Common Position (2005/69/JHA), and called on them, the Commission and Interpol to take a number of actions as regards Interpol's SLTD database.[219]

The overall objective of having more Member States input data and check more systematically the SLTD database of Interpol is still relevant. Furthermore, the requirement for Member States to systematically check (and input data into) the SLTD database is also still relevant, considering that this is the only database that collects data on stolen and lost travel documents in countries outside the EU. Finally, the requirement that EU Member States should enter their data on stolen and lost travel documents in the SLTD database of Interpol, even though they also enter the same data in SIS, also remains relevant in terms of allowing third countries to check that EU citizens crossing their borders do not travel with stolen or lost travel documents.

[219] 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.

With the entry into force of the revised Schengen Border Code in April 2017, the objective of the Common Position as regards the consultation of Interpol's SLTD database is met by the revised Schengen Border Code (SBC), which is a legally binding instrument which can be acted upon in case of non-compliance by EU Member States.

Inside the EU, the Commission has long been a supporter of the full use of Interpol's SLTD by EU Member States. For instance, at political level, the Commission's European Agenda on Security of 2015 calls for fuller use of the Schengen Information System together with Interpol's Stolen and Lost Travel Documents (SLTD) database in order to further strengthen security at our external borders.

Furthermore, in terms of support, the Commission has also expressed to EU Member States in many fora that it remains committed, including financially, to help them use automated border controls with checks of the Schengen Information System and SLTD databases.

The Commission also conducted in 2015 a survey with Member States on how they use the SLTD database and the problems they face when using it. A number of practical implementation problems were identified in this assessment, which was presented to Member States and communicated to Interpol.

Finally, the Commission is in early stages of discussions with Interpol to help the least performing EU Member States in terms of deployment and use of SLTD.

As to fundamental rights, preamble 9 states that *"This Common Position respects the fundamental rights and observes the principles recognised in particular by Article 6 of the Treaty on European Union and reflected in the Charter of Fundamental Rights of the European Union".*

Limitations and safeguards are provided by Article 3 paragraph 5 which stipulates that "*The exchange of personal data in compliance with the obligation laid down in this Common Position shall take place for the purpose set out in Article 1, ensuring an adequate level of protection of personal data in the relevant Interpol Member Country and the respect for fundamental rights and liberties regarding the automatic processing of personal data. To that end, Member States shall ensure that the exchange and sharing of data takes place on the appropriate conditions and subject to the above requirements*".

The external dimension of internal security is incorporated in the Common Position, since it recognises implicitly that the SLTD database of Interpol is the only database that stores stolen and lost travel documents of countries outside the EU, and that it should therefore be used by Member States in the course of their tasks falling within the scope of the Common Position.

2. Law enforcement: the role of the EU agencies (Europol, the EU Policy cycle, CEPOL)

Europol

1. Legal framework

Regulation 2016/794 of the European Parliament and of the Council on the European Union Agency for Law Enforcement Cooperation, replacing and repealing Council Decision 2009/371/JHA establishing the European Police Office (Europol) and Council Decisions 2009/934/JHA, 2009/935/JHA, 2009/936/JHA 935,936/968[1] is based on Article 88 TFEU. It replaces the Europol Council Decision since 1 May 2017. The regulation needed to be adopted following the entry into force of the Treaty of Lisbon that required to have a regulation as a legal basis for Europol and to introduce parliamentary scrutiny over the Europol activities.

2. Analysis

The Europol regulation provides a legal basis for the EU agency supporting cooperation among law enforcement authorities in the Union.

Europol supports and strengthen action by the law enforcement authorities of the Member States and their mutual cooperation in preventing and combating serious crime affecting to or more Member States, terrorism and forms of crime which affect a common interest covered by a Union policy.

The Europol regulation is considered relevant to the current needs. It recently entered into application (1st May 2017). The Europol regulation has yet to unravel its full potential, and it is therefore too early to assess its added-value.

However, the Regulation lays the foundations for Europol to become the EU information hub for law enforcement agencies across Europe. Such an objective could not have been achieved at the national level or via bilateral cooperation between Member States. It allows for pooling together information on serious cross-border crime and terrorism, providing analytical and operational support for Member States investigations and operations.

At the same time, while allowing Europol to be flexible and more efficient, the Regulation introduces mechanisms for the scrutiny of Europol's activities by the European Parliament together with national parliaments and strengthens the protection of personal data. It allows also streamlining processing of data by Europol by providing for a flexible data management architecture where information could be more easily cross-matched and criminal analyses be made in a more effective way. Finally, it changes the rules on cooperation between Europol and external partners by simplifying strategic and technical cooperation with third countries as well as making the Commission responsible for negotiating operational agreements on the cooperation with third countries (instead of Europol).

The Europol Regulation respects the fundamental rights and observes the principles recognised in particular by the Charter of Fundamental Rights of the European Union, in particular the right to the protection of personal data and the right to privacy as protected by Articles 8 and 7 of the Charter, as well as by Article 16 TFEU,

The issue of fundamental rights features prominently in the chapter on transfer of personal data (Chapter V). Whenever such transfers are to be undertaken by Europol (notwithstanding which instrument is used for that), the existence of data protection safeguards and respect for fundamental rights need to be taken into consideration.

The Europol regulation provides Europol with even more robust data protection regime. Its standards are aligned with the standards of the new Data Protection package. It also replaces the current external data protection supervisor (the Joint Supervisory Body) by the European Data Protection Supervisor that enjoys full independence and effective powers, as required by the ECJ jurisprudence.

The Europol regulation changes profoundly the external relations between Europol and third countries and organisations. In line with the Treaty of Lisbon, Europol will lose its treaty making power. It will be the Commission that will provide for a legal framework for the operational cooperation between Europol and third countries: it will either be based on a COM decision finding that the third country offers adequate data protection standards ('adequacy decisions') or an international agreement concluded on the basis of Art.218 of the Treaty. The Commission services have recently proposed priorities for the negotiations of such agreements. With regard to the strategic cooperation with third countries, not requiring exchange of personal data, Europol could engage without any formalities as long as it is necessary for its objectives.

Some third countries are already very important contributors to Europol databases and important cooperation partners. It is assessed that the Europol regulation will enhance even further this cooperation which would be mutually beneficial for the third countries and the EU as a whole.

The European Counter Terrorism Centre (ECTC) at Europol

1. Legal framework

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).[220]

2. Analysis

The ECTC, launched in January 2016 under the previous Europol Regulation, aims at optimising the use of counter-terrorism capabilities previously scattered through better pooling and streamlining of relevant tools (CT databases, financial intelligence, firearms, etc.). It was set up specifically in order to:

- Step up operational support to Member States' counterterrorism investigations
- Facilitate information sharing among Member States and with third countries (information hub)
- Maximise the use of existing structures, services and instruments at Europol (including specialised Focal Point, financial intelligence instruments, capabilities on firearms, CBRN and explosives)

On 7-8 February 2017, European Police Chiefs and heads of counter-terrorism units gathered in Berlin and stressed the importance of close cooperation and coordination among all European security authorities. The role of the ECTC as a "keystone" for a European security network was recognised.[221]

The ECTC will be further equipped to provide support to Member States with new instruments such as access to PNR data, improved access to the Schengen Information System, the future (if adopted) Entry Exit System and ETIAS, and through the embedment of the FIU.net network of financial intelligence units.

While cooperation among Member States' security services takes place outside the EU framework (Counter Terrorism Group), there is consensus on the need to ensure better coordination between intelligence and law enforcement communities. While this coordination takes first and foremost place at national level, Member States were invited to explore practical solutions for closer cooperation between the ECTC and CTG[222], including through secure anonymised hit/no hit search solutions, which preserve the necessary separation between law enforcement and intelligence work and the required principles of information ownership, third party rule and source protection.

The ECTC provides analytical support to the European Parliament, the Council and the Commission through strategic analysis report on the evolution of the terrorist threat (e.g. the annual TE-SAT report) to inform EU decision-making and effective response. It cooperates with the EU INTCEN to provide the most comprehensive threat picture.

One year after its official launch, the ECTC has successfully contributed to a significant increase in information sharing at EU level, as reported by Europol: +75% SIENA cases on terrorism in 2016 compared to 2015, +48% in operations supported by the focal points in the ECTC.[223]

The ECTC has developed a 24/7 capacity to support Member States investigators, notably in case of crisis: Europol activated its Emergency Response Team (EMRT) and deployed analysts in the aftermath of the Paris and Brussels attacks in 2015 and 2016.

---

[220] http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016R0794.
[221] https://www.europol.europa.eu/newsroom/news/fighting-terrorism-in-europe.
[222] http://www.europarl.europa.eu/RegData/etudes/STUD/2017/583124/IPOL_STU(2017)583124_EN.pdf.
[223] https://www.europol.europa.eu/newsroom/news/information-sharing-counter-terrorism-in-eu-has-reached-all-time-high.

This progress is also due to the adaptation of SIENA (Secure Information Exchange Network Application) to the specific needs of the counter-terrorism community with an upgrade to EU CONFIDENTIAL and peer-to-peer communication.

The EU Internet Referral Unit (IRU) has developed close cooperation with social media and online service providers, reaching a 91.4% success rate in removing illegal content. In addition, the IRU provides operational support to investigations across the EU and focused efforts in the immediate aftermath of high-profile events.[224]

The function of "information hub" with third countries provides access to valuable information (e.g. on foreign terrorist suspects) to Member States that do nott have the capacity to maintain cooperation channels with those countries.

To account for respect of fundamental rights, the ECTC operates within the legal framework of Europol, as strengthened by the new legal framework in place: legal provisions on fundamental rights and in particular the protection of personal data (chapter VI of the new Europol regulation) apply accordingly.

In respect of the external dimension, the ECTC benefits from the network of partners developed by Europol. The ECTC has already developed close cooperation with some partners (e.g. United States, Norway, Switzerland and Interpol).

The ECTC participates in the counter-terrorism/security dialogues with partner countries (Western Balkans, Turkey, MENA countries) and contributes to the implementation of agreed action plans.

In September 2016, the Commission tabled new proposals to maximise the benefits of international cooperation, making full use of the opportunities provided by the entry into application of its new Regulation on 1 May 2017. The Commission, the EEAS and Europol are exploring ways to optimise the cooperation with the CT/Security experts deployed in EU Delegations and explore avenues for increasing the sharing of information, including through Interpol.

CEPOL

1. Legal framework

Regulation (EU) 2015/2219 of the European Parliament and of the Council of 25 November 2015 on the European Union Agency for Law Enforcement Training (CEPOL) and replacing and repealing Council Decision 2005/681/JHA.

It was adopted in response to the call from the European Council in the Stockholm Programme to step up training on Union- related issues and to make such training systematically accessible to law enforcement officials of all ranks, and to the request from the European Parliament for a stronger Union framework for judicial and police training.

The ‘Stockholm Programme — An open and secure Europe serving and protecting citizens’ aimed at creating a genuine European law enforcement culture by setting up European training schemes and exchange programmes for all relevant law enforcement professionals at national and Union level.

2. Analysis

The CEPOL regulation sets a legal framework for the EU agency that supports, develops, implements and coordinates training for officers carrying out law enforcement tasks.

The objectives of CEPOL regulation are structured in line with the following set of general principles:

[224] https://www.europol.europa.eu/newsroom/news/europol-internet-referral-unit-one-year.

1) supports Member States in providing training in order to improve basic knowledge of the Union dimension of law enforcement;
2) supports Member States, upon their request, in the development of bilateral and regional cooperation through law enforcement training;
3) develops, implements and coordinates training in specific criminal or policing thematic areas;
4) develops, implements and coordinates training in relation to Union missions and law enforcement capacity-building activities in third countries.

That set of general principles should represent the European Law Enforcement Training Scheme (LETS), which aims to ensure that Union level training for law enforcement officials is of a high quality, coherent and consistent. Those general principles reflect the four strands identified by the Commission on the basis of the mapping of training needs and delivery conducted by CEPOL in cooperation with Member States.

The CEPOL regulation applies only as from 1 July 2016. It is very recent and well adapted to the needs of the law enforcement community. Contrary to the former instrument on CEPOL it allows CEPOL to support more targeted and relevant training with the EU dimension in line with the principles of LETS, widens up its target audience, engages CEPOL further in relations to the external relations cooperation, capacity building in third countries and preparations for Union missions.

In order to ensure that CEPOL training activities are fully embedded in security policy and are aligned with the EU priorities, the Regulation envisages that CEPOL will develop multi-annual strategic training needs assessments. A methodology to carry out this exercise is currently being developed.

As the CEPOL regulation has only recently entered into application, it is too early to assess how far it adds value in practice.

CEPOL supports Member States in providing training increasing basic knowledge of the EU and its instruments to the law enforcement officers. Without training, there can be no meaningful cooperation between law enforcement authorities in the EU. CEPOL can assist Member States in developing bilateral and regional cooperation via law enforcement training. It develops and coordinates the organisation of thematic training. With regard to the outreach to the third countries, it can contribute to the capacity building of law enforcement officials, thus, indirectly contributing to the good operational cooperation between third country authorities and their counterparts in the EU.

CEPOL is the EU agency that ensures that the law enforcement officials are well prepared for the cross-border cooperation and are aware and use the cooperation tools that the EU offers. It complements, stimulates and leverages Member States training activities as its cooperation model relies on CEPOL national units which liaise between CEPOL and the network of national training institutes for law enforcement officials in the Member States.

CEPOL awards grants to a network of framework partners for organising training.

CEPOL trainings are carried out in close coordination and cooperation with other European Agencies (mainly Europol, European Coast and Border Guard, EMCDDA, Eurojust, FRA, EASO) and other EU partners (EEAS, European Security and Defence College and others).

The CEPOL regulation provides that in its training activities, CEPOL promotes common respect for, and understanding of, fundamental rights in law enforcement, such as privacy, data protection and the rights, support and protection of victims, witnesses and suspects of crime, including safeguarding the rights of victims of gender-based violence. The very objective of CEPOL, as set out in Article 3 is to support, develop, implement and coordinate training for law enforcement officials, while putting particular emphasis on the protection of human rights and fundamental freedoms in the context of law enforcement.

Indeed, fundamental rights are one of the important components of training organised or supported by CEPOL.

CEPOL develops, implements and coordinates training in relation to EU missions and law enforcement capacity-building activities in third countries. This ensures that the law enforcement officials both in third countries and the ones deployed in EU missions are fully equipped to cooperate effectively with their cooperation partners.

CEPOL is open to the participation of the authorities and training institutes of third countries that have entered into agreements with the EU to that effect.

In so far as necessary for the performance of its tasks, CEPOL may establish and maintain cooperative relations with authorities and training institutes of third countries, with international organisations. To this effect, CEPOL concludes working arrangements 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, including provisions relating to participation in CEPOL's initiatives, financial contributions and staff. CEPOL has only recently started to develop the new external relations in line with the new regulation.

3. Other Information Exchange and Police Cooperation Instruments

The "Prüm Decisions"

1. Legal framework

Council Decision 2008/615/JHA on the stepping up of cross-border cooperation, particularly in combating terrorism and cross-border crime and Council Decision 2008/616/JHA on the implementation of Council Decision 2008/615/JHA are known as the "Prüm Decisions" (OJ L 201, 6.8.2008, p. 1–72). The Prüm Decisions build upon and incorporate most of the provisions of the Treaty of Prüm, which was signed in May 2005 by seven Member States. The deadline for implementing the Decisions expired on 26 August 2011.

2. Analysis

The Prüm Convention was signed on 27 May 2005 by Austria, Belgium, France, Germany, Luxembourg, the Netherlands and Spain. The Convention aimed at enabling its signatories to exchange data regarding DNA, fingerprints and vehicle registration of concerned persons and enhance cross-border cooperation against crime and terrorism. The Convention became part of the EU legal framework with two Council Decisions enacted in 2008[225].

The Prüm Decisions are primarily aimed at considerably speeding up the procedures enabling Member States to find out whether any other Member State, and if so, which, has the information it needs by conducting cross-border data comparison. The Decisions introduced procedures for fast and efficient data exchange in specific areas. The core of the Prüm framework lays down provisions under which EU Member *States* grant each other access to their automated DNA analysis files, automated fingerprint identification systems and vehicle registration data. DNA and fingerprint exchanges take place based on a "hit/no-hit" approach, which means that DNA profiles or fingerprints found at a crime scene in one EU Member State can be compared automatically with profiles held in the databases of other EU States. . If a hit is found, the requesting Member State can ask for personal data from the Member State administering the file and, where necessary, request further information through mutual assistance procedures, including those adopted pursuant to the Swedish Framework Decision. It is worth noticing that the Prüm Decision also contains rules for operational police cooperation such as joint patrols/joint operations, and on the exchange of personal data for terrorism purpose.

The Prüm Decisions remain very relevant to current needs and the statistics demonstrate increased usage by Member States law enforcement authorites of the possibilities that this tool offers in the investigation of serious crime. For example, 2568 fingerprint matches were verified in 2011 – this rose to 5826 in 2015. 20686 DNA matches were verified in 2011, rising to 37313 in 2015. 260,253 VRD responses were received by Member States in 2011, rising to 2,176,172 in 2015. The ability to conduct automated comparisons of data found at crime scenes against comparable data held in other Member States remains a significant tool for law enforcement.

The Decisions contain a provision that required the Commission to submit a report to the Council by 28 July 2012 on implementation, together with any such proposals as it deems appropriate for any further development. In its 2012 report[226], the Commission decided not to consider further developments before full implementation. It was felt that to do so would slow down implementation and create an unstable legal environment. A more recent study recommended that the progress of Member States in the implementation of the Prüm

[225] Council Decision 2008/615/JHA of 23 June 2008 on the stepping up of cross-border cooperation, particularly in combating terrorism and cross-border crime and Council Decision 2008/616/JHA of 23 June 2008 on the implementation of Decision 2008/615/JHA on the stepping up of cross-border cooperation, particularly in combating terrorism and cross-border crime.
[226] Brussels, 7.12.2012 COM(2012) 732 final.

Decisions should be analysed further and adequate action should be taken in order to ensure compliance with implementation[227]. In addition, the study noted that the delays in the implementation of Prüm could be a factor decreasing motivation in some Member States to put effort into the implementation and application of EU instruments, if they see that their counterparts are not doing the same.

Following the expiry of the transitional period under Article 10(3) of Protocol 36 to the Treaties ceasing five years after entry into force of the Treaty of Lisbon, i.e. on 1 December 2014, the limitations to the judicial control by the Court of Justice of the EU and to the Commission's enforcement powers, have been lifted. Since that date, the Commission can, under Article 258 TFEU, monitor the complete and correct transposition and implementation of these former third pillar instruments, which have not been repealed, annulled or amended after the entry into force of the Lisbon Treaty. This includes the possibility of launching infringement proceedings where appropriate. Using these new possibilities, on 29 September 2016 the European Commission addressed letters of formal notice to Croatia, Greece, Ireland, Italy and Portugal for failing to comply with the Prüm Decisions. These Member States had not yet ensured automated data exchanges in at least two of the three data categories of DNA, fingerprints and national vehicle registration data.

As mentioned, this measure provides an excellent investigative tool for law enforcement by allowing automated searching of other Member States DNA analysis files, fingerprint identification systems and vehicle registration data.

In addition to the launch of infringement proceedings, the Commission organised a workshop, which took place on 19 January 2017 with Member States on the implementation of the Prüm Decisions, designed primarily for the benefit of practitioners to allow them to learn from one another and build even stronger cooperation. Experienced, operational Member States shared their experiences of using the system, including what lessons they have learned and how they have addressed various challenges that they faced over the years. Member States concurred in highlighting the benefits that they have obtained by using Prüm – with large numbers of 'matches' providing assistance in criminal investigations.

In recognising the importance of Prüm, the Commission has provided funding and support over many years to encourage full implementation of this measure. Under the old ISEC funding, the Commission provided over € 20 million euro to Prüm-related projects. Under the current Internal Security Fund – Police, possibilities continue to exist for implementation of Prüm funding under the national programmes.

While there are centralised databases that contain some elements of similar data to those existing in Prüm (e.g. fingerprints stored SIS, the EIS, or Interpol), they contain very limited amounts of data in comparison with that which is accessible under the Prüm Decisions.

Prüm is primarily a tool to assist in the investigation of serious criminal offences. It is mainly used as a way to identify the originator of a crime stain (biological material of latent fingerprint), generating an important element in criminal investigations, potentially leading to an arrest or even to the conviction of the individual. As such, it contains a very high verification threshold in order to ensure that the correct individuals are arrested and eventually convicted.

Prüm is not designed as an identity checking tool for border guards or to give immediate answers or an on the spot instruction to a police officer or a border guard to take action. This presents an essential difference compared to databases like the SIS, which functionality it is to allow for such checking and specific follow-up instructions. As such, the use of the Prüm

[227] Study on the implementation of the European Information Exchange Model (EIXM) for strengthening law enforcement cooperation, 26.01.2015.

system serves a different purpose compared to SIS. These systems are complementary rather than in competition to each other.

The Prüm Decisions build in the data protection safeguards. Member States are subject to an evaluation on their compliance with the national data protection provisions before they are entitled to receive and supply personal data and grant one another access rights to their automated DNA analysis files, automated dactyloscopic identification systems and vehicle registration data.

In the case of data from national DNA analysis files and automated dactyloscopic identification systems, a hit/no hit system enables the searching Member State, in a second step, to request specific related personal data from the Member State administering the file and, where necessary, to request further information through mutual assistance procedures. The hit/no hit system provides for a structure of comparing anonymous profiles, where additional personal data is exchanged only after a hit, the supply and receipt of which is governed by national law, including legal assistance rules. This has enabled law enforcement authorities within the Member States to compare DNA profiles and fingerprints found at crime scenes with (anonymised) database entries in databases of all Member States. In a second step, specific related personal data can be requested from the Member State administering the file in order to match the crime evidence with the database information.

The Prüm Decisions do not have an external dimension. However, Member States have negotiated Prüm like bilateral agreements with third countries. The Commission has negotiated an agreement on accession to Prüm by Norway and Iceland and is in the process of working on a similar agreement for Switzerland and Lichtenstein.

Possible improvements to the current Prüm set up were discussed in the context of the High Level Expert Group on Interoperability of the Commission.[228] Experts present did not favour of a 'centralized' Prüm framework. In addition, in the context of the current SIS revision, Member States have expressed a preference to conduct latent fingerprint comparison work via the Prüm framework.

The Swedish Framework Decision

1. Legal framework

Framework Decision 2006/960/JHA on simplifying the exchange of information and intelligence between law enforcement authorities of the Member States of the European Union.

Sweden presented a legislative initiative on 4 June 2004 following the Council Declaration on combating Terrorism of 25 March 2004 that called for 'exploration of possibilities of greater intelligence sharing on terrorist matters'. The Council adopted the Swedish Framework Decision (the SFD) on 18 December 2006.

The legal basis is Articles 30(1)(a) and (b) and 34(2)(b) of the then Treaty on European Union.

2. Analysis

The SFD sets out common rules on procedures according to which information may be exchanged between Member States' law enforcement authorities. The essence of the SFD is that Member States must ensure that the conditions applied to providing and requesting information and criminal intelligence to or from competent law enforcement authorities from other countries are not stricter than those applicable at national level. This is referred to as the principle of "equivalent access", which is considered as a major step forward in cross-border

[228] http://ec.europa.eu/transparency/regexpert/index.cfm?do=groupDetail.groupDetail&groupID=3435.

law information exchange. The designated authorities are obliged to reply within at most eight hours in urgent cases, as long as the requested information or criminal intelligence is directly accessible to their law enforcement authorities. In addition, the SFD seeks to promote information exchange with Europol and Eurojust for crimes that fall within their mandates. The annex of the SFD provides forms aimed at facilitating the exchange between Member States.

Previous studies[229] have generally pointed out that the lack of full transposition has been a particular gap. That is no longer the case, with only Luxembourg having failed to transpose the Decision in national law. This forms part of an infringement procedure, aimed at ensuring that Luxembourg will transpose the Decision as soon as possible.

The Commission's report on the application of the SFD states that the time limits seemed to be complied with in most cases. However, the report also states that the forms provided in the annex of the SFD are rarely used because they are not considered helpful by Member States.

Recently the Commission has launched an external evaluation of the Decision. The evaluation will look at legal compliance and at practical implementation. Although legal compliance is important, the actual practical compliance by Member States, in particular how the common rules on procedures according to which information may be exchanged between Member States' law enforcement authorities are applied, is of great relevance. This is important in view of the essence of the Decision mentioned above, i.e. that Member States must ensure that the conditions applied to providing and requesting information and criminal intelligence to or from competent law enforcement authorities from other Member States are not stricter than those applicable at national level. At this stage the Commission does not have a clear picture of whether Member States are complying with the Decision – in particular, whether they are indeed making information available in accordance with the principle of equivalent access and if they are doing so within the time limits prescribed.

The Commission has routinely called for full use of the Decision[230] and has now used its infringement powers when that was necessary.

The time limits set out in the Decision are kept to in most cases and it would appear that refusals to requests are an exception.[231] On that basis, it would appear that the measure does indeed add value. However, the Commission study is now several years old and took place when a number of Member States had not transposed the SFD. As such, it merits an updated, detailed examination and this will take place via the compliance study

Links with Prüm. In the case of DNA and fingerprint data, Member States use Prüm to connect their criminal databases to the one of other Member States and can request to search the other Member States databases on a hit/no hit basis. If a hit is found, the requesting Member State can ask for personal data from the Member State administering the file and, where necessary, request further information through mutual assistance procedures, including those adopted pursuant to the SFD.

Links with the Convention Implementing the Schengen Agreement (CISA). The legislative framework for Schengen police cooperation a.o. consists of the Convention Implementing the Schengen Agreement (Articles 39-47 CISA). The provision on information exchange of Art 39 on the assistance for the purposes of preventing and detecting criminal offences has been

[229] Commission Staff Working Paper on the operation of the Swedish Framework Decision, SEC(2011) 593 Council Framework Decision 2006/960/JHA – Assessment of compliance pursuant to Article 11(2), Council Report, Council doc 14755/1/12 REV 1.

[230] Communication from the Commission to the European Parliament and the Council - Strengthening law enforcement cooperation in the EU: the European Information Exchange Model (EIXM).

[231] Study on the implementation of the European Information Exchange Model (EIXM) for strengthening law enforcement cooperation , 26.01.2015.

replaced by the SFD. The provision on information exchange of Art 46 to prevent future crime has been replaced by the SFD.

External Dimension: the SFD does not have an external dimension as it sets out common rules on procedures according to which information may be exchanged between Member States' law enforcement authorities.

Council Decision 2004/919/EC of 22 December 2004 on tackling vehicle crime with cross-border implications

1. Legal framework

The Decision was issued at a time when it was considered that vehicle crime was causing significant material damage and was seriously damaging EU citizens' sense of justice and feeling of security Consequently, it was felt that the attainment of the objective of Article 29 of the Treaty, that is to say to provide citizens with a high level of safety within an area of freedom, security and justice, was hampered. Tackling vehicle crime is a matter for the law enforcement agencies of the Member States. However, a common approach involving — wherever practicable and necessary — cooperation between the Member States and law enforcement authorities of the Member States was felt to be necessary and proportionate in order to address the cross-border aspects of this form of crime.

The legal basis of the Decision was Article 30(1)(a) and Article 34(2)(c) of the Treaty on European Union.

2. Analysis

Council Decision 2004/919/EC of 22 December 2004 requires Member States to enhance mutual cooperation between national competent authorities, to facilitate procedures for a quick repatriation of vehicles seized by the national competent authorities, to designate a contact point for tackling cross-border vehicle crime and, whenever a vehicle is reported stolen, to enter it in the SIS and, where possible, in Interpol's stolen motor vehicle database.

Pursuant to Article 12 of Council Decision 2004/919/EC, a first evaluation of the implementation of this Decision was carried out under the Slovenian Presidency in the first half 2008, and a second one was carried out by the Netherlands Presidency in the first half 2016, due to the developments initiated by the EU network of national contact points for tackling cross-border vehicle crime (CARPOL), such as the streamlining of the network of the National Contact Points (NCPs).

Among other findings, the evaluation found that CARPOL added professionalism to and strengthened the network of NCPs, and that there remains a need to need to maintain CARPOL in the long term. It would therefore appear from this evaluation that the objectives and instruments are still adapted to current needs.

In addition, Europol is actively supporting CARPOL (for instance by hosting his meetings) and by supporting joint investigation teams on the theft of luxury cars or on drugs trafficking.

Council Decision 2004/919/EC does not impact on fundamental rights. Article 5 paragraph 2 states that "*Member States shall authorise the contact points to exchange experience, expertise as well as general and technical information concerning vehicle crime on the basis of existing applicable legislation. Information exchange shall extend to methods and best practices of prevention of vehicle crime. Such exchanges shall not include exchanges of personal data*".

The external dimension of internal security has not been incorporated in the Council Decision.

Common use of liaison officers posted abroad by the law enforcement agencies of the Member States

1. Legal framework

Council Decision 2003/170/JHA of 27 February 2003 on the common use of liaison officers posted abroad by the law enforcement agencies of the Member States[232] was adopted in the light of the new possibilities opened up by the Treaty of Amsterdam to strengthen police cooperation and the action against cross-border crime. It constitutes a development of the Schengen acquis for EU Member States and Schengen Associated Countries.

Following the first evaluation of the Decision, the Council adopted 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[233].

2. Analysis

The objective of Council Decision 2003/170/JHA 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 act was inspired by similar provisions under multilateral agreements such as the Nordic or the Benelux cooperation framework.

To take account of the potential of Member States making better use of the Europol liaison officers abroad Council Decision 2006/560/JHA amended Council Decision 2003/170/JHA accordingly.

The Schengen evaluations in the field of police cooperation revealed that with a view to the growing nexus between internal and external security most Member States would like to increase the number of liaison officers posted abroad. However, following the constraints on resources as imposed by the financial crisis Member States must make very efficient use of the law enforcement liaison officer networks available. Council Decision 2003/170/JHA provides a solid legal basis for that.

The Decision allowed the Member States to enlarge their information base by improving the links between their international liaison officer networks. The concrete activities covered include networking meetings[234] and joint seminars[235] of all posted EU liaison officers in a specific country or an international organisation. The same range of activities applies to Europol liaison officers posted abroad[236].

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[237].

Any information exchanged between Member States' liaison officers posted abroad as well as between liaison officers and authorities of other Member States or international organisations is subject to compliance with national provisions governing the protection of personal data[238].

Council Decision 2003/170/JHA has an external dimension, since it is about the law enforcement information flow from and to third countries, as well as international organisations, via liaison officers. The secondment of international liaison officers is a substantial legal, financial and logistical investment for the Member States.

---

[232] OJL 67, 12.3.2003, p. 27.
[233] OJL 219, 10.8.2006, p. 31.
[234] Article 4 (1) of Council Decision 2003/170/JHA.
[235] Article 6 of Council Decision 2003/170/JHA.
[236] Article 8 of Council Decision 2003/170/JHA.
[237] Article 4 (3) of Council Decision 2003/170/JHA.
[238] Article 5 (2) and 5(5) of Council Decision 2003/170/JHA.

The Schengen evaluations carried out in the field of police cooperation show that in most countries the secondment of international liaison officers is outlined in an international police cooperation strategy. Sometimes a specific procedure is in place to identify the locations where liaison officers will have the most added value.

Council Decision 2003/170/JHA helps Member States to cover their international information exchange needs by connecting their liaison officer networks to those of other Member States.

Council Decision 2007/274/JHA of 23 April 2007 concerning the conclusion of the Agreement between the European Union and the Government of the United States of America on the security of classified information

1. Legal framework

The legal basis for Security of Information Agreements (SIAs) was formerly Articles 24 and 38 of the TEU, and is now Art 218 TFEU. Furthermore, the 2001 Council security regulations provided for "agreements on security procedures for the exchange of classified information" (Part II, Section XII). The Council mandate for an Agreement to be concluded with the United States is set out in Council document 13819/03.

2. Analysis

The specific objectives set in the 2003 mandate from the Council were to draw up an agreement on security *procedures* for the exchange of classified information with (inter alia) the United States, defining the purpose of cooperation and the reciprocal rules on the protection of the information exchanged. These specific objectives were expanded upon in the second recital to the Agreement, which establishes the more general objective shared by the United States Government and the EU "to strengthen their own security in all ways and to provide their citizens with a high level of safety within an area of security".

There is no *a priori* limit on the subject matter of classified information which can be exchanged under an SIA, and there is no pre-set termination date for the Agreement. An SIA provides the EU and the third country/international organisation with a long-term procedural framework that ensures that any classified information exchanged between the parties is given a level of protection commensurate with its security classification. An Agreement of this kind does not create an obligation on a Party to provide any information to the other Party, and as such there is no regular assessment of whether the objective of the Agreement itself is being attained. However, the EEAS hosted a three-day visit by the United States Office of the Under Secretary of Defence for Policy in the Spring of 2016, and the US conveyed its satisfaction with the system and procedures in place on the EU side for exchanging classified information under the Agreement.

As a result of the entry into force of the Treaty of Lisbon in 2009, a Council Note Verbale was issued to bring the EEAS, the High Representative and the European Council into the scope of the existing SIA with the United States (which hitherto on the EU side had only covered the Council and the Commission).

SIAs concluded on behalf of the EU do not "substitute" existing bilateral agreements between a Member State and a given third State on exchanging classified information. Neither do EU SIAs obviate the need for any future bilateral agreements on classified information exchanges between a Member State and a given third State.

This Agreement with the United States is just one in a series - the EU has Security of Information Agreements with: Australia, BiH, FYROM, Iceland, Israel Liechtenstein, Montenegro, Norway, Serbia, Switzerland, Ukraine, United States, and with several international organisations: NATO and the European Space Agency (ESA). Negotiations are also underway for further Security of Information Agreements with Canada, Turkey, the Russian Federation, Albania, Georgia, Moldova, Morocco and OCCAR. The EU also has a

cooperation agreement with the International Criminal Court which enables it to disclose EU classified information.

The United States receives classified information under the SIA for its participation in two European cooperation projects in the area of CFSP:

a. the European Union Rule of Law Mission EULEX KOSOVO
b. the European Union mission to provide advice and assistance for security sector reform in the Democratic Republic of the Congo (EUSEC RD Congo)

SIAs also facilitate the participation of non-EU States in joint EU projects such as Galileo, various research projects, aviation security, terrorism and for managing external borders, for example.

SIAs do not contain a specific reference to Fundamental Rights, however, they support EU military operations and civilian missions, which themselves protect Fundamental Rights.

SIAs are external instruments. Furthermore, exchanging classified information with certain non-EU countries on terrorism or on war criminals, for instance, has a strong potential to improve the internal security of the EU.

4. Eurojust and related judicial cooperation tools

Eurojust

1. Legal framework

Council decision of 28 February 2002 setting up Eurojust with a view to reinforcing the fight against serious crime (2002/187/JHA) was adopted on the basis of Articles 31 and 34(2)(c) TEU.

Council Decision 2005/671/JHA of 20 September 2005 on the exchange of information and cooperation concerning terrorist provides that Member States shall take the necessary measures to ensure that at least the information concerning prosecutions and convictions for terrorist offences which affect or may affect two or more Member States, gathered by the relevant authority, is transmitted to Eurojust.

The Commission proposed a Regulation of the European Parliament and of the Council on the European Union Agency for Criminal Justice Cooperation (Eurojust) on 17/07/2013 (2013/0256/COD) (replacing the above mentioned Decision), based on Article 85 TFEU.

2. Analysis

Eurojust's priorities, as set up by the European Agendas on security and on migration, are the fight against terrorism, cybercrime and the smuggling of migrants. The role of Eurojust is particularly emphasised in four areas of activity: (i) assisting the Member States in complex MLA requests with countries outside the European Union, especially through the network of Eurojust contact points; (ii) being fully involved in the activities of the European Counter Terrorism Centre (ECTC) at Europol to improve coordination of investigations and prosecutions; (iii) offering more expertise and assistance to national authorities when conducting financial investigations; and (iv) continuing to facilitate the exchange of best practice and identifying the challenges faced in the collection and use of e-evidence in investigations and prosecutions of Internet-facilitated crimes. Eurojust was set up in 2002 to reinforce the fight against serious organised crime in the European Union. Ever since, Eurojust has facilitated 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.

The fight against organised crime and the disruption of criminal organisations remain a daily challenge. Terrorism, cybercrime, drug trafficking and trafficking in human beings, in particular migrants, fraud and corruption are some examples of those cross-border crimes. Their common feature is that they are committed across borders by highly mobile and flexible groups operating in multiple jurisdictions and criminal sectors. Combatting them effectively therefore requires a coordinated pan-European response.

Under the Lisbon Treaty, new possibilities to enhance Eurojust's efficiency in tackling these forms of criminality have been introduced. Article 85 TFEU explicitly recognises Eurojust's mission of supporting and strengthening coordination and cooperation between national investigating and prosecuting authorities in relation to serious crime affecting two or more Member States or requiring a prosecution on common bases.

The proposal for a Regulation takes all these elements into consideration and provides a single and renovated legal framework for a new Agency for Criminal Justice Cooperation (Eurojust) which will be the legal successor of Eurojust as established by Council Decision 2002/187/JHA. Whilst maintaining elements that have proved efficient in the management and operation of Eurojust, the Regulation modernises its legal framework and streamlines its functioning and structure in line with the Lisbon Treaty and the requirements of the Common Approach on Agencies, as far as its nature allows.

Eurojust interacts with national law authorities and other Union agencies, in particular Europol and its recently created centres of expertise, regarding their three common priorities on terrorism, migration and cybercrime. Eurojust may be less visible than other operational agencies, given its essentially coordination functions with regard to national prosecutorial and judicial action, undertaken by Member States, but its added value is regularly praised by Member States and the EU Institutions. Member States trust Eurojust and refer an increasing number of serious cross-border cases to Eurojust for coordination. The constant growth of Eurojust's activities is a clear demonstration of its added value (increase of 23% of caseload in 2015 compared to 2014 and of 4% in 2016 compared to 2015).

Support to the policy implementation in the field of fight against crime (including cybercrime) and terrorism has also been provided by the security research programme in both Framework Programme 7[239] and Horizon 2020[240]**.** A large number of projects delivered concrete results, guidelines, trainings, etc[241].

In the framework of its activities Eurojust respects fundamental rights, in particular data protection rules. These are reflected in the legal framework currently applicable to Eurojust and in the proposed Regulation.

Links with third countries are very frequently detected in serious and organised crime cases, hereby rendering crucially the close cooperation with these countries. Eurojust has cooperation agreements, which allow for the exchange of operational information, with the US, Switzerland, Norway, the Former Yugoslav Republic of Macedonia, Iceland, Liechtenstein, Moldova, Montenegro and Ukraine[242].

Eurojust's current priority is to swiftly conclude cooperation agreements with all enlargement countries as well as with Georgia and Israel.

[239] https://ec.europa.eu/research/fp7/index_en.cfm?pg=security.
[240] https://ec.europa.eu/programmes/horizon2020/en/h2020-section/secure-societies-%E2%80%93-protecting-freedom-and-security-europe-and-its-citizens.
[241] The full list of security research projects, including those dealing with fight against crime and terrorism, can be found here: https://ec.europa.eu/home-affairs/financing/fundings/research-for-security_en
[242] Agreements with Montenegro and Ukraine have not yet entered into force.

As a consequence of the Lisbon Treaty, Agencies will no longer be able to negotiate international agreements themselves – such agreements will have to be established in accordance with Article 218 TFEU (negotiation by the Commission based on a mandate of the Council). This should allow for a coordinated approach amongst EU Agencies, e.g. amongst Eurojust and Europol.

Where Cooperation Agreements do not yet exist (because of data protection requirements/rule of law standards), cooperation is nevertheless possible to a more limited extent, and without the possibility of exchanging operational information. Cooperation is organised through Eurojust's worldwide network of (today 41) Contact Points within the judicial authorities in third countries. Efforts have been made in recent months to expand the network of Contact Points especially in the Middle East and North Africa region, with good progress.

Where cooperation agreements are signed and in force, Eurojust has the legal basis (not yet used) for posting EU liaison magistrates in counterpart countries and liaison magistrates from third countries can be posted at Eurojust (currently one from US, Norway and Switzerland).

Council Framework Decision of 13 June 2002 on the European arrest warrant and the surrender procedures between Member States 2002/584/JHA

1. Legal framework

Council Framework Decision of 13 June 2002 on the European arrest warrant and the surrender procedures between Member States 2002/584/JHA is based on Art. 31(a) and (b) and Art. 34(2)(b) TEU.

The Vienna Action Plan (item 45 c), the conclusions of the Tampere European Council (point 35), the Strategy of the European Union for the next millennium as regards prevention and control of organised crime (recommendation 28), joint declaration by the heads of State and Government of the European Union, the President of the European Parliament, the President of the European Commission, and the High Representative for the Common Foreign and Security Policy of 14 September 2001 following the terrorist attacks of 11 September 2001.

2. Analysis

- The purpose of the European arrest warrant (EAW)[243] is the enforced surrender of a person from one Member State to another. The proposed procedure replaces the traditional extradition procedure in all respects and not limited to certain offences.
- The mechanism is based on the mutual recognition of judicial decisions. The basic idea is as follows: when a judicial authority of a Member State requests the surrender of a person, either because he has been convicted of an offence or because he is being prosecuted, its decision must be recognised and executed automatically throughout the Union.
- The procedure for executing the European arrest warrant is judicial procedure among the national judicial authority. The political phase inherent in the extradition procedure is abolished. Accordingly, the administrative redress phase following the political decision is also abolished. The removal of these two procedural levels should considerably improve the effectiveness and speed of the mechanism.
- The European arrest warrant takes into account the principle of citizenship of the Union. The exception made for the nationals should no longer apply.
- The grounds for refusal to execute the arrest warrant are limited and are listed in order to simplify and accelerate the procedure. The principle of double criminal liability is abolished with regard to a list of 32 offences.

[243] http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52001PC0522.

- The elements appearing in the European arrest warrant are standardised at the level of the Union.

The Commission has issued a number of implementation reports[244] based on information provided by Member States. In its reports the Commission has identified some problems with the implementation or application. There have been a number of activities aimed at capacity building in the Member States to facilitate the day-to-day application for the national authorities dealing with EAW cases. The Commission conducts regular dialogues with Member States to discuss concrete issues of application of EAW at the level of experts meetings, at Council Working Group meetings and on a bilateral basis. The Commission has worked with the Member States to develop a comprehensive handbook on the use of the EAW. The handbook is aimed at practitioners (notably national judges dealing with EAW) and it provides guidance on how to issue and execute EAW in different scenarios. At the same time the EU adopted the procedural rights package that reinforces procedural rights of suspected or accused persons, including those who are requested under the EAW[245].

The application of the Framework Decision is also sometimes obstructed by elements which are not related to the Framework Decision itself as e.g. the violation of fundamental rights of the requested person in the issuing Member State related to poor prison conditions[246]. These problems are being approached in particular by working together with the Council of Europe, and stakeholders involved on possible steps that can be taken to improve detention conditions in Member States in order to enhance the efficient operation of the EAW.

The EAW, the first instrument adopted on the basis of mutual recognition of judicial decisions, is today the most frequently used EU instrument in the area of judicial cooperation in criminal matters. During 13 years of its operation it has become a key tool in the fight against crime, and an important aspect of internal security in the EU.

The EAW replaced lengthy extradition procedures within the EU. It improves and simplifies judicial procedures designed to surrender persons for the purpose of conducting a criminal prosecution or executing a custodial sentence or detention order.

Member States issued over 120,000 European arrest warrants between 2005 and 2015, leading to over 70,000 persons being surrendered.

Before the EAW, with the traditional extradition procedures it used to take on average one year to surrender a person from one state to another. EAW has had a marked effect in speeding up the transfer of persons between Member States. In 2015 it took on average only 15 days to have a person surrendered from another Member State in case of the requested person's consent and only 54 days in case if the requested person did not consent.

While the 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.

Article 1(3) and recitals 12 and 13 clarify that fundamental rights and fundamental legal principles should be respected in the context of the EAW. The Framework Decision on EAW also grants the requested person several procedural rights. In accordance with Article 11 the requested person has the right to be informed of the EAW and of its contents, the possibility of consenting to the surrender and to a legal counsel and an interpreter. These rights must be

[244] Commission issued implementation reports in 2005, 2007 and 2011.

[245] Recently adopted EU provisions within the "procedural rights package" strengthen procedural rights of persons requested under European arrest warrant by providing for a right of access to a lawyer, right to information (letter of rights), right to interpretation and translation, right to have a third person informed and a right to communicate with consular authorities elated to procedural rights.

[246] Ex. in January 2017 the execution of an EAW issued in Romania was put to an end for the first time by a Dutch court in line with the CJEU judgement in Aranyosi/Caldararu judgement (case C-404/15) because of risks of violation of the requested person's fundamental rights due to poor prison conditions in Romania.

provided in accordance with the national law of the executing Member State. In addition, various provisions of the Framework Decision on EAW grant the requested person rights, in particular Article 4a(2) (right to information on judgments rendered *in absentia*) Articles 12 (provisional release), 13(2) (legal counsel for taking the decision to consent), 14 (right to be heard), 19 (right to be heard), 23(5) (release upon expiry of the time limits for surrender of the person). These rights are strengthened by the specific instruments on procedural guarantees.

Based on the CJEU judgment in Aranyosi/Caldararu, the consideration of risks of violation of the requested person's fundamental rights in the issuing state are to be taken into account by the executing judicial authority.

In addition, the above-mentioned handbook on how to issue and execute a EAW is expected to result in a more proportionate use of the EAW.

Exchange of information and cooperation concerning terrorist offences (Decision 2005/671/JHA)

1. Legal framework:

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[247]

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[248]

2. Analysis

- Mandatory collection and sharing of information concerning criminal investigations by law enforcement authorities on terrorist offences with Europol and other interested Member States
- Mandatory collection and sharing of information concerning prosecutions and convictions for terrorist offences with Eurojust and with other interested Member States

Information exchange is a prerequisite for effective counterterrorism cooperation at EU and international levels. This was recognised in the 2005 *EU Counter-Terrorism Strategy*[249] and more recently by the European Council, the European Parliament, the Council and the Commission, including in the 2015 European Agenda on Security.

The *UNSC Resolution 2178 (2014)* urges Member States to intensify and accelerate the exchange of operational information regarding actions or movement of terrorists or terrorist networks.[250]

The *Additional Protocol to the Council of Europe Convention on the Prevention of Terrorism* of 22.10.2015 includes further provisions on the exchange of information, including through the designation of a point of contact allowing for 24/7 exchange.[251]

The Decision contains unique provision on the mandatory sharing of information with Europol and other interested Member States on terrorist offences. The new Europol regulation (article 7 (6)) does not include such specific and mandatory provisions.[252] These provisions

[247] http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32005D0671.
[248] http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:32017L0541.
[249] http://register.consilium.europa.eu/doc/srv?l=EN&f=ST%2014469%202005%20REV%204.
[250] http://www.un.org/press/en/2014/sc11580.doc.htm.
[251] https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=090000168047c5ea.
[252] http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32016R0794.

have been further strengthened with the adoption of the new Directive on combating terrorism in March 2017 in regard to exchange of information between Member States.

While the Decision has proved challenging to effectively monitor and enforce, the legal provisions coupled with the political commitment (by the European Council, the Parliament, the Council and the Commission) and 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.[253] Yet, as pointed out by the Counter Terrorism Coordinator, "information sharing still does not reflect the threat"[254]: there remains significant room for improvement in the sharing of information with both Europol and Eurojust. The Commission will address this issue in the transpositions workshops on the Directive on combating terrorism in the context of the amendments of the Decision by that Directive.

Within Europol, the European Counter Terrorism Centre (ECTC) was established to support Member States' anti-terrorism law enforcement authorities, pool resources and maximise the use of already existing structures, services and tools available to the Agency.

The more Member States proactively share information with Europol (and with each other), the more likely cross-checks against other databases (Europol databases such as the EIS or the Focal Points, or other EU instruments such as the SIS, VIS, Eurodac, financial intelligence and TFTP data, and in the future PNR data, EES and ETIAS) will generate hits and additional leads for further investigation. With the launch of the ECTC, Member States have significantly increased their information exchange with Europol (+75% SIENA cases on terrorism) which in turn led to an increase (+48%) in the number of operation supported by the focal points.[255]

The CTC noted that the experience of Europol's Task Force *Fraternité* provides a "blueprint" of the support that Europol (ECTC) can provide to Member States' investigators.[256] Europol received an unprecedented amount of high-value information (19 TB of data) which led to 2500 SIENA messages, 1247 leads from the TFTP, 60 PNR requests and 80 operational analysis reports.

The Decision mentions clearly that it respects the fundamental rights and observes the principles recognised in particular the Charter of Fundamental Rights of the European Union. In implementing the rules of the Decision, Member States are bound to respect the Charter. In addition, fundamental rights provisions of Europol and Eurojust regulations apply.

The Decision does not provide for the exchange of information with third countries. However, the UN Security Council Resolution and the Additional Protocol to the Council of Europe's Convention on the Prevention of Terrorism contain relevant provisions in that regard.

Europol acts as an information hub on terrorist offences with third countries on the basis of existing cooperation agreements, as well as data received directly or through Interpol.

5. Security Dimension of Borders

Customs Co-operation / Mutual administrative assistance in customs matters

1. Legal framework

[253] https://www.europol.europa.eu/newsroom/news/information-sharing-counter-terrorism-in-eu-has-reached-all-time-high.
[254] http://data.consilium.europa.eu/doc/document/ST-6785-2016-INIT/en/pdf.
[255] https://www.europol.europa.eu/newsroom/news/information-sharing-counter-terrorism-in-eu-has-reached-all-time-high.
[256] Ibid.

Customs co-operation and mutual administrative assistance in customs matters are governed by three main instruments:

(1.) Regulation 515/97 of 13 March 1997 on mutual assistance between the administrative authorities of the Member States and co-operation between the latter and the Commission to ensure the correct application of the law on customs and agricultural matters. This Regulation was adopted within the framework of the EU Customs Union and lastly revised by Regulation 1525/2015 of 9 September 2015 (based on Art. 33 and 325 of the TFEU).

(2.) Council Act of 18 December 1997 drawing up the Convention on mutual assistance and cooperation between customs administrations (also called **'Naples II' Convention**). The Naples II Convention was adopted on the basis of Art. K.3 of the TEU (currently Art. 87 TFEU) and includes provisions for mutual assistance and cooperation between customs administrations in order to investigate and prosecute customs infringements. The Naples II Convention was adopted within the framework of the former third pillar area. It largely mirrors the provisions of Regulation 515/97.

(3.) 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). This Decision, which establishes the Customs Information system ('**CIS Decision**'), was adopted within the framework of the former third pillar area and replaced the Convention of 26 July 1995 on the use of information technology for customs purposes. The CIS Decision duplicates the corresponding provisions of Regulation 515/97 with regard to national aspects.

2. Analysis

(1.) Regulation 515/97 covers **administrative assistance between the customs authorities** of the Member States and between Member States and the Commission. The purpose of this assistance is to ensure the correct application of the EU customs and agricultural legislations through mutual exchange of information which includes:

- administrative investigations upon request;
- spontaneous exchange of information;
- cooperation with the Commission (OLAF) for cases presenting an EU dimension;
- Joint Customs Operations (JCOs are carried out by Member States in co-operation with OLAF with specific checks at EU level; they are coordinated and targeted actions of a limited duration with the aim of combating the smuggling of sensitive goods and fraud in certain risky areas and/or on identified trade routes).

Furthermore, this Regulation provides a legal basis for a number of databases, which are accessible through an IT platform (**AFIS, Anti-Fraud Information System**), to exchange and collect data in order to ensure the correct application of the customs and agricultural legislations:

- Customs Information System (CIS), which contains information on suspected or established infringements and fraud in customs matters, including customs investigations, as well as requests for taking specific actions;
- Customs File Identification Database (FIDE), which allows the Commission and Member States, when opening a file or investigating one or more persons or businesses, to identify competent authorities of other Member States/Commission which are or have been investigating those identical persons or businesses;
- Container Status Messages (CSM) database, a large new IT tool which contains information on movements of containers entering or leaving the EU territory;
- Import, Export and Transit (IET) database (only excisable goods at export).

This Regulation is also used to fight *inter alia* cigarette smuggling by coordinating investigations.

In the context of the Security Union, the Regulation can also formally be applied when other Regulations refer to the use of Regulation 515/1997 *mutatis mutandis*, e.g. concerning **fire arms trafficking, IPR fraud, cash movements**, etc.

Regulation 515/97 was updated in 2015 and amended by Regulation 2015/1525. Despite the progress brought by this reform there are still a number of areas for improvements, in particular some Member States have recently considered insufficient the legal basis to exchange information with a third country in the absence of a mutual administrative assistance agreement between the EU and this country.

Regulation 515/97 contains detailed provisions on data protection including personal data. The European Data Protection Supervisor (EDPS) supervises compliance of the CIS with Regulation 45/2001 on personal data protection.

Regulation 515/97 contains provisions on relations with third countries. Under certain conditions, information obtained pursuant this Regulation may be communicated to third countries by the Commission or Member States. Such communication by Member States shall be made in compliance with its domestic provisions applicable to the transfer of personal data to third countries. In all cases, it shall be ensured that the rules of the third country concerned offer a degree of protection equivalent to that provided for in that Regulation. Moreover, under certain conditions notably the prior authorisation of the Member States which included them in the CIS, the transfer of data obtained from the CIS to third countries and international or regional organisations is also envisaged.

(2.) The **Naples II Convention** is a legal tool which 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. This Convention only covers co-operation and information exchanges between Member States. The Commission/OLAF does not play any specific role in this context.

This Convention meets the needs 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 Convention applies to the national customs provisions, including prohibitions and restrictions such as **illicit drugs, weapons, munitions, explosives, as well as nuclear materials and equipment for biological and chemical weapons**. The Convention defines 'infringements' in a broad sense. They cover all forms of participation and attempts, participation in a criminal organisation and money laundering. Mutual assistance is provided upon request or spontaneously.

The Convention also covers special forms of cooperation, which are not specifically foreseen in Regulation 515/97, such as cross border surveillance, hot pursuit, controlled delivery, covert investigations and joint special investigation teams. Requests are normally exchanged between the central coordinating units appointed within each national customs administration. Requests are made in writing but can be made orally in emergency situations.

The Naples II Convention has not been revised since its adoption in 1997 and may need to be updated by another legal tool in order to take account of the development of fraud methods and adapt Member States needs for the exchange of information. At this stage, no assessment has been made on potential gaps/shortcomings.

The Naples II Convention contains provisions on data protection for the exchange of data. These provisions have not been updated since 1997.

The Naples II Convention does not contain specific provisions on relations with third countries.

(3.) Council Decision 2009/917/JHA creates the Customs Information System (CIS) and the Customs Files Identification Database (FIDE) to assist in preventing, investigating and prosecuting serious contraventions of national laws by making information available more rapidly. The provisions on the CIS and FIDE under this Decision mirror the corresponding provisions of Regulation 515/97. The Commission/OLAF is responsible for the operation of these systems but has no access to the data.

In practice, unlike the CIS under Regulation 515/97 which allows Member States and the Commission to exchange information on cases of infringement of EU law for example in the areas of tobacco, intellectual property rights and cash movements, the CIS under this Decision allows Member States to exchange information on cases of infringement of national laws for example in the areas of **weapons and drug trafficking**.

The notion of 'national laws' is interpreted broadly. It means not only national laws or regulations in the application of which the customs administration has total or partial competence concerning the movement of goods subject to measures of prohibition, restriction or control, but also includes the transfer, conversion, concealment, or disguise of property or proceeds acquired or obtained directly or indirectly through illicit international drug trafficking or by infringement of measures of prohibition, restriction or control.

Council Decision 2009/917/JHA could be further updated, if only in order to align its provisions with the improvements introduced by Regulation 2015/1525 (e.g. on access to data).

Council Decision 2009/917/JHA contains provisions on data protection including personal data and establishes the Customs Joint Supervisory Authority to oversee the protection of personal data collected under this Decision. The EDPS co-ordinates with the Joint Supervisory Authority, each acting within the scope of their respective competence, with a view to ensuring co-ordinated supervision and audits of the CIS.

Council Decision 2009/917/JHA provides, under certain conditions notably the prior authorisation of the Member States which included them in the CIS, the transfer of data obtained from the CIS to third countries and international or regional organisations.

The creation of databases and IT systems centralised at EU level (managed by OLAF) and allowing Member States authorities to not only have direct access to relevant information but also to exchange information between each other and the Commission for anti-fraud purposes has contributed to supporting and facilitating European co-operation, improving national capabilities and complementing Member States action.

Directive on advance passenger information (API)

1. Legal framework

Council Directive 2004/82/EC of 29 April 2004 on the obligation to communicate passenger data has been adopted on the basis of Art. 62(2)(a) (measures on the crossing of the external borders of the Member States) and Art. 63(3)(b) (measures on immigration policy) of the Treaty establishing the European Community. These Articles are now Art. 77(1)(b) and Art. 79(2)(c) TFSU.

The API Directive was adopted as a measure aiming both at efficiently monitoring the crossing of external borders and tackling illegal immigration.

2. Analysis

- To improve border control and to fight illegal immigration: API has facilitated the improvement of border controls and contributed to the reduction of irregular migration.

- To improve law enforcement: API was also considered as effective in improving law enforcement where law enforcement authorities had access to API in accordance with national law.

Air carriers must transmit at the request of the authorities responsible for carrying out checks on persons at external borders, by the end of the check-in, API data (number and type of travel document, nationality, full names, border crossing point of entry, code of transport, departure and arrival time of the transportation, total number of passengers carried and initial point of embarkation) of the passengers they carry to an EU Member State (EU inbound flights).

The API Directive has been evaluated in 2012[257].

The Commission must assess the need to revise the API Directive in 2017 (see COM(2016) 205 on Stronger and Smarter Information Systems for Borders and Security).

API has been effective in **improving border controls**, primarily in helping border management authorities to better prepare for the control of specific passengers through advance screening of their API data. However, the effectiveness of API in improving border controls has been limited because the relative quality of API data submitted by carriers.

API is considered to have contributed to **reducing irregular migration** by improving risk-based profiling of international passengers and by increasing the rate of detection of persons identified as irregular migrants.

In the context of law enforcement, API have **helped identifying persons** posing security risks and other persons including victims of human trafficking and smugglers. API has also helped to keep track of identified suspicious persons.

The inclusion of EU outbound flights and the systematic transmission of API data for all EU inbound and outbound flights could be areas for improvement (see COM(2016)205). The API Directive has provided Member States a legal basis for requesting airlines the transmission of API data of the passengers they carry to the EU. In the absence of such legal basis, airlines do not transmit API data of their passengers. By providing minimum standards, the API Directive has supported Member States in harmonising to some extent the standards of national API programmes. In its 2016 Communication on stronger and smarter information systems for borders and security, the Commission emphasised that the added value of API data would increase if Member States were establishing automated cross checking of API data against SIS and Interpol's SLTD database.

Directive (EU) 2016/681 on passenger name record (PNR) includes API data as part of PNR data. Therefore, provisions of the PNR Directive must be taken into account where relevant (e.g. access to API by law enforcement authorities for the purposes of the PNR Directive) and its implementing acts (defining the data format and protocols for the transmission of API pursuant to the PNR Directive).

Important to note is that while there is always a PNR file for each passenger, air carriers collect API data of passengers only if required to do so by the competent authorities of the country of arrival. The PNR Directive states that air carriers must transmit API data only to the extent that they are collected in the normal course of their business. Consequently, a distinct legal basis requiring air carriers to collect and transmit API data (systematically or upon request) is necessary. In the absence of a legal requirement, airlines do not usually collect API data because they don't need them to operate a flight.

Consistency with Directive 2001/51/EC (carriers' liability): the transmission of API data does not discharge air carriers from their obligations under Directive 2001/51/EC.

[257]Final Report for Directorate General Home Affairs, ICF, GHK, September 2012, available at http://ec.europa.eu/dgs/home-affairs/e-library/documents/categories/reports/index_en.htm.

Commission's proposals on the Entry-Exit System (EES) and on the European Travel Information and Authorisation System (ETIAS) provide for the query of EES and ETIAS by air carriers. EES and ETIAS should be queried using the API data contained in the machine readable zone of the passenger's travel document via an interactive API system.

A number of safeguards apply to the processing of API data. First, the Directive comes under the scope of Directive 95/46/EC which applies with regard to the processing of personal data by the authorities of the Member States. In addition, the API Directive specifically lays down that after passengers have entered, the authorities shall delete the data received within 24 hours after transmission (unless the data are needed for the purposes of exercising the statutory functions of the authorities responsible for carrying out checks on persons at external borders). Air carriers must delete these data within 24 hours of the arrival of the means of transportation. Passengers must be informed that their API data are processed.

According to an external study carried out in 2012 on the implementation of the Directive, the remit and activities of the actors involved in the implementation and functioning of the Directive (Ministries, border authorities, data protection authorities, law enforcement authorities, judicial authorities) are in line with the Directive requirements and with the division of competences set by the national legal systems and no major compliance problems with data protection rules have occurred.

Overall, stakeholders have not experienced any major problems in relation to data protection, including fundamental rights breaches. Stakeholders also reported that the risk of occurrence is pretty low since Data Protection rules are observed and specific mechanisms have been put in place. These conclusions remain valid.[258]

The API Directive has an intrinsic external dimension as it covers EU inbound flights.

Regulation 428/2009 setting up a Union regime for the control of exports, transfer, brokering, technical assistance and transit of dual-use items

1. Legal framework

Regulation (EC) No 428/2009 (below the "Regulation") is a trade instrument that forms part of the common commercial policy under Article 207 TFEU while pursuing foreign and security policy objectives.

Export controls derive from international obligations (in particular UN Security Council Resolution 1540, the nuclear Non-Proliferation Treaty, the Chemical Weapons Convention and the Biological Weapons Convention) and essentially transpose into EU law the commitments agreed upon in multilateral export control regimes. They contribute directly to the EU Security Strategy and the EU Strategy against proliferation of Weapons of Mass Destruction (WMD).

2. Analysis

The objective of the Regulation is to control trade in dual-use items – goods, software and technology that have both civilian and military applications – in order to prevent the risks that this may pose for international security. Specifically, the Regulation aims at preventing EU trade from contributing to the proliferation of nuclear, biological or chemical weapons or their means of delivery or to the destabilising accumulation of conventional weapons or to regional conflicts.

The Commission's 2013 report to the European Parliament and Council[259] concluded that, although the system provides solid legal and institutional foundations, it cannot remain static

[258] Evaluation on the implementation and functioning of the obligation of carriers to communicate passenger data set up by Directive 2004/82 – GHK – 17.09.2012.
[259] COM(2013)710 of 16 October 2013.

and must be upgraded in order to face new challenges and generate the modern control capabilities the EU needs for the coming decade and beyond. The European Parliament and the Council, for their part, also called for a review and strengthening of export controls. A 2014 Commission Communication[260] outlined options for its modernisation and adaptation to rapidly changing technological, economic and political circumstances. The Commission subsequently conducted an impact assessment and adopted a legislative proposal for the modernisation of EU export controls[261].

The gradual development of an EU export control system since the late 1990's has offered added-value by:

- providing a solid and common legal basis for Member States to apply controls in a consistent and coordinated manner e.g. to the same list of dual-items;
- providing for coordination and information exchange, as well as operational support tools (e.g. IT infrastructure and database) that enhance the capacity of national competent authorities to implement controls;
- providing a forum for coordination of policies and development of common approaches to third countries.

Policy, regulatory and operational support actions at EU level have contributed to reducing security loopholes and distortions of competition.

The Regulation enables competent authorities to prevent the export of certain items – in particular cyber-surveillance technology – when there is evidence that the export may contribute to the human rights violations in third countries, and thus contributes to the protection of human rights.

The Regulation provides for controls to apply within EU jurisdiction but pursues objectives that relate broadly to international security, including internal and external security consideration. Data on export denials shows that controls regularly prevent export of sensitive technologies that might otherwise be used e.g. for fuelling regional conflicts, WMD proliferation or terrorism.

Regulation (EU) No 1077/2011 of the European Parliament and of the Council of 25 October 2011 establishing a European Agency for the operational management of large-scale IT systems in the area of freedom, security and justice

1. Legal framework

The Regulation establishing eu-LISA was adopted in 2011 and amended in 2015. The Regulation is based on Articles 74, 77(2)(a) and (b), 78(2)(e), 79(2)(c), 74, 82(1)(d) and 87(2)(a) and 88(2) TFSU. In joint statements accompanying the SIS II and VIS legal instruments, the Council and the European Parliament invited the Commission, following an Impact Assessment containing a substantive analysis of alternatives, from the financial, operational and organisational perspective, to present the necessary legislative proposals entrusting an agency with the long term operational management of SIS II and VIS. After the analysis of different options in the impact assessment[262], a new Regulatory Agency was found to be the most feasible alternative for carrying out the tasks of a "Management Authority" for these systems in the long term.

2. Analysis

The main objective of the measure was to establish an Agency responsible for the long-term operational management of the second-generation Schengen Information System (SIS II), the

[260] COM(2014)244 of 24 April 2014.
[261] COM(2016)616 of 28 September 2016.
[262] COM (2009) 293 final.

Visa Information System (VIS) and EURODAC. The Regulation also lays down the framework for the development and the operational management by the Agency of other large-scale IT systems in the area of freedom, security and justice if so provided by relevant legislative instruments.

In accordance with Article 31 of the establishing Regulation the first evaluation was carried out by the Commission in close consultation with the Management Board to examine the way and extent to which the Agency effectively contributes to the operational management of large-scale IT systems in the area of freedom, security and justice and fulfils its tasks laid down in the establishing Regulation. On the basis of the evaluation, the Commission after consulting the Management Board should issue recommendations regarding changes to the Regulation and shall forward them, as well as appropriate proposals to the European Parliament, the Council and the European Data Protection Supervisor. The recommendations have been included in the evaluation report to be adopted on 28 June 2017 and taken into account for the elaboration of the revision of the eu LISA legal basis, adopted the same day

Four years after the Agency took over its core tasks in December 2012, the evaluation findings have showed that the Agency has fulfilled its tasks, including new tasks entrusted to it, in an effective and efficient manner. The findings have also indicated that eu-LISA has effectively contributed to the establishment of a coordinated, effective and coherent IT environment for the management of large-scale IT systems supporting the implementation of JHA policies.

However, there are shortcomings to be remedied in order to improve the functioning of the Agency and enhance and strengthen its role, to ensure that its mandate is adapted to meets current challenges at EU level in the area of migration and security. Most of the shortcomings identified in the evaluation can be addressed without legislative amendments.

The shortcomings which would require legislative amendments as identified in the evaluation are the following:

- the coherence of the management of the communication infrastructure should be improved by transferring the Commission's related tasks (in particular the implementation of the budget, acquisition and renewal and contractual matters) to the Agency;
- the scope of cooperation with other JHA agencies should be clarified within the eu-LISA mandate;
- an interim report to the Commission should be presented by the end of August each year on progress on planned activities to allow proper monitoring;
- the scope of pilot projects which eu-LISA may carry out should be extended at least to pilot projects with an existing basic act;
- eu-LISA should be given an extended responsibility for statistics on the systems;
- a new task should be entrusted to eu-LISA to produce data quality and data analysis reports to improve the control of implementation of the systems' legal instruments.

Moreover recent policy and legislative developments call for limited revision or extension of, the tasks entrusted to eu-LISA in the establishing Regulation and the systems' legal instruments. In 2016 the Commission adopted proposals to entrust new systems to the Agency: the Entry/Exit System, the automated system for registration, monitoring and the allocation mechanism of applications for international protection and the EU Travel Information and Authorisation system (ETIAS). The adoption of those initiatives by the co-legislators would require changes to the eu-LISA Regulation. eu-LISA could also be given explicit mandate to carry out the tasks described in the Communication from the Commission to the European Parliament and the Council: Stronger and Smarter Information Systems for

Borders and Security adopted on 4 April 2016[263] and in the Commission's Seventh progress report towards an effective and genuine Security Union of 16 May 2017.[264]

In general, the evaluation provided the necessary reassurance that the creation of eu-LISA has provided an added value, notably through bringing the three systems together 'under one roof', pooling of expertise, harnessing of synergies and allowing a more flexible framework than was possible before. The Commission can now focus on its policy/normative prerogatives rather than having to deal, at the same time, with issues related to the operational management of the systems.

Article 28 of Regulation (EU) No 1077/2011 provides that, without prejudice to the provisions on data protection laid down in the legislative instruments governing the development, establishment, operation and use of large-scale IT systems, the information processed by the Agency in accordance with this Regulation shall be subject to Regulation (EC) No 45/2001. The proposal to revise the mandate of the Agency also respects fundamental rights and observes the principles set out in the Charter of Fundamental Rights of the European Union. It enlarges the scope of its tasks in particular by entrusting it with new large-scale IT systems, subject to the adoption of relevant legislative instruments. A The Agency has proved to effectively ensure the operational management of SIS, VIS and Eurodac as well as the new tasks entrusted to it.

As was underlined in the European Agenda on Security[265] common high standards of border management are essential to prevent cross-border crime and terrorism. The current eu-LISA Regulation contributes to achieving a high-level of internal security by enabling eu-LISA to operate SIS, VIS and Eurodac which are essential tools for the effective control and security of the external borders of the Union. The new proposal will also contribute to this objective by enabling the Agency to take on the development and operational management of new systems (EES, ETIAS and ECRIS-TCN) as well as other tasks which will effectively contribute to that end, subject to the adoption of the relevant legislative instruments.

Schengen evaluation and monitoring mechanism

Legal framework

The (new) evaluation mechanism is implemented according to the provisions of Council Regulation no. 1053/2013 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[266].

2. Analysis

After 15 years of implementation of the 1998 Decision of the Executive Committee, the Commission proposed an up-date of the Schengen Evaluation mechanism in order to improve the efficiency, accountability of the parties involved and transparency of the process. The Council has adopted this proposal after consultation of the European Parliament confirming the role of the European Parliament in the Schengen evaluation mechanism to increase democratic control.

The new rules allow for an effective, consistent and transparent application of the Schengen rules and regulations by the Schengen Member States, while at the same time maintaining a high level of mutual trust between those Member States. The Commission is given a central

[263] COM(2016)205 final.
[264] COM(2017) 261 final.
[265] COM(2015) 185 final, 28.4.2015.

[266] OJ L 295, 6.11.2013, p. 27.

role when it comes to monitoring and evaluation and, in close cooperation with experts from the Member States, has the competence to ensure that the Schengen rules will be respected.

The new evaluation rules mean a shift from the former intergovernmental system of peer review to an EU-based approach where the central coordinating role was given to the Commission, while keeping the peer review element. The new system also introduces a clause providing for unannounced visits and clearer rules for the follow-up to evaluations.

In addition to these improvements, the new evaluation process also includes measures aimed to assist Member States in fulfilling the recommendations adopted as part of the evaluation process.

Although the implementation of these support measures would normally be sufficient to deal with any problem that may occur, the new system also provides (via an amendment of the Schengen Borders Code) for the very exceptional situation where deficiencies in the management of the external border are still not adequately addressed: the new rules include the possibility for Member States to decide (based on a proposal from the Commission for a recommendation from the Council) on a prolonged reintroduction of controls in case of serious deficiencies in the external border management of an evaluated Member State which put at risk the overall functioning of the Schengen area.

The Member States and the Commission are jointly responsible for the implementation of the evaluation and monitoring mechanism, with the support of the Union bodies, offices and agencies involved in the implementation of the Schengen acquis. The Commission has an overall coordination role in establishing the annual and multiannual evaluation programmes, drafting questionnaires and establishing schedules of visits, conducting them and drafting evaluation reports and proposing recommendations. In addition, the Commission ensures that the follow-up and monitoring of the evaluation reports and recommendations are carried out appropriately.

The Member States and the Commission cooperate fully at all stages of the evaluation, especially through participation in the on-site teams, but also in the framework of the activities of the Committee for the implementation of the new evaluation mechanism - Schengen Committee (EU and associated Member states representatives), that assists the Commission in the process of implementing the new Schengen evaluation mechanism.

Under the new mechanism, a special attention is paid to the training of the Schengen evaluators (including on respect for fundamental rights), in close cooperation with the relevant European agencies. The experts participating in the evaluation must have solid theoretical knowledge and practical experience in the areas covered by the evaluation mechanism, along with a sound knowledge of the evaluation principle, procedure and techniques.

The strengthened mechanism covers all aspects of the Schengen acquis, including external borders, visa policy, the Schengen Information System, data protection, police cooperation, judicial cooperation in criminal matters, return as well as the absence of border control at the internal borders and the functioning of the authorities applying the relevant parts of the Schengen acquis. Respect of fundamental rights in the implementation of the Schengen acquis is covered within the scope of the evaluations. In addition, each year the European Border and Coast Guard Agency (EBCGA), the Fundamental Rights Agency (FRA) and Europol are invited by the Commission to provide a report risk analysis in accordance with their respective mandates, related to the Member States to be evaluated in the following year. The report is used for the planning of the evaluation missions and the unannounced visits in the Member States. These and other EU-Agencies also take an active part in the on-site visits with an observer.

The European Parliament started at the end of 2016 a new working group on "Schengen Scrutiny". The group is considering how Schengen can provide solutions to some of the

challenges currently faced by the EU. The Commission is invited to give oral briefings on the results of the Schengen evaluation mechanism to the working group on a regular basis, e.g. 2-3 times per year. To ensure confidentiality, these meetings take place in camera.

There have been neither any provisions nor actions directly related to the Schengen evaluation and monitoring mechanism outside the EU. However, in the framework of the on-site visits organised for the areas of external borders and police cooperation the on-site team assesses the level of cooperation between the evaluated Member States and the neighbouring third country at the EU external borders. In the same vein, the police cooperation components represented by the deployment of liaison officers in third countries, in particular those generating illegal migration flows and cross-border criminality, the exchange of information and intelligence and the overall cooperation framework, are evaluated by the on-site teams.

Union Customs Code (Regulation (EU) No 952/2013)

1. Legal framework

The legal basis for the development of a common framework for risk management of the supply chain was provided by the 'security amendment' of the Customs Code in 2005[267]. This followed two Commission Communications dealing with integrated management of the external borders[268] in direct response to the December 2001 Laeken European Council call for better management of the Union's external border controls.

The Communication on the role of customs in the integrated management of external borders refers explicitly to *"... threats to public security in the movement of goods (criminal, terrorist or other trafficking or illegal trade in firearms, biological products or explosives, for example), but also the threats to society's security from trade in goods which pose a risk to public health, the environment and consumers"*. Council conclusions in 2003[269] called for appropriate control tools and consideration of their financing including aspects of possible burden sharing and for special attention to strengthening the information exchange between all administrations or agencies and operators involved in international trade.

2. Analysis

The aim was to ensure an equivalent level of protection and minimise risks for the EU, its citizens and trading partners in relation to risks posed by cargo entering and leaving the EU. More specifically, to achieve effective security risk assessment and customs control of high-risk goods movements crossing EU external borders based upon commonly agreed standards and risk criteria. The approach was to be enabled by development of trans-European IT systems supporting pre-arrival/pre-departure security risk analysis based on cargo information submitted electronically by traders prior to arrival or departure of goods in/from the EU; the exchange of risk-related information among competent authorities; and the contribution of Authorised Economic Operators (AEO) in a customs-trade partnership to securing and facilitating international legitimate trade.

The security amendment required development of IT systems over a number of years with full implementation scheduled in 2011. A preliminary assessment of initial implementation made with Member States' customs authorities gave rise to a more in-depth study of EU risk analysis and targeting capabilities[270]. The study concluded that several issues required urgent action including data quality, supply chain modelling and certain aspects of the methodology

[267] Regulation (EC) No 648/2005 of the European Parliament and of the Council of 13 April 2005 and Commission Regulation (EC) No 1875/2006 of 18 December 2006.
[268] Communication on the integrated management of the external borders of the EU COM(2002) 233 final, 7.5.2002; Communication on the role of customs in the integrated management of external borders COM(2003) 452 final 25.7.2003.
[269] 13981/03 UD93 FIN 446 14 November 2003.
[270] Study on possible ways to enhance EU-level capabilities for customs risk analysis and targeting, PricewaterhouseCoopers, 31 May 2012.

applied. Evaluations made by the Commission and the Member States demonstrated the gaps and weaknesses identified as systemic. These include: poor quality data from trade; lack of systematic, real-time sharing or pooling of data and information among customs authorities and between customs and relevant authorities responsible for security matters; inadequate arrangements for risk mitigation; and unacceptable variance in capacities to implement common risk criteria. Crucially, under the current set-up, the risk assessment and control decision taken by the Member State of first entry may be taken in the absence of potentially critical information available to another Member State.

Subsequently, the Commission reviewed the implementation of customs risk management policy including identified gaps and weaknesses; put forward a strategic approach and made recommendations for action with a focus on efficient deployment of resources[271]. Following a Council request for a coherent strategy[272], the Commission in August 2014 published an "EU Strategy and Action Plan for customs risk management"[273] supported by a Cost-Benefit Analysis[274]. The Strategy and Action Plan seeks to ensure customs has the capacities to fulfil its security mission in cooperation with other law enforcement and security agencies and is part and parcel of the EU security agenda; it was endorsed by the Council in December 2014[275].

Actions involving customs would almost certainly have been undertaken in some Member States in light of the US decision post 9/11 to secure cargo entering the US. This US policy had direct consequences via new export control security requirements on container traffic from EU ports destined for the US. Nevertheless, this measure related to customs supervision of the Union's international trade led directly to positive EU-wide outcomes, notably: an IT system enabling the receipt of (limited) advance cargo information from trade sources by customs at first points of entry, the establishment of common risk criteria for security risk assessment by first points of entry, and the AEO programme; more systematic exchange of risk-related information via a dedicated electronic system connecting seaports, airports and external land frontier customs posts. EU funding through the customs programmes has provided added value in terms of the design and roll out of pan-European IT systems, enhanced capabilities through the leveraging and pooling of expertise via EU level networks, international cooperation and the EU-wide 'cultural' adaptation of customs authorities toward pro-active and systematic management of security and safety risks.

The main relevant programmes/initiatives are:

- the *European Agenda on Security*[276], which calls for measures to improve security in relation to movement of goods, to tackle illicit activities such as weapons, drugs, cigarettes trafficking via full exploitation of the Customs Advance Cargo Information System by ensuring sharing of information between the customs and other law enforcement authorities.
- *EU action plan against illicit trafficking in and use of firearms and explosives*[277], aimed to reinforce customs risk-based controls at the external border and calls for acceleration of all security-related actions foreseen in the EU Customs Risk Management Strategy and action plan.

[271] Communication on Customs Risk Management and Security of the Supply Chain COM (2012) 793, 8.1.2013
[272] Council Conclusions on Strengthening the Security of the Supply Chain and Customs Risk Management of 18 June 2013 (8761/3/13).
[273] COM (2014) 527, 21.8.2014 supported by Cost-Benefit Analysis carried out by PricewaterhouseCoopers
[274] The Cost-Benefit Analysis has been categorised "limited high" and has only been released to customs authorities for their internal administrative purposes.
[275] 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).
[276] C (2015) 185 final.
[277] COM(2015) 624 final.

- *Joint Framework on countering hybrid threats; a European Union response*[278], in relation to transport and supply chain security examining the ways how respond to hybrid threats, in particular those concerning transport critical infrastructure.
- *Stronger and Smarter Information Systems for Borders and Security*[279], where the Commission engages to explore synergies and convergence between information systems and their corresponding infrastructures for EU border management and for customs operations.
- *Enhancing security in a world of mobility: improved information exchange in the fight against terrorism and stronger external borders*[280], in developing the Security Union, the need to reinforce Europol by effective and timely information-sharing among relevant authorities (security and law enforcement authorities, including customs and border guards where relevant) as a vital prerequisite for successful action against terrorism and serious crime.
- *European Union Maritime Security Strategy and its Action plan*[281], where the Council calls to explore novel information-based risk analysis techniques as well as data sources currently not exploited and to improve the common pre-arrival security risk assessment for the movement of goods through the global supply chain.

As to fundamental rights, the Union Customs Code is in conformity with the Charter of Fundamental Rights of the EU in particular with a view to the right of appeal and the right to be heard.[282]

On the external dimension, cooperation with international trading partners on supply chain security has progressed in particular through mutual recognition agreements on trusted trader programmes with the US, China and Japan as well as with Norway and Switzerland which also cover harmonised customs security measures.

The EU Strategy and Action plan for customs risk management addresses current deficiencies in particular through a wholesale transformation of information systems for customs risk management in the EU. While the Union Customs Code has provided the necessary legal basis, the reform of the Advance Cargo Information System (ICS 2) is at the centre of the operational efforts.

An effective framework and capacity for the EU to systematically address supply chain security risks is integral to the European Agenda on Security objectives of tackling terrorism and disrupting organised crime. While this reform programme responds comprehensively to the system weaknesses identified, which significantly affect customs' ability to fulfil its security role and properly integrate its contribution to broader EU security needs, resource constraints at EU and national levels are severely hampering timely implementation.

In its December 2016 Conclusions on the progress report on the implementation of the EU Strategy and Action Plan [283] the Council underlined that the development of appropriate IT systems is crucial to ensure the availability and sharing of supply chain data and risk-relevant

[278] JOIN(2016) 18 final.
[279] COM(2016) 205 final.
[280] COM(2016) 602 final.
[281] 11205/14, 24.6.2014, 17002/14, 16.12.2014.
[282] Recital 27 of the Union Customs Code.
[283] Progress Report on the implementation of the EU Strategy and Action Plan for customs risk management (11415/16 + ADD 1) and Council Conclusions on the Progress Report of 6 December 2016 (14894/16).

information and that timely funding is essential. The need to ensure adequate resourcing for ICS 2 should therefore be addressed as a top priority.[284]

European Border Surveillance System (Eurosur)

1. Legal framework

The Regulation (EU) 1052/2013 of the European Parliament and of the Council of 22 October 2013 establishing the European Border Surveillance System (Eurosur)[285] is based on Article 77(2)(d) of the TFEU), according to which the European Parliament and the Council, acting in accordance with the ordinary legislative procedure, shall adopt measures concerning any measure necessary for the gradual establishment of an integrated management system for external borders.

The establishment of EUROSUR forms part of a policy aimed at reinforcing the management of the external borders of the Member States through a specific policy instrument which streamlines cooperation and enable systematic information exchange between Member States as well as with the Agency on border surveillance.

2. Analysis

Eurosur provides a common framework for the exchange of information and for the cooperation between Member States and the European Border and Coast Guard Agency in order to improve situational awareness and to increase reaction capability at the external borders for the purpose of

- detecting, preventing and combating illegal immigration;
- detecting, preventing and combating cross-border crime and;
- contributing to ensuring the protection and saving the lives of migrants.

The Eurosur regulation precisely defines the scope of the framework both in terms of areas and actions covered and the different components of the framework both at national and European level including the role of the Agency.

This Regulation applies to the surveillance of external land and sea borders, including the monitoring, detection, identification, tracking, prevention and interception of unauthorised border crossings. For this purpose, all Member States have established *national coordination centres*, which are connected to the classified *Eurosur communication network*. These centres maintain the *national situational pictures*, which contain

- incident reports on illegal immigration, **cross-border crime** and SAR incidents of migrants;
- information on the position and status of their patrolling assets and
- risk analysis and intelligence reports.

These centres feed parts of this information into the similarly structured *European Situational Picture* maintained by European Border and Coast Guard Agency. The agency also maintains the *Common Pre-frontier Intelligence Picture*, which is fed with information collected via the *Eurosur Fusion Services* (using e.g. satellite imagery, ship reporting systems, surveillance planes and soon RPAS).

[284] About €17m is currently earmarked for the development of ICS2. A 2015 estimate indicated development of the full project could cost up to 10 times the present budget in capital expenditure.

[285] OJ L 295/11 of 6.11.2013. There is a call for evaluating the Regulation in 2017, paying particular attention to the results achieved against the objectives set, the continuing validity of the underlying rationale, the application of this Regulation in the Member States and by the Agency and the compliance with and impact on fundamental rights. A cost benefit evaluation will also be included.

The Eurosur Regulation may also apply to checks at border crossing points if Member States voluntarily provide such information to Eurosur. About 50% of the Member States use Eurosur for border checks, reporting incidents not only on irregular migrants, but also on **smuggling of contraband and other illicit goods**.

Making Eurosur mandatory for border checks is requested by some Member States. It would allow Member States and the European Border and Coast Guard Agency to have a more complete picture at national and EU level not only with regard to illegal immigration, but also with regard to **cross-border crime**.

However, a careful analysis needs to be carried out on the current role of the national coordination centres in each Member State and their evolution and on the information already contained in the national situational pictures and their possible evolution with regards to further information available in other databases in SIS, SIRENE, VIS, Eurodac, EES and ETIAS.

Eurosur has considerably improved the *situational awareness* of the Member States at the external borders and in the pre-frontier area: For example, European Border and Coast Guard Agency – using the Eurosur Fusion Services – is detecting 80-90% of the departures of migrant vessels still on the Turkish coast and the vast majority of migrant vessels close to the Libyan coast. The combined use of these Eurosur components allows to regularly detect and intercept vessels smuggling not only migrants, but also **arms and contraband**.

- Use of Eurosur by military actors: European Border and Coast Guard Agency is regularly sharing detections made by the *Eurosur Fusion Services* with the military CSDP operation EUNAVFOR Med Sophia.
- Use of Eurosur by law enforcement actors: European Border and Coast Guard Agency is supporting Europol's JOT MARE via the Eurosur Fusion Services. Member States' border guard authorities share information from Eurosur (e.g. incident reports) with other law enforcement authorities via the national coordination centres.
- Use of Eurosur by Member States' authorities carrying coast guard functions: European Border and Coast Guard Agency, EMSA and EFCA are currently interlinking their information systems, capabilities and operations not only for the benefit of border surveillance (which was already done under Eurosur), but also other coast guard functions' activities, such as fisheries control (in line with Article 53 of the EBCG Regulation and the corresponding amendments of the EMSA and EFCA mandates).
- European Border and Coast Guard Agency is using the Copernicus programme for co-funding the Eurosur Fusion Services.
- Support to the policy implementation in the field of European border surveillance has also been provided by the security research programme, in both Framework Programme 7 and Horizon 2020. Projects such as PERSEUS "Protection of European seas and borders through the intelligent use of surveillance", CLOSEYE "Collaborative evaLuation Of border Surveillance technologies in maritime Environment bY pre-operational validation of innovativE solutions" or RANGER "RANGER: RAdars for loNG distance maritime surveillancE and SaR opeRations" are directly linked to EUROSUR and the EU Maritime Security Strategy Action Plan. The excellent exploitation of synergies in this field is underlined by the award decision of a grant of the Commission under ISF to Spain and Portugal to support the improvement of border surveillance by enhancing cooperation in the framework of EUROSUR based on a proposal that follows CLOSEYE.

The Eurosur Regulation and Handbook contain provisions aiming at a full respect of the fundamental rights and principles set out in the Charter of Fundamental Rights of the European Union, including the protection of personal data, as well as the non-refoulment principle.

Member States ensure via their national coordination centres the information flow between Eurosur (which is strictly limited to Member States) and the regional cooperation networks established with neighbouring third countries in the Baltic Sea[286], the Black Sea[287] and the Western Med[288], exchanging information also on **cross-border crime** incidents. A similar network for the Central and Eastern Med[289] should become operational in 2017.

Directive 2014/41/EU of the European Parliament and of the Council of 3 April 2014 regarding the European Investigation Order in Criminal Matters

1. Legal framework

Directive 2014/41/EU of the European Parliament and of the Council of 3 April 2014 regarding the European Investigation Order in Criminal Matters was adopted on the basis of Article 82(1) of the TFEU, following an initiative presented by 7 Member States.

It followed on the call for a comprehensive system for obtaining evidence in the Stockholm Programme adopted by the European Council of 10-11 December 2009.

2. Analysis

The general objective[290] of the Directive was to improve the search for truth in criminal proceedings with a transnational aspect. More specifically, it aims at:

1. Accelerating the procedure: resolving rapidly criminal cases is a key element for both the efficiency and the quality of the system.

- specific deadlines applicable to all types of measures;
- general principle according to which the investigative measure should be carried out in the executing Member States with the same celerity and priority as for a similar national case ("assimilation principle").

2. Ensuring the admissibility of evidence: evidence can merely be useful as part of a case if it is admissible in court.

- the executing authority shall comply with the formalities and procedures expressly indicated by the issuing authority unless otherwise provided in this Directive and provided that such formalities and procedures are not contrary to the fundamental principles of law of the executing State.

3. Simplifying the procedure.

- one single instrument replacing the fragmented regime (judicial authorities had to use two different regimes: mutual legal assistance and mutual recognition);
- flexibility in the execution of the measure.

4. Maintaining a high level of protection of fundamental rights, especially procedural rights.

5. Reducing the financial costs.

- results from the facilitation and acceleration of the procedures.

6. Increasing mutual trust and cooperation between the Member States.

- increased and more automatic cooperation while maintaining direct contacts.

[286] BSRBCC – Baltic Sea Region Border Control Cooperation.
[287] Black Sea Coast/Border Guard Cooperation Forum (BSCF) and Black Sea Border Coordination and Information Centre (BSBCIC).
[288] Seahorse Atlantic network.
[289] Seahorse Mediterranean network.
[290] http://register.consilium.europa.eu/doc/srv?l=EN&f=ST%209288%202010%20ADD%202.

At this stage it would be premature to assess how the Directive meets the current needs as it has not yet been transposed by all Member States[291]. However, in the framework of the implementation of the Council Conclusions of 9 June 2016 on Improving Criminal Justice in Cyberspace, one of the strands the Commission is working is finding ways to secure and obtain electronic evidence more quickly and effectively by streamlining the use of mutual legal assistance proceedings and where applicable, mutual recognition in the context of the European Investigation Order. [292]

The Directive simplifies the procedure by eliminating the coexistence of two different regimes in order to obtain evidence across internal EU-borders: on the one hand mutual legal assistance and on the other hand mutual recognition. This inconsistency is a result of the limited scope of the Framework Decisions 2003/577/JHA and 2008/978/JHA. Although these instruments introduce the principle of mutual recognition in the field of evidence, they are criticised because their restricted range of application actually complicates the international cooperation, instead of simplifying it, for example, separate requests had to be sent for different types of investigative measures requested in the same criminal proceedings (with different rules applicable and different competent authorities). Given the absence of the obligation to apply instruments of mutual recognition, instruments of mutual legal assistance were mainly used by the practitioners.

Simplification of the legal framework leads to a better administration of justice and reinforces mutual trust and cooperation.

The Directive ensures a high level of protection of fundamental rights– the issuing authorities must assess the necessity and proportionality of the investigative measure requested; a EIO has to be issued or validated by a judicial authority; the issuing of an EIO may be requested by a suspected or accused person, or by a lawyer on his/her behalf; Member States must ensure that interested parties are entitled to legal remedies equivalent to those available in a similar domestic case and that they are properly informed of these possibilities; execution of the EIO might be refused if the EIO would be incompatible with the executing State's obligations in accordance with Article 6 TEU and the Charter.

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

1. Legal framework

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.[293]

The adoption of the Regulation followed the reoccurring fatalities in the Mediterranean and the need to address the differences of interpretation of applicable rules under Union law and international maritime law as regards to disembarkation of migrants intercepted or rescued at

[291] The Directive was adopted on 3 April 2014 and has to be transposed by 22 May 2017. DK and IE are not participating in the EIO. So far, only FR, DE and RO communicated national transposition measures.
[292] The Commission is requested to consider and make recommendations on how to adapt, where appropriate, existing standardised forms and procedures to request the securing and obtaining of e-evidence, and to develop a secure platform for online exchange between judicial authorities of e-evidence.
[293] OJ L 189 of 27.6.2014 p.93.

high sea during border surveillance operations coordinated by the European Border and Coast Guard Agency.

2. Analysis

The objective of the Regulation is to ensure the efficient monitoring of the crossing of external borders including through border surveillance, while contributing to ensuring the protection and saving of lives by setting out binding rules applicable border surveillance operations carried out by Member States at their 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 (European Border and Coast Guard Agency [294]).

The binding rules set out by the Regulation are to be applied during any maritime operations coordinated by the European Border and Coast Guard Agency with regard to detection and interception of irregular migrants at sea as well as to search and rescue situations and disembarkation of people intercepted or rescued.

Application of those rules contribute to addressing migratory challenges and potential future threats at the external borders, thereby contributing to addressing serious crime with a cross-border dimension and ensuring a high level of internal security within the Union.

The external maritime borders of the EU, notably in the Mediterranean have been under steady and heavy irregular migratory pressure since 2011. Consequently the Agency has been coordinating quasi permanent joint operations to stem the flows (.e.g. JO Triton hosted by Italy and JO Poseidon hosted by Greece).

The rules set out by the Regulation are reflected in the operational plan for each and every maritime joint operations.

The rules set out by the Regulation meet the current needs and their added value is shown by broad participation of Member States in such operations.

One of the obstacles for engaging Member States in participation in maritime joint operations hosted by other Member States was the lack of agreement regarding the applicable rules for interception, and even more pertinently, for disembarkation of the migrants intercepted or rescued, due to different interpretation of applicable provisions of international maritime law.

Based on this Regulation, drawing up an operational plan no longer require finding a compromise between the host and participating Member States as regards the right of intervention on another Member States' territorial water or contiguous zone and the place of disembarkation.

Another incentive for Member States participation is the fact that the cost of deployment of assets and crew is reimbursed by the Agency (but this is not deriving from the provisions of the Regulation.

Chapter II (General Rules) of the Regulation sets out extensive provisions about protection of fundamental rights and the principle of non-refoulement.

The Regulation does not concern directly the external dimension of internal security of the EU or its Member States. However, given the new mandate of the Agency which may provide for joint operations being carried out on the territory of neighbouring third country and deployment of EBCG teams and assets for those operations with their consent, application of the rules set out by the Regulation may, in principle, also be agreed with the third countries concerned.

[294] The Agency was renamed as European Border and Coast Guard Agent by Regulation (EU) 2016/1624, - OJ L 251 of 16.9.2016 p.1.

Document security

1. Legal framework

Passports, residence permits or visas are used for travel purposes or as a proof of identity. To improve the security of these documents, there are rules at EU level on their advanced security features and biometrics (facial image and fingerprints). This set of measures helps to fight against the falsification and counterfeiting of travel documents, while biometric identifiers establish a reliable link between the document and its holder. Security standards for travel documents and border control requirements are set at EU level, but Member States retain full responsibility for the breeder documents and actually producing and issuing travel documents.

With regard to passports, their format is still a matter of national competence of Member States and has been "harmonised" by legally non-binding Resolutions of Member States meeting within the Council i.e. outside the EU legislative framework[295]. The security features of passports and travel documents of Member States have been harmonised by EU law. Minimum standards for security features and biometrics have been set out in 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.[296]

With regard to residence permits, the EU has also established a uniform format for non-EU nationals' residence permits, which is used by all EU States as well as by Iceland, Norway, Switzerland and Lichtenstein. These residence permits are issued as stand-alone documents and include the same biometric features as the EU passports. A residence card of a family member of a Union citizen is issued to non-EU national family members of an EU citizen who is exercising his/her right to free movement. A uniform format for residence permits for third country nationals was established by Council Regulation (EC) No 1030/2002 of 13 June 2002 laying down a uniform format for residence permits for third-country nationals.[297] The regulation is currently being revised following a proposed made by the Commission in 2016.[298.]

All EU States as well as Iceland, Norway, Switzerland and Lichtenstein also use a uniform format for visas. However, the visa holder's biometric identifiers are not be stored in the visa sticker itself, but in a database (Visa Information System). A uniform format for visas has been established by Council Regulation (EC) No 1683/95 of 29 May 1995 laying down a uniform format for visas[299]. The regulation is currently being revised following a proposed made by the Commission in 2015.[300]

With regard to exchange of information, Council Decision 2000/261/JHA on the improved exchange of information to combat counterfeit travel documents was adopted on 27 March 2000. Howev it is no longer used by Member States and superseded.

---

[295] Resolution of the Representatives of the Governments of the Member States of the European Communities, meeting within the Council of 23 June 1981 (OJ C 241, 19.9.1981, p. 1–7); supplemented by Resolution of the representatives of the Governments of the Member States, meeting within the Council of 8 June 2004 to the resolutions of 23 June 1981, 30 June 1982, 14 July 1986 and 10 July 1995 concerning the introduction of a passport of uniform pattern, (Council document 10038/1/04, REV 13 June 2004).

[296] OJ L 385, 29.12.2004, p. 1–6; Amended by Regulation (EC) No 444/2009 of the European Parliament and of the Council of 28 May 2009 amending Council Regulation (EC) No 2252/2004 on standards for security features and biometrics in passports and travel documents issued by Member States (Official Journal L 142, 06/06/2009 p. 1 - 4).

[297] OJ L 157, 15.6.2002, p. 41–42.

[298] Proposal for a Regulation of the European Parliament and of the Council amending Council Regulation (EC) No 1030/2002 laying down a uniform format for residence permits for third-country nationals, COM(2016) 434 final.

[299] OJ L 164, 14.7.1995, p. 1 – 4.

[300] Proposal for a Regulation of the European Parliament and of the Council amending Regulation (EC) No 1683/1995 of 29 May 1995 laying down a uniform format for visas -COM(2015) 303 final/2.

An Action plan to strengthen the European response to travel document fraud[301] was adopted by the Commission in December 2016 with a report required for 1st quarter of 2018.

All Regulations above are supplemented by Commission Implementing decisions regarding the common technical specifications. However, all annexes of decisions are classified as EU Secret, because of its sensitivity of information.

2. Analysis

All instruments listed above ensure that all European travel documents correspond to a high security level protecting against fraud. The technical specifications are regularly updated and modernised to counter the activities of fraudsters and to be ahead of their fraudulent activities.

Currently, the work on document security is guided by the Action Plan of 2016 looks at concepts and processes to manage identity, identifies actions to close potential loopholes and proposes measures for the Commission, the Council and the European Parliament, but also for Member States action under national policies on all aspects of travel document security.The recommendations are grouped in four key areas of the Identity infrastructure: 1. Registration of identity, 2. Issuance of documents, 3. Document production (security features in travel documents, enrolment of biometrics), and 4. Document control (electronic checks on non-EU nationals' travel documents, database checks, training, tools, and biometrics in travel documents).

On 27 March 2017 the Council adopted Conclusions focusing on certain key elements of the Action Plan. It underlined the importance of more secure breeder documents and the need for an overhaul of FADO database on false and authentic documents, including a change of its legal basis. The Commission is monitoring the implementing of the Action Plan.

The harmonisation of security of European travel documents and the format of the visa and residence permit eases border controls. Border guards do no longer have to know 31 different documents with varying security features but can focus on a uniform format, recognisable at first sight and with common security features and biometrics.

The protection of the personal data and biometrics stored on a contactless chip in passports and residence permits for third country nationals is of a very high standard. A judgment of the ECJ[302] confirmed that these requirements were not infringing fundamental rights.

The security of travel documents has to be of a very high standard. In order to ensure global interoperability, ICAO recommendations have been rendered mandatory by the above EU law. This ensures a facilitated control and establishment of the identity of the holder when crossing the external borders.

The role of the European Border and Coast Guard Agency in the field of internal security

1. Legal framework

Regulation (EU) 2016/1624 of the European Parliament and of the Council of 14 September 2016 on the European Border and Coast Guard and amending Regulation (EU) 2016/399 of the European Parliament and of the Council and repealing Regulation (EC) No 863/2007 of the European Parliament and of the Council, Council Regulation (EC) No 2007/2004 and Council Decision 2005/267/EC[303].

2. Analysis

[301] Commission Communication on an Action plan to strengthen the European response to travel document fraud (COM (2016) 790 final).
[302] Case C 291/12.
[303] http://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1482146473208&uri=CELEX:32016R1624.

The Regulation is aimed to develop and implement European integrated border management at national and Union level, which is a necessary corollary to the free movement of persons within the Union and is a fundamental component of an area of freedom, security and justice. European integrated border management is central to improving migration management. The aim is to manage the crossing of the external borders efficiently and address migratory challenges and potential future threats at those borders, thereby contributing to addressing serious crime with a cross-border dimension and ensuring a high level of internal security within the Union. At the same time, it is necessary to act in full respect of fundamental rights and in a manner that safeguards the free movement of persons within the Union.

The Regulation which has entered into force on 6 October 2016 constitutes a further development of the Schengen acquis regarding control on persons at the external borders. It defines for the first time in binding Union law the core elements of European integrated border management, including notably border control, including measures to facilitate legitimate border crossings and, where appropriate, measures related to the prevention and detection of cross-border crime; inter-agency cooperation among the national authorities in each Member State which are responsible for border control or for other tasks carried out at the border; cooperation with third countries in the areas covered by the Regulation; technical and operational measures within the Schengen area which are related to border control and designed to address illegal immigration and to counter cross-border crime better.

The implementation of the Regulation has just started thus it would be premature to assess its impact on the cooperation among Member States in relation to internal security.

The Regulation leaves no doubt that whilst implementation of the European integrated border management as a shared responsibility of the Member States and the European Border and Coast Guard Agency contributes to ensuring a high level of internal security these provisions and the role of the European Border and Coast Guard Agency shall not interfere with the measures adopted at EU level in relation to judicial cooperation in criminal matters and police cooperation.

In respect in particular to the role of Europol and Eurojust: in accordance with Art. 8(m) of the Regulation, European Border and Coast Guard Agency shall cooperate with them, within the respective mandates of the agencies concerned, and provide support to Member States in circumstances requiring increased technical and operational assistance at the external borders in the fight against organised cross-border crime and terrorism.

The Regulation includes a number of Articles aimed at safeguarding the respect of fundamental rights in the context of its implementation, including general provisions on protection of fundamental rights and a fundamental rights strategy, provisions on civil and criminal liability, provisions on a consultative forum, on a fundamental rights officer and on a complaints mechanism.

The Regulation provides for rules on cooperation with third countries and international organisations in matters covered by the Regulation. The establishment of cooperation with third countries shall serve to promote European border management standards which are based on full respect of fundamental rights.

Targeted amendment to the Schengen Borders Code to introduce systematic checks against relevant databases for all persons including EU citizens at the external borders

1. Legal framework

Regulation (EU) 2017/458 amending Regulation 2016/399 of the European Parliament and of the Council of 9 March 2016 on a Union Code on the rules governing the movement of persons across borders (Schengen Borders Code)[304][305].

The new rules adopted by the European Parliament and the Council on 7 March, and which entered into force on 7 April 2017, aim at strengthening the management of the EU external borders, on the basis of a Commission proposal presented as a direct response to the attacks in Paris in November 2015 and the growing threat from foreign terrorist fighters (FTF).

2. Analysis

The overall objective of the amendments is to increase security in the EU by reinforcing checks at the external borders by introducing the following changes:

- Removing limitations concerning the consultation of relevant databases with regard to EU citizens at the external borders; (until now only Interpol Stolen and Lost travel Documents Database could be consulted systematically with regard to EU citizens whereas SIS and other EU databases could be checked only on a targeted basis). This amendment will help to apprehend at exit and re-entry into the EU persons subjects to an alert, including foreign terrorist fighters. Thus it will contribute to increasing security in the EU.
- Making the obligation to systematically consult relevant databases with regard to third country nationals upon exit more explicit.
- Aligning the databases to be consulted with regard to the third country nationals, EU citizens and persons benefiting from the freedom of movement under Union law.

The EU is facing an unprecedented level of terrorist threat. New terrorist attacks are likely, as foreign terrorist fighters are expected to return from conflict zones. Comprehensive border controls at the external borders are instrumental in apprehending such persons and thus preventing possible attacks.

Under previous rules, the consultation of data bases on the basis of common risk indicators focused on foreign terrorist fighters was making it possible for persons for whom an alert has been issued to nevertheless cross the border unnoticed.

Not all Member States have faced terrorist attacks on their soil, yet terrorism is a common threat to all which in the absence of controls at internal borders may spread to different Member States. The travelling routes of FTF take into account the varying sensitivity to terrorism threats among the Member States. Therefore, it is in the interest of all Member States that the controls at EU external borders are carried out according to identical high standards.

Making mandatory for all Member States to check EU citizens at the external borders systematically against relevant databases, and third country nationals also upon exit, should increase the trust between the Member States and this should support cooperation among them.

In the process of preparation for the new rules the Member States increased the number of abc gates at the airports. The increased number of abc gates and increased use of API data allowed some of the biggest airports in Europe to comply with the new rules without the need of requesting a temporary derogation from the principle.

More importantly, the obligation to consult SIS in all instances gave a boost to the use of this European database. According to the information from some Member States since the entry into force of the new rules the number of standard queries has increased.

The main characteristics of the new rules are as follows:

[304] http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0399&from=EN.
[305] http://data.consilium.europa.eu/doc/document/PE-55-2016-INIT/en/pdf

- Systematic checks of the relevant databases enable synergies in the architecture of the systems which until recently were not possible due to the asymmetry between possible systematic checks on documents and non-systematic checks for security reasons with regard to EU citizens.
- Systematic checks boosted the deployment of e-gates and the use of API data.
- The new rules remain consistent with the freedom of movement as guaranteed by the Treaty and as further detailed in Directive 2004/38/EC.
- The new rules take into account the need to assure fluidity of the traffic. To this end derogations are allowed at land and sea borders, as long as the level of security remains unhampered. Moreover, a transitional period of 6 months has been proposed for the air borders with a view to allow enough time for any possible adaptations (investments in equipment, staff, etc.). Only in exceptional situations, this transitional period could be prolonged at certain airports up to 18 months, subject to the assessment by the Commission on a case by case basis. The expenses for the necessary adaptations are eligible for financial support from the EU funds (ISF-B).
- The Commission will evaluate the use of the new rules by 8 April 2019.

The amendment fully respects the fundamental rights and principles set out in the Charter of Fundamental Rights of the European Union, the right to respect of private and family life (Article 7), the protection of personal data (Article 8) and the freedom of movement and residence (Article 45). The safeguards in this regard provided by Article 4 of the Schengen Borders Code continue to apply. It might be underlined that consultations of databases are carried out on a hit/no hit basis.

VI. Workshops

1. European Political Strategy Centre (EPSC) High-Level Seminar on "The Security Union. State of Play and Future Perspectives"

The High-Level Seminar on "The Security Union. State of Play and Future Perspectives" organised by EPSC in collaboration with the European Commission, was held on 3 April 2017, in Brussels.

The purpose of the Seminar was to facilitate an open discussion between think tanks, senior Commission officials and Commissioner King on current progress towards a Security Union and on future needs and opportunities.

Main takeaways

- With the removal of internal borders between Member States, external border protection in those Member States sharing a border with third countries as well as internal security became an European interest. An efficient and reliable border management is an indispensable prerequisite for the Security Union.
- Security is a shared competence between the EU and its Member States. In as much as Art. 4 (2) TEU refers only to "national security", the EU has to meet its duty to protect "Schengen security" and with due respect for the principle of subsidiarity and the rule of law to deliver on aspects of cross border security.
- Information and mutual trust are key elements of the Security Union. Whereas national security remains the responsibility of each Member State, the EU has to ensure collective security by bringing in a European picture on security. A genuine Security Union therefore is about "connecting the dots". It requires sharing and pooling of relevant information as well as breaking down borders in intelligence and law enforcement cooperation.
- Taking into account the principle of subsidiarity this does not imply a shift of competences in this sense, that – for example – Europol should be developed into a European kind of FBI. It does rather imply the establishment of a network of European institutions and competent authorities of Member States, coordinated by an European platform.

Conclusions of the discussion

Without denying deficiencies and the need to further improve internal security, many participants acknowledged the achievements already made on European level in certain policy fields. Apart from this, in a more holistic perspective, the lack of a definition of the Security Union was criticised by several experts ("just labelling"): what is the Security Union, who is in charge and which institutions should be involved? The need for a vision or long-term strategy was noted. In this regard, a lack of communication of achievements throughout the last years and the concept of Security Union became obvious.

Implementation was considered to be key to follow up on the policy initiatives on European level. Implementation of the EBCG and hotspots were brought as an examples as well as the transposition of the NIS Directive.

Emphasis was put on the need to, in a second step, better communicate the progress made. Particularly "practitioners on the ground" should be targeted more efficiently, for they often do not know about the practical initiatives and contact points. But also the general public needs to receive explanations on the things that do not work or seem not to work – a lack of communication in this regard will inevitably lead to the erosion of trust into the Union's capability to provide security.

Cooperation among all actors will be crucial in all policy fields in order to succeed. This concerns closer cooperation between Member States and the EU, built on mutual trust and, in

this regard, requiring an effort by some to scale up capabilities; but also collaboration and information exchange across silos concerning all law enforcement authorities and security institutions on every level.

Information was seen as a key by some: if European institutions (the positive example of Europol was mentioned) can provide law enforcement authorities in the Member States with helpful information; this will attract interest, create trust and by this start a dynamic towards closer cooperation.

Last but not least, experts called on closer cooperation with the private sector and promoted further public private partnerships..

2. High-Level Brainstorming to assess EU Counterterrorism Policies

An event with Member States hosted by the European Counter Terrorism Coordinator took place in the framework of the comprehensive assessment of EU security policy on 10 April 2017, in Brussels.

The objective was to hold an informal, high level, strategic discussion about key aspects of the EU's counter-terrorism policies, initiatives and instruments, what works, what does not work, what is particularly important and useful to Member States as well as the future threat picture and the potential direction of future EU counter-terrorism action in support of Member States.

The event was structured around four main themes: 1. Prevention of radicalisation, including external aspects, 2. Information sharing environment, 3. Operational cooperation, including Europol, Eurojust, European Border and Coast Guard Agency, CEPOL and external aspects, 4. Critical infrastructure protection and soft targets.

Main takeaways

- There was no indication of issues or areas where the EU should stop working or abandon ongoing activities;
- The expectations are for doing more, being better organised and to maximise the use of the available resources;
- There is a huge appetite for more work on prevent, both inside and outside the EU, synergies between existing tools are needed, RAN has the potential to be further developed, enhance information exchange on counter-narratives among Member States;
- On information sharing: focus on collecting more and better data, pool analytical capabilities, improve training and across sector work;
- On soft targets: Member States have to organise more exercises to train the population, closer involvement of the private sector is needed, Europol’s platform about malicious software could be replicated on other matters.

Overview of sessions

1. Prevention of radicalisation, including external aspects

Participants emphasised the role of ideology and hence the importance of analysis and research in this area. The nexus between organised crime, radicalisation in prisons and terrorist groups was pointed out. Also radicalisation over the internet was identified as a major source. Therefore, closer work with internet companies is needed.

RAN as a Centre of Excellence could support the identification of early signs of radicalisation and help to build resilience to social factors influencing radicalisation such as social exclusion, educational disadvantage etc. Closer work on prevention with intelligence community and judiciary is needed.

The issue of returnees represents a concern, particularly as people without strong academic background are recruited to work in refugee and migration centres and might miss signs of radicalisation.

On external aspects, Counter Terrorism (CT) attachés have to be more involved, they have to inform Member States and not only the EU institutions. Actions must be better coordinated. Participants welcomed more Counter Violent Extremism (CVE) engagement in the EU's neighbourhood and insisted on better integration of CVE-relevant policies.

2. Information sharing environment

It was stressed that the quality of data is as important as quantity. Hence, criteria in order to prioritise information and to be able to deal with a tremendous amount of data are needed. Links should be created between finance, migration, customs, police authorities and data, and silos removed.

Participants agreed that procedures must be kept as simple as possible as otherwise possibilities would not be pursued. Although intelligence services are not seen as a European competence, the role of the EU could be strengthened in this regard. Developing capabilities of and trainings for analysts could be an option for further enhancement. The need for a "common language" on this issue was acknowledged. Concretely, a new peer evaluation was suggested on counter-terrorism policies, comparable to an exercise which took place after 11 September 2001.

Further recommendations included the enhanced used of IntCen by Member States and stronger EU support in the collection of evidence in third countries. One specific issue concerns the access to and collection of battlefield evidence. The question was raised whether an EU model for agreement on extradition and Mutual Legal Assistance was needed. On a final note, law enforcement's access to EURODAC was identified as a problem.

3. Operational cooperation

It was commonly agreed that in the digital field, it is in the interest of both EU and its Member States to bring resources together. Europol should be more active on new areas (cyber) but this will have consequences on resources. The agency should be allowed to recruit teams more qualified on cyber, with an appropriate academic background. There was a consensus on Europol as a centre of excellence.

The European Border and Coast Guard Agency acts as an instrumental platform, but is not being used sufficiently. Identity management is weak, but the link with Europol is a success. Border crossing information could be used for law enforcement, such as information from interviews with migrants/asylum seekers at the borders.

Agencies should have more links with IntCen. The allocation of resources has to been balanced between police and other actors. However, the question of how much more proactive the EU wants to be was raised

4. Critical infrastructures protection and soft targets

There was a consensus for the need for Member States to organise more exercises on crisis response also in third countries and that the private sector should be stronger involved in the protection of critical infrastructures and soft targets. More technological tools should be used to protect soft targets. Europol’s platform about malicious software could be replicated on other matters and Security related research could be enhanced.

3. Europol workshop on "EU Security Policy"

On 19 April 2017, took place a joint workshop of Europol and the Commission on EU Security Policy in the framework of the comprehensive assessment of EU Security Policy.

The purpose was to facilitate an open discussion with Member States' experts on the effectiveness of the operational cooperation in fighting serious and organised crime and to identify what could be done in political-strategic and legislative terms at EU level to improve it further. Specific case studies were presented on cooperation in combating illicit trafficking of firearms, asset recovery and cybercrime.

Participants were senior police or policy officers and executives mostly from Member States' Interior Ministries, Police or Security Service. JHA Agencies (Cepol, EMCDDA, eu-LISA and FRA) were represented, as well representatives from the Commission , Counter Terrorism Coordinator's office and the Council secretariat.

Horizontal takeaways

- Calls for implementing well existing legislation rather than adoption of new one.
- Calls for more cooperation and exchange of experiences among Member States and with agencies (possible twinning, training, exchange of experts, JITs).
- Pooling of resources and building centres of excellence and expertise especially on cyber – in Europol.
- Specialised training for prosecutors and judges – especially on cyber.
- Integrated response with other services – notably customs, FIUs.
- Continue capacity building in the EU (e.g. firearms), ensure cooperation with third countries, ensure interoperability of different databases.

Overview of conclusions per session

Panel 1 - Organised crime

Background: Serious and organised cross-border crime is finding new avenues to operate and new ways to escape detection. One of the key priorities in the Security Agenda is to disrupt organised criminal networks by stepping up cross border investigations with the support of EU agencies. This cooperation however also relies on legal instruments developed at EU level in the past and it is necessary to assess their relevance in today's security context. As a result, these are the EU measures on which the present assessment puts particular focus: Council Framework Decision 2008/841/JHA of 24 October 2008 on the fight against organised crime

Summary of the discussion: Participants demanded not to engage in legislative changes to further extend the definition of organised crime. Several speakers supported the idea of trying to get some parallelism with what has been done in recent years on terrorism in order to get a better grip on organised crime. Many difficulties were noted in tackling organised crime group directly, in most cases there is still a commodity approach which does not show the necessary links across commodities. Participants acknowledged the availability of different tools, but insisted that more should be done on JITs and the procedure used to ask for cooperation. The demand was not for more legislation but an educational approach. The importance of data and evidence-based policy making was acknowledged, the only comprehensive view was seen in the field of drugs. It was called for risk analysis and better links to customs, namely a better cooperation with customs authorities. Interagency cooperation should be examined together with Europol and Eurojust. A more dynamic definition of offences, different forms of patterns (particularly financial patterns) and activities of influence should be assessed. Positive experience with the exchange of information via Europol was pointed out and the steady increase of incoming information allowed making the link and making it clear to the local prosecutor that the case concerns organised crime groups. Also the importance of international aspects was discussed.

Panel 2 - Asset Recovery

Background: The primary goal of organised crime is profit. Law enforcement must therefore have the capacity to turn the spotlight on the finance of organised crime, often inherently linked to corruption, fraud, counterfeiting and smuggling. International criminal networks use legal business structures to conceal the source of their profits, so action is needed to address the infiltration of the ilicit economy by organised crime. The infiltration of organised crime in the economy should be countered by a confiscation policy based on effective national systems and on cooperation between Member States. The ability to confiscate criminal assets depends directly on the ability to identify and trace them. Consequently, the present assessment will put a particular focus on the following EU measure: Council Decision 2007/845/JHA on cooperation between EU countries' Asset Recovery Offices in the field of tracing and identification of proceeds from, or other property related to crime.

Summary of the discussion: Although the time limits in the Swedish initiative are generally respected, participants plead to speed up the response time to Asset Recovery Offices (AROs). The question on how to enhance requests, quality and responses could be addressed by an increase of the level of training and skills. Additionally, there is a need to look at high risk sectors and to map out investments made by organised crime groups in order to better detect the infiltration in the economy. There is support for centralised registers and AROs access to them. Still, it is necessary to increase the cooperation between AROs, customs and Financial Intelligence Units (FIU). However, there are mixed preliminary views on whether AROs should have power to freeze assets, which is only supported by some countries, this issue will need to be further examined. Above that, it is necessary to look at other types of information about assets such as land registers. On the access to company data: the Commission is currently working with Europol on a pilot project to support the investigative community. Finally, cooperation with third countries must be strengthened; the Commission and Europol support the CARIN network (Camden Asset Recovery Inter-Agency network) with one law enforcement and one judicial contact point.

Panel 3 – Firearms

Background: The illicit trafficking of firearms is part of the core business of organised crime groups as a source of revenues, because it makes possible other forms of crime and they are used for intimidation, coercion and gang violence. Above all, the series of terrorist attacks have shown the imperative to cut off access to both firearms and explosives. The European Institutions have initiated various political, strategic and operational measures which contributed to a better understanding of firearms trafficking within different EU countries though different means (studies and operations).

The decision to prioritise firearms under the 2014-17 serious and organised crime policy cycle offered an unprecedented opportunity for concerted action by the EU over several years. In addition, the European Commission adopted on 2nd December 2015 an Action Plan to better prevent, detect, investigate and seize firearms, explosives and explosives precursors to be used for criminal and terrorist purposes as part of a Security Package. It complemented the legal initiatives adopted on 18 November 2015[306]proposing stricter rules in the legal use of firearms and common firearms deactivation standards. In view of this new legal landscape, the present assessment aims to focus on the recent actions taken at EU level on this issue, in implementing the following EU measure: the 2015 EU action plan against illicit trafficking in and use of firearms and explosives.

Summary of the discussion: The correct implementation of the current legislation must be ensured. Firearms should be kept in the operational political spotlight and as a separate priority in the Policy Cycle. Capacity building in the EU was discussed as an important area to be continued and the setup of national focal points and its connection the European focal points were envisaged. Cooperation with 3rd countries must be ensured, particularly with the

[306] See IP/15/6110.

Western Balkans. Furthermore, interoperability of different databases must be ensured, especially on ballistics. Despite this, the progress on other databases was noted. The technological dimension of tracing should be introduced and work on the tracing of deactivated firearms should be stepped up. The essential core of the work must be the cooperation with customs, services but also more cooperation with private actors and better use of the network of support from the private sector.

Panel 4 – Cybercrime

Background: Ensuring full implementation of existing EU legislation is the first step in confronting cybercrime. The 2013 Directive on attacks against information systems criminalises the interference with information systems, thus covering more than only computer systems, the mere provision of tools such as malicious software and strengthens the framework for information exchange on attacks. The 2011 Directive on child sexual exploitation approximates national legislation to prevent child sexual abuse online. The Commission has been working with the Member States to ensure correct implementation of these Directives. Rules also have to be kept up to date. Citizens are concerned about issues like payment fraud. However, the 2001 framework decision combating fraud and counterfeiting of non-cash means of payments may appear to no longer reflect today's realities and new challenges such as virtual currencies and mobile payment.

Cybercrime is borderless, flexible and innovative. Cooperation 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 digital age. The Commission is currently reviewing how to remove obstacles to the investigation of cyber-supported crime and terrorism, as well as it is currently reviewing mechanisms available for obtaining cross-border access to electronic evidence. The Commission has just begun a review of the role of encryption in criminal investigations. The Commission services have built upon these parallel processes instead of duplicating them in the context of the present assessment.

Summary of the discussion: Support was noted for the ongoing work on data retention, e-evidence, encryption and non-cash payment fraud. Also the use of the Budapest convention as a vehicle for international cooperation requires support, possibly via an additional protocol. Participants recognised the need for enhanced training, particularly for prosecutors and judges, but also of analysts. Besides this, there is a need to ensure that the existing legislation is properly implemented. Concerns were raised regarding the Internet of Things. Ideas must be developed on how to deal with suspects in non-cooperative third countries. Participants agreed that this is an area where joint bodies such as Europol and Eurojust can do more on the practical side. More collaboration and resources sharing for the development of technological tools and centres of excellence as well as expertise are welcomed. These could be based in the agencies. Concerns were expressed that fundamental differences would remain. An additional protocol to the Budapest Convention with a number of principles for efficiency could be an option. Also discussed was the link between encryption, Internet of Things and authorisation. The process of granting access could be better calibrated; there is the possibility for public authorities to set certification or standards for encryption and all inter-connected subjects. Discussants agreed on the need to increase cooperation with strategic partners. A sense of collective responsibility with the actors providing services and technologies needs to be created.

The role of Europol

Europol presented areas in the agency has and can develop further added value.

Europol considers that it plays an important role in trust building: Europol is also about building trust between Member States; among the Member States but also with third parties,

including the agencies and the private sector. The agency seeks to establish more connection – for example to Financial Intelligence Units and customs, by not only connecting the people but also databases. Legal activities are streamlined; proper processes of how firearms are dealt with, encryption, and retention need to be secured. The positive attitude towards putting forward ideas also for Europol in a support function for the Member States was noted.

4. Civil Liberties, Justice and Home Affairs Committee (LIBE) "Exchange of Views – European Parliament, National Parliaments and Civil Society

Following up on the Commission's request for input to the comprehensive assessment, the LIBE committee organised an exchange of views on the EU's security policy with representatives of national Parliaments and civil society on 11 May 2017.

In his opening remarks, Commissioner King underlined that the transnational nature of security threats required EU level coordination while the primary responsibility in this field rested with Member States. He also explained that the Security Union objective was to close down the space in which terrorists operate and to build resilience. He informed that the stakeholders had welcomed the comprehensive assessment as a way to exchange ideas freely in parallel to the traditional institutional framework. He informed of the comprehensive assessment's methodology and process, and the main issues emerging from the input received so far:

- Need for improved implementation;
- Need for pooling resources and building shared centres of excellence;
- Need for exchange of best practices;
- Need for synergies and multidisciplinary approach – between internal and external aspects, law enforcement and customs;
- Strong appetite for further work on radicalisation;
- Interest in reinforcing our experience and expertise in data sharing.

Representatives of the BE and IT Parliaments informed of ongoing legislative work in their respective countries and provided their views on issues requiring increased attention. In particular, they:

- Considered that there was a shift in the nature of terrorism and warned against reactive/emergency legislation;
- Highlighted work on the implementation of PNR and on pre-paid SIM cards;
- Stressed the importance of data and information sharing and proposed the establishment of a clearing house for this purpose;
- Highlighted links between terrorist financing and illegal migration ;
- Called for proposals extending interoperability of systems to the judicial area and to third countries.

Contributions from civil society organisations included:

- Stressed that safeguarding human rights and rule of law contribute to security;
- Criticised the Directive on Combating Terrorism for its expedited procedure and broad definitions, and stressed that the Directive's implementation must be closely monitored;
- Argued against fast track legislation and called for regular impact assessments to accompany proposals;

- Called for CEPOL to provide assistance for developing minimum standards across Member States for policing, in particular for police training and equipment;
- Suggested that a minimum percentage of the GDP should set aside for security purposes in Europe;
- Highlighted the diverging policing practices in Europe and the diverging economic situation in Member States, and suggested to allocate ISF funds according to Member States needs;
- Called for an Erasmus type of programme for police officers, extended to non-senior ranks.

MEPs and representatives from National Parliaments raised the following issues:

- Rights and protection of victims;
- International cooperation on security;
- Importance of fighting money laundering including fighting org crime and cybercrime;
- Phenomenon of home grown terrorists and the causes of terrorism;
- Importance of anti-radicalisation and appropriate funding for this purpose;
- Heterogeneity of police forces, their resources and practices;
- Need for harmonised rules on organised crime;
- Possible voluntary measures to block online terrorist content;
- Rule of law, data retention and sovereignty issues;
- Information exchange also between national parliaments and the need for a platform provided by the Commission for national Parliaments to discuss legal acts related to the reduction and management of threats;
- Need for proper implementation.

Commissioner King concluded by inviting national Parliaments and civil society to submit their contributions in writing. He acknowledged the importance of human rights and transparency and reiterated the importance of implementation. He called for bringing down barriers to information exchange and asked for support for the work of EU Agencies. He also underlined that a comprehensive approach was needed for effective prevention and de-radicalisation.

The event was public. Further information and a video recording can be found here: http://www.europarl.europa.eu/ep-live/en/committees/video?event=20170511-0900-COMMITTEE-LIBE

5. Policy Meeting of the Centre for European Policy Studies (CEPS)

This meeting held on 12 May 2017 aimed at bringing together a selection of EU policy makers and academics, and collect inputs contributing to an evidence-based assessment of EU Security Policy.

The event gathered a number of scholars who actively follow EU and nationally-funded social sciences and humanities research projects covering themes of direct relevance for the Security Union, alongside Commission officials. It provided a unique opportunity for the exchange of perspectives and inter-disciplinary knowledge, and fed into the Comprehensive Assessment.

Engaging in participative roundtable panels, the attendants were invited to identify key issues, challenges and gaps in the existing EU security policy instruments in relation to: the use of information systems and EU data bases, cross-border criminal and judicial investigations and international cooperation. In discussing these issues, particular attention was paid to effectiveness, proportionality, fundamental rights and societal implications.

The meeting fell within the scope of the SOURCE research project, a network of excellence funded by the Seventh Framework Research Programme (FP7) of the European Commission.

Panel 1, Information Sharing

Coordinated actions in cross-border criminal and judicial investigations and proceedings constitute a central component of the EU Security Agenda. EU cooperation on extradition and the gathering of evidence (EIO) and joint investigation teams coordinated by EU agencies represent illustrative examples. Questions addressed: To what extent are these tools used and have they been 'effective'? What should be improved? Also, what challenges to criminal justice systems and the fundamental rights of defence and fair trial pose the expansive use of electronic communications and an intelligence-driven ('preventive justice') policing approach to law enforcement?

Issues addressed

- **The European Investigation Order (EIO):** as a tool to simplify and speed up cross-border criminal investigations; **it sets strict deadlines for gathering the evidence requested** - Member States have up to 30 days to decide if they accept a request; **it protects the fundamental rights of the defence**; it represents a new standards for legislation in the field;
- **Joint investigation Teams (JITs):** highly complex operations; welcomed by practitioners; need to prevent overuse; attention to costs involved;
- **EU policy making** as driven by events and urgency; need to give more emphasis on the protection of human rights;
- **Terrorism Directive:** careful observation of implementation is needed to prevent goldplating in transposition by the Member States;
- **Impact assessments** which bring clear understanding of effectiveness are needed, the right questions need to be asked in the right order; must be presented with every major legislative initiative; hence the use of impact assessment needs to be increased and enhanced;
- Role of **national courts** must be acknowledged and reinforced;
- No call for more legislation, but for **effective implementation** of current instruments;
- Counter-radicalisation efforts must foster a **strong culture** and offer **alternative narrative**.

Panel 2, Cross-Border Criminal Investigations

The effectiveness of information tools for law enforcement purposes is a priority of the EU Security Agenda and a key challenge, raising issues related to their access but also to their actual use by law enforcement agencies. As part of this priority, the goal of full interoperability of EU data bases or information exchange systems (e.g. SIS II, VIS, Eurodac, Prüm, etc) is another challenging issue. Questions addressed: Is 'more data' the most efficient answer in view of current experience and future trends? What are the issues raised by the increasing use of EU information systems, and the development of biometric technologies, for law enforcement purposes in the light of the principles of proportionality, necessity and the fundamental rights of data protection and privacy?

Issues addressed

- **Information and data systems:** Member States are relying more and more on information systems and the use of SIS and VIS is increasing steadily, we need to make better use of what we have now and improve systems; burden of evidence and explanation;
- **Good practice and data protection:** good practice is needed to ensure the right input of information and to uphold principles, data protection authorities are protecting the data and ensure the proper assessment, every person has the right to access its own data;
- **Interoperability:** objective must be analysed in order to achieve it; systems have different objectives, these should not be merged; although the discussion on interoperability is not new, the nature of threats and the security environment have changed;
- **Issue of trust:** systems help to increase mutual trust;
- **Security in practice:** there is an assumption of consensus of what type of security is wanted, but in practice there is no unanimity; purpose limitation principles are no danger but are there for security;
    - **Communication:** Member States do not understand all policies properly; this is due to a lack of clear, honest and open communication of the purposes for which the instruments are used.

Panel 3, International Cooperation

International cooperation is an additional component of fundamental and increasing relevance for the EU Security Union. Cooperation with third countries through information exchange and capacity building aim at reinforcing the EU security. In the area of criminal investigations and judicial proceedings, the EU relies on specific agreements with countries covering access and exchange of information tools (e.g. PNR, TFTP) and mutual legal assistance treaties. However, in an era of increasingly dematerialized exchanges and reliance on electronic information and IT communications, access to data and evidence poses a number of challenges related to issues such as conflicts of laws, jurisdiction and EU data protection legislation.

Issues addressed

- **Agencies:** stronger protection of JHA agencies is needed ; joint training must be increased, a strategic decision and budget is needed for Eurojust, Interpol needs to be promoted as a tool;
- **Third countries:** with new legislation Europol has more possibilities to receive information; Council tools need to be promoted more judicial cooperation with third countries such as the MENA countries; a differentiation between EU databases and access for third countries is needed;
- **Interoperability and outreach:** increased deployment of Liaison officers enhances exchange of information, first hand exchange visits are needed;
- **Profiling:** issue needs to be solved, input from academia is needed;
- **Cybersecurity:** issue of human resources rather than policies; best experts are needed to help Member States in practice; cooperation with private sector is needed;
- **Electronic / e-evidence:** if a company offers services in countries abroad (e.g. Whatsapp) it must answer to law enforcement enquiries, it should not be required to ask the country of origin for the information; the European Border and Coast Guard Agency asks migrants on a voluntary basis to share information from their phones;
- **Data exchange and retention:** Member States have to agree on a case by case basis and only if legally allowed; ad-hoc exchanges including a proportionality assessment are only possible with 3rd countries without an agreement in place; no exchange between databases as they have been initiated for different reasons; a valid assessment and a legal framework for the retention of data is necessary to ensure that it is consistent with human rights, need to think about long-term implications and the ethical dimension;

- **Defence through deterrence:** how to merge defence concept and information sphere?;
- **Role of the EU:** ABC = amplify, build capacities and coordinate (also with external actors), knowledge on what happens on the ground needs to come from civil society organisations and NGOs; need to provide solutions which are more agile and flexible to adapt quickly, bring more attention to the "world of the judiciary", more on national judges and courts is needed, promote better agreements of Mutual Legal Assistance (MLA);
- **Radicalisation:** need to learn from each other;
- **HLEG:** consider to extend its scope to include industry.

6. European Organisation for Security (EOS) "High Level Event on European Security"

Discussions with the industry took place in the framework of a High-Level Event on European Security hosted by the European Organisation for Security) on 15 May 20017 in Brussels. 28 representatives from different companies – members of EOS participated in the event. The discussions focussed on security research activities and EU industrial policy.

Main takeaways

- There is a strong need to explain the value of concrete results developed through EU security research projects and to establish a consolidated approach to streamline the market uptake of research by practitioners;
- An interest in discussing how to overcome market fragmentation through better certification procedures, and develop more embedded procedures that can lead to certification;
- Continue the dialogue on capabilities development in the EU by identifying areas such as borders, reinforcing cPPP and continue structured dialogue with practitioners, for example in the field of transport.
- Optimise the current research tools and normative tools and some of the ways we conceive security policy.

The following points were raised in the discussion:

There is a need for the EU and the industry to jointly explain the value of what has been done together, drawing more on the industry to get examples of concrete, possibly already commercialised solutions or technologies stemming from FP7and Horizon 2020 security research projects.

Capabilities must be developed within the EU and possibly identifying capability gaps for priority action. Borders were named as an important area of interest. Here, border management includes also the collection and analysis of data. Collaboration with the industry in this area could bring added value; as an example was given the framework for NATO-industry engagement. The stronger involvement of the "European Border and Coast Guard Agency" (EBCG) in the management of border related security research projects was welcomed as a highly promising action to increase practitioner uptake of research.

Cybersecurity was mentioned as an area with potential for more collaboration. The discussion focussed on how to better link private sector funds and other funds for cyber security. The lack of experts for critical companies was noted and the how best to support job creation and education. In terms of the cPPP on cyber, the need to define results together to get appreciation of what is needed was noted. A potential to exploit this approach was noted for soft targets; the industrial dimension was mentioned as extremely important for the future strategy and consolidation of EU capabilities.

A lack of continuity between research and operations, i.e. better linking FP7/H2020 research to ISF/AMIF, was criticised. Suggestions for improvement included the creation of a

structuring programme "Securing Europe Facility" (SEF) as an equivalent of "Connecting Europe Facility" (CEF). This could enhance the link of innovation results and standardisation issues and support Member States in financing and implementing security solutions. The application process for research in H2020 was criticised as being too complex, the administrative burden was too high for small and medium sized enterprises.

A network of security practitioners in the area of border surveillance was mentioned. Its creation could provide horizontal support for the community and industry, thereby establishing link which can help industry understand where support and further development is needed.

The need for standardisation, certification and harmonisation was discussed. It was noted that certification could defragment the markets and could support especially small and medium enterprises. Standardisation issues were linked to the capacity of Member States and agencies to procure together thereby turning public procurement into de facto standardisation tool.

On interoperability, it was noted that the first phase of the HLEG was more trying to bring authorities together to appraise the weaknesses from the user perspective, but the industry will need to be more present. Feasibility studies should be performed on how to translate the recommendations. There is a need for a strong industrial dimension. Regarding the financing, conditionality should be reinforced and the context of future research programmes and types of financing must be made available.

Finally, an annual high-level debate on the development of security policies and research within the EU would be highly welcomed by the discussants. Also bilateral meetings on a rather operational level would be appreciated. The industry was urged to share their ideas and concerns on a regular basis as the receipt of feedback, suggestions and recommendations on EU security policies and activities will contribute to better collaboration and development.

VII. Questionnaires

Questionnaires to Member States and JHA Agencies

Question 1

What are the areas in which EU measures have had most positive results and/or impact in your country, at internal and external level (eg. supporting EU values and interests externally and/or at global level) and for what reasons? When possible, please assess and describe the benefits brought in by EU measures. Please provide concrete examples of success stories where EU tools were instrumental for achieving concrete results on the ground (e.g. prevented attacks, dismantling of organised crime networks, etc.).

Various Member States underlined in their replies that EU cooperation instruments were more effective than traditional forms of police and judicial cooperation. Overall, the most positive results obtained had been in the facilitation of information exchange, accelerated investigations, the facilitation of the collection and exchange of evidence, and the support provided in strategic planning and operational activities.

Mutual Legal Assistance (MLA), joint investigation teams (JIT), the Schengen Information System (SIS II), the European Arrest Warrant (EAW) were among the most commonly mentioned as having given or facilitated law enforcement and prosecutors access to information and evidence that helped them bring offenders to justice. To illustrate the impact of these instruments, some Member States noted the considerable increase in arrested wanted criminals after joining EU tools such as SIS II and the EAW.

A number of Member States considered that progress had been achieved more particularly as regards the cooperation in the fight against terrorism.

In that context, they put forward the role of Europol, the effectiveness of the Schengen Information System which allowed locating individuals and detecting the return of foreign fighters, and the use of JITs. SIENA CT was also valued for allowing direct and swift exchange of information between law enforcement, and contributing to substantial quantitative and qualitative improvement of the cooperation. Within Europol, the establishment of the ECTC as a hub to exchange information, conduct analysis and coordinate operation support was a progress and the Internet Referral Unit was also seen as effective in supporting Member States in removing illegal terrorist and radicalisation content from the Internet. A Member State also noted that EU platforms such as the RAN, the EU internet forum and the European Strategic Communication network had proved useful for the exchange of good practices and lessons learned in countering radicalisation.

Many Member States stressed the practical benefits resulting from JITs, which included improved information exchange, enhanced mutual trust, best practices having been exchanged, enhanced collection of evidence, and optimisation of the procedures within the investigation by mutual recognition of the actions carried out by the parties.

As regards the exchange of information, some Member States underlined that the Prum decisions and the Swedish initiative have become indispensable and particularly effective to ensure a swift information exchange, support everyday forensic work and provide a legal framework for organising joint operations and providing assistance in the case of major events. A few Member State also mentioned the ENFAST network which allowed to sharing information on high profile internationally wanted criminals.

Member States noted that Europol had allowed for increased information sharing, increased coordination and cooperation and provided useful analytical tools. A Member State noted that SOCTA helped understanding crime dynamics.

Various Member States also underlined the benefits of the EU Policy Cycle which allowed Member States to cooperate on common priorities and to work closely on operational actions. Its impact on the cooperation with third countries was also positively assessed and as

underlined by one Member State, its positive effect on national coordination (among national police forces, border police, customs and judicial authorities). The implementation of operational actions within EMPACT has resulted in an increase of cross border investigations, operations, crime prevention activities and interagency cooperation. Funding through the EMPACT delegation agreement and, from 2017, from Europol's budget is providing support to the implementation of operational actions by member States.

On drugs, as noted by an Agency, EU strategies and actions plans have provided a catalyst for a European vision based on a balanced approach and respect for human rights. It allowed the EU to speak with a stronger voice at international level. Council decision 2005/387/JHA on the information exchange, risk assessment and control of new psycho active substances, is an example of a measure which facilitated the exchange of information and allowed to identify emerging threats. Risks assessment and EU wide control measures have helped create a level playing field for law enforcement to tackle these challenges.

On firearms, a Member State underlined that EU measures had proven to be useful for improving traceability, introducing stricter specifications for deactivation resulting in seizures, develop intelligence led approach (EMPACT) and funding disarmament programmes. The European expert group on firearms was also mentioned by a Member State as having been critical to understand the threat related to firearms trafficking.

A few Member States also mentioned positive results in fighting financial crime resulting from EU instruments, the anti-money laundering directive driving the cooperation across the EU to tackle financial crime, while requiring Member States to set up FIUs. The Asset Recovery Offices (ARO) platform was considered by two Member States as an essential tool for locating criminal assets. Some Member States emphasised that the ARO platform had been essential to foster information exchange but also to perform analysis at operational and strategic level.

Member States provided various examples of concrete cooperation in the context of Europol allowing for dismantling organised international criminal groups operating in various countries. They also mentioned the successful cooperation achieved with the EU migrant smuggling centre and with the Internet Referral unit which had worked to improve the partners capability to increase referrals, intelligence collection and disruption opportunities relating to groups utilising social media as a communication or advertising tools to conduct their criminal activity.

Another concrete example given by a Member State was the positive impact of the definition of a common taxonomy on cybercrime which had facilitated the communication at national and EU level between cybercrime units and CERT centres.

Various Member States underlined that EU financial instruments enabled to improve the investigative methods, tactics and strategies of law enforcement, allowed the acquisition of equipment and the development of databases or information systems. In the field of border security, a Member State noted that projects funded by EU programmes had a benefit for the whole Schengen area, while, on the other, they would not have taken place otherwise.

Changes in the JHA policy landscape has been reflected with important evolutions of the EU large scale IT systems. As an example, there was an average of 550 hits on a daily basis in SIS II compared with 350 in 2014, illustrating the increased use and relevance of the system.

Agencies also noted the benefits which could be taken out from Eurojust analyses in terrorism related cases in the context of the Council Decision 2005/671/JHA on the exchange of information on terrorist offences.

Another progress noted in Agencies' contribution is the key role played by the EU level of governance in creating an environment in which rights and freedoms are well protected. Among the mechanisms which ensure that security measures are designed and implemented in a legitimate and proportionate manner is the EU Charter of Fundamental Rights. Some EU

measures which are primarily security oriented in nature have also additional objectives important in the context of fundamental rights, for example the Directive on combating terrorism which incorporates central provisions on the protection of, support to and rights of victims of terrorism at international level, promotion of and action on human rights is a component in enhancing security. Fundamental rights checks and balances in practice can underscore the EU as a credible actor, which can support efforts to reduce terrorism, radicalisation and organised crime.

Question 2

Have EU measures facilitated your cooperation with other Member States, and if so, in what way(s) (for example by improving national capabilities, by complementing or stimulating Member States' action, by agreeing on common priorities)? Please identify, in which of the three areas (terrorism and radicalisation, organised crime and cybercrime) EU measures have most facilitated your cross-border cooperation at operational level, with other Member States?

Many measures have been mentioned by Member States as having facilitated operational cooperation which is seen as having significantly improved in recent years (see also the replies to Question 1). EU instruments contributed to and improved international cooperation and information exchange at operational level. Some Member States also noted that improved awareness of each other's procedures and legislations had contributed to better operational cooperation.

As noted by a Member State, EU instruments in general contribute to improving national capabilities. Some specific instruments were mentioned though as having a particular effect. In first instance, trainings and seminars organised at EU level (Europol, CEPOL, RAN, Commission). The use of the Europol Information System as well as the lessons learned and best practices shared in the context of the EMPACT projects and in the RAN were mentioned. The pressure resulting from evaluations done at EU level was also mentioned as, even less directly, having an effect.

The role of Europol with multiagency cooperation and analytical working files (AWF) as well as instruments such as SIENA allowing for a swift and secure exchange of information were highly valued. Information sharing on counterterrorism between the Member States as well as through and with Europol reached an all-time peak in 2016, demonstrating a significant increase in the level of trust in and awareness of Europol's support services among national counterterrorism authorities.

The Schengen Information System was another instrument most frequently quoted by the Member States as one of the most successful tools for an effective cooperation between immigration, customs, police and judicial authorities in the EU and the Schengen associated countries, some of them underlining that it has become, after limited use at the beginning due to scepticism and worries about the protection of information, a major and indispensable instrument allowing for successful cases which led to a broader use for very sensitive cases. SIS is valued for the information it allows to share on persons and objects checked and the clarity of the practical instructions it provides about what needs to be done.

The European Arrest Warrant in the field of law enforcement and judicial cooperation, Joint Investigative Teams (JIT) have been extensively used by many Member States.

The EU Policy Cycle and EMPACT was also mentioned by many Member States and Agencies as an instrument which allowed on one hand to agree on common priorities, and on the other hand to reach tangible results and improve interoperability by sharing best practices, data and experience through the many operational actions taking place in that framework. The EU Policy Cycle has facilitated cooperation with the Member States but also between Agencies.

Many operational results have also been credited to ECRIS which significantly simplified and accelerated info exchange about convictions and the Prum Decisions which allowed for DNA analyses and fingerprint exchange of information facilitating criminal investigations and supported the organisation of mixed patrols and joint operations. Police and Customs Cooperation Centres have been established in many Member States which valued their contribution to facilitating the exchange of information. ENFAST has also enabled Member States to take immediate actions for locating and arresting fugitives. Other operational support mentioned by Member States includes the risk analysis and situational awareness provided by the European Border and Coast Guard Agency and the support provided by the EMCDDA as a hub for early warning on synthetic drugs.

The fight against cybercrime is an area where Member States noted that progress in the cooperation has been particularly important. The role of Europol was again underlined and the EC3 analysis resulting in identifying and locating suspects, as well as of the EU Policy Cycle with many joint operation and preventive initiatives against cyber-attacks and sexual exploitation of children on the internet organised. The EU Internet Forum was seen as helpful in developing a consistent approach with internet service providers (ISPs).

As regards the fight against serious and organised crime, a Member State noted that it is in this area that the EU has played the most notable role, while playing an increasing role against cybercrime and terrorism in the last two years. Europol is helping by the sharing of intelligence and set EU priorities as well as the projects carried out under EMPACT and the funding programmes (ISEC, ISF). A positive effect of these tools is they incited partners to analyse criminal phenomena beyond national situations. EU measures aimed at disrupting the finances of organised crime and on mutual recognition were mentioned as well as the EU Drugs strategy for their valuable contribution. In the area of trafficking in human beings, EU instruments have been providing a significant contribution to police cooperation and facilitated and accelerated both the detection of offenders and international investigations.

As for the fight against terrorism, the SIENA communication channel allowing for direct connection of anti-terrorism units and SIS II were mentioned as making a significant contribution, allowing exchanging information in real time. Joint Investigation Teams, the Radicalisation Network (RAN) and the joint liaison officers have proved useful. The API Directive and the TFTP have also provided operational support. The support provided by Europol, and the potential of the ECTC in the context of Europol, was also emphasised as demonstrated by the increased quantity and quality of data exchanged. The work done by the EU Intcen was valued. The exchange of experiences concerning counter-terrorism strategies was also considered as a positive contribution of the actions at EU level. Overall, EU instruments were recognised by different Member States as enhancing prevention, detection and response capacities.

The EU is playing an important role in fostering a common understanding among practitioners working in different Member states of what fundamental rights obligations mean in practice. Mechanisms such as the Schengen evaluations foster a common understanding of fundamental rights standards and their approximation across the EU. Agencies also allow for exchange of operational know how between Member States.

Agencies also noted that inter-agencies cooperation and partnerships have allowed for joint activities (including training) and projects which have created synergies and economies of scale.

Question 3

What limitations have you identified in the design and/or in the implementation of the EU measures (such as for example limited technical or financial resources) which have hampered their effectiveness?

Member States highlighted limitations related to resources and financial matters.

Notwithstanding improvements since 2016, Europol's information management capabilities have not been fully exploited in the area of counter-terrorism. There seems to be a lack of financial and human resources in Member States to ensure the effective implementation of the EU Policy Cycle. Resource limitation can also slow down the implementation of new information systems or system evolution.

The implementation of some complex legislative proposals has been identified as difficult and time-consuming. Member States often need technical (expertise) and financial support. For instance, as regards the implementation of the PNR Directive and the participation/cooperation of all EU Member States, despite the relevant Implementation Plan elaborated by the Commission and the setting up of relevant working groups at national level, only few Member States [at the time of the questionnaire] have so far been considered to possess fully operational systems and a legal background that can support PNR.

Some Member States also pointed out the limits in the available financial resources through the ISF (Internal Security Fund) compared to the needs for border surveillance issues.

The applicable procedures and the timeframe were seen as difficult to be managed by the operational units, which might not have both experience and resources to manage such projects. The financial rules applying to EU funding in the Policy Cycle and EMPACT process may also seem overly complex and potentially burdensome.

All Member States still do not contribute with own data to the information exchange process. In addition, the lack of full interconnection and interoperability of the existing information systems at EU level that could allow faster search – exchange of information among EU law enforcement authorities has been again identified as one limitation.

Lastly, it should also be noted that there is no mechanism in place which would systematize reporting to Member States on irregularities and errors existing in the framework of information exchange between criminal registers. The data exchange by ECRIS system is an effective tool; however works should also be developed on unification of interpretation of the legal acts, as well as on technical and business model of the ECRIS system.

Another point was that the numerous initiatives taken by the EU might sometimes confuse the Member States and divide already limited national resources. It has been highlighted that the constant pressure of having to implement new initiatives might be counter-productive.

Specific limitations and difficulties in the operational cooperation in cybercrime cases have been reported by Europol and Eurojust in a joint paper on the common challenges in combating cybercrimes based on both agencies' operational and practical experience. In the cyber-crime area, there are major limitations in the policy framework in relation with the loss of data, loss of location, differences in legislation, international cooperation and public private partnership as well as expertise gap.

The political responses to meet security challenges not always take into account training needs among the measures to be taken in the early planning stages.

The implementation of instruments for judicial cooperation meets a series of limitations and difficulties including difficulties in the interception of telecommunications and cross border surveillance, insufficient or inadequate use of the exchange of information tool, lack of an indication of time limits in urgent request, different rules on gathering, admissibility and disclosure of evidence, difficulties in the cross border recognition of civil seizure and confiscation, delays in the execution of freezing orders or in the recovery of frozen assets. The

implementation of the EAW faces difficulties related to the insufficient translation resources at national level.

Links between border management and internal security should be better ensured in order to avoid a silo approach. This applies to migration management, document security or identity management, policies related to the collection nd use of advances passenger information (API and PNR).

Question 4

Are there EU measures and tools aimed to facilitate cross border cooperation at operational level (e.g. police-customs cooperation centres (PCCCs), joint investigation teams (JITs), joint customs operations (JCOs)), which you believe are not used to their full potential? If so, which ones and for what reason (e.g.: procedural complexity; technical difficulty)?

Most Member States noted that all the available EU measures-tools, aimed at facilitating cross border cooperation at operational level, are not used to their full potential.

An agency noted that information, awareness and knowledge of existing EU instruments were not sufficiently widespread among law enforcement officials, with likely shortcomings in the circulation of information and the cascading of gained knowledge.

Among the reasons explaining the limits in the use of the EU Policy Cycle were factors such as low budget allocation for certain EMPACT priorities and burden linked to the financial grants/expenditures and management, cases of overlapping with other initiatives, a lack of recommendations for the engagement of certain actors within certain priorities.

In the case of Joint Investigation Teams (JITS), there is still a lack of awareness on the overall usefulness of the tool and the ways it can facilitate cross border cooperation.

Some Member States considered that these instruments have not been used to the full extent due to a lack of sufficiently valuable operational information, the complexity of the actions needed at all stages, the unequal involvement of individual Member States and different approaches adopted by the Member States due to their different legal and organizational requirements.

Different ways were suggested to improve the cooperation within JIT, including organising seminars and lectures for the law enforcement authorities and prosecutors to disseminate the knowledge about JITs, publishing materials on JITs dedicated for practitioners, extending the possibility of using Eurojust's funding also for national costs borne by JIT's members during the activities conducted and Joint Police Operations and Joint Actions Days.

Various Member States noted that the possibilities offered by Article 17 of the Council Decision 2008/615/JHA (Prum Decision) were not fully used. In the absence of other instruments, such as international agreements, the cooperation in the forms of joint actions and joint patrols is more difficult. Also the Manual on Cross-Border Operations – national fact sheet, does not contain complete contact points or detailed procedures for the implementation of Article 17 of the Council Decision 2008/615/JHA.

With regard to the Police-customs cooperation centres (PCCCs) most Member States identified them as a proved valuable for facilitating cross border cooperation. The PCCCs provide a fruitful cooperation due to the fact that the presence of Police Forces of different Countries, in the same working place, is fully developed and produce faster and positive working performances. In order to use of PCCC at maximum potential by expanding the possibilities for cooperation beyond the PCCC partners, it has been suggested that the uniform approach of the information exchange between the PCCCs has been appropriate. Some Member States called for a unified approach to chain requests, within all the PCCCs (some seing this as a good practice).

Nonetheless, each state has its own individual needs, thus some of the instruments (for example, PCCC) even though very efficient in certain states, are irrelevant in other states.

On the other hand, some Member States noted that the Entry/Exit system and ETIAS proposals are likely to make cross border cooperation more efficient in the future as well as the new SIS functionalities proposed by the Commission.

It is possible to state, that the general obstacles encountered in using the tools are: missing national implementation at all (e.g. Prüm) (perhaps due to lack of resources) and non-pro-European implementation in some countries (e.g. EAW). Implementation of common operations (e.g. within EMPACTs) faces difficulties in co-ordination between different Member States due to different already scheduled activities and stronger national priorities for use of resources.

AROs cooperation has proved efficient with a high impact on the increase of asset recovery, but there is room for improvement of the general framework of the cross-border crime. Likewise, Council Decision 2007/845/JHA of 6 December 2007 concerning cooperation between Asset Recovery Offices of the Member States in the field of tracing and identification of proceeds from, or other property related to crime is one of the instruments that could be reviewed by extending the powers of the AROs with respect to seizing, creating a centralized data base for bank accounts within each Member State, which should be accessible to AROs, as well as the exchange of good practices concerning the identification and tracking of virtual coins.

There is also a lack of cross border operations applying special tactics and, in some cases, a lack of proper legislative means to do so (for example in the case of controlled delivery of stolen vehicles).

Awareness on joint customs operations could be increased and joint customs and police operations could be further developed within the EU Policy Cycle.

Member States do not use the existing IT systems to their full potential. Data quality is an issue which contributes to hampering IT systems to their full. The deployment of SIENA to all competent authorities would facilitate cross-sectorial and cross-border cooperation further.

In the context of discussions on information systems and interoperability, consideration could be given to enhancing the potential fundamental rights beneficial effects by some of the IT systems, such as in relation to missing children.

According to agencies, practitioners are not all familiar with the support that Eurojust can provide in cybercrime cases. The information exchange between competent authorities and Eurojust under Article 13 of the Eurojust Decision could be further improved, as well as in the harmonisation of information provided on the basis of the Council Decision 20045/671/JHA.

The instrument in place for sending drug samples across borders seems cumbersome and could be usefully revised to reflect needs to exchange samples of new psychoactive substances which may be controlled in some countries but not in others.

Question 5

Are there specific areas where you consider that the EU measures brought little or no added value? If so, which ones and for what reason?

In general Member States highlighted the opportunities created by the European Union to use the most relevant measures, taking into consideration the needs and specific features of each Member State.

There were a few examples mentioned though of areas that would bring little or no added value.

In the judicial co-operation area, some Member States pointed at the "European orders" which supplemented existing tools but would be more complicated.

Procedures for Law enforcement access to Eurodac were seen as overly complicated and their implementation difficult, with the result that these instruments have been underused.

In the area of police co-operation two Member States considered that the so called Swedish initiative did not bring substantial added value and permitted very different national implementations. The procedures were considered as complicated and the exchange of some of the required information would not be possible to provide because of legal obstacles in each country's legislation.

Some Member States noted that current technical solutions and IT systems set-up under EU law remain fragmented with little synergy between different instruments. This would lead in some cases to multiple capturing of similar data and gaps in information at the same time. Efforts for reviewing the access conditions of various IT systems and reducing the fragmentation in data management should therefore be continued as a priority.

In some cases, such as for the Prüm decisions, it was highlighted that there is an implementation gap in some Member States which reduces their overall potential.

Some Member States were concerned about the multiplicity of Council's working parties dealing with similar issues, which would not necessarily add value.

In the fight against terrorism a number of European tools have provided a real added value. Some Member States noted that Europol's initiatives in this area, which are constantly increasing do not always take into account the objections of individual Member States.

Financial investigations, although being a priority in terrorism related cases, constitute an action that has not been used to its full extent. The lack of significant results in this field was explained as being linked to the complexity of these investigations, the high level of expertise required for their implementation, the time-consuming procedures necessary to check the financial information obtained, the legal impediments that may prevent the authorities from conducting parallel investigations, the absence of coordination and cooperation on an internal level.

The potential of some measures to ensure the rule of law was considered by an Agency as remaining untapped, such as the EU Framework to strengthen the rule of law which could be an important instrument also in the context of how security measures are applied at the Member State' level.

A limitation in the PNR Directive was identified concerning the impossibility to share at EU level the risk indicators and screening rules to be developed by national PIUs on the basis of PNR data, which would lead to different performances as regards risk assessment of travellers coming to the EU/Schengen area.

Question 6

Have you identified area(s) where EU measures overlap with other EU policy/instruments, and if so, which ones within the EU Security Policy?

The majority of the Member States did not identify any significant overlap. An Agency noted that some overlaps between instruments could even be beneficial, provided they are fostering synergies.

Yet Member States highlighted that a better coordination between all EU agencies, on the one hand, and with other international organisations on the other hand would be needed to avoiding possible duplications of various actions as well as cross fertilize civil and military actions. Cross-sectoral joint training and exercises are needed both at national and EU level to better tackle potential large scale incidents. An Agency noted the need for a better

coordination between internal security policy and external action and underlined the importance of sufficient coordination between actors to ensure the sustainability and impact of projects.

A Member State called for improving cooperation between Customs authorities and the European Border and Coast Guard Agency as well as between Customs and national border agencies. On the other hand, an Agency noted that further coordination between operational actions falling under the EU Policy Cycle and the Customs Cooperation Working party would contribute to avoid potential overlaps.

At a more general level, a Member State emphasised that even though there was no real overlaps of measures, some issues would still need to be dealt with in a more transversal way.

Member States stressed that more awareness about existing instruments as well as cooperation for achieving results in the same areas would make the EU Policy Cycle even more efficient.

Some aspects of MLAs and JITs could overlap, especially if their setup and goals are not clearly defined. Similarly JITs could overlap with particular OAPs.

E-evidence and online measures to help curb terrorism and serious and organised crime were identified by a Member State as areas where more work could be done in order to bring common information to all actors and fora and ensure that that there are no repetitions in measures or conflicting approaches. Measures related to online trade of illicit goods and services should be synchronised to avoid potential overlaps.

There would also be some overlap between the contents of SIS II in terms of stolen or misappropriated travel documents and the Interpol SLTD database. Although it was acknowledged that databases are usually complementary given their different user communities, it was underlined that interoperability should be reinforced to avoid or reduce overlaps, with particular attention to be paid to the concept of common data repository.

As regards funding, more clarity would be needed on which funding sources should be used to avoid overlaps through the ISF and Europol.

Question 7

In what area(s) have you observed that EU measures led to negative side effects (including for example complaint from stakeholders), and if so which ones and why?

In general, Member States have not identified any example of significant negative side effect in the implementation of an EU instrument. One Member State considered however that the mandatory checks for EU nationals as per the changes introduced to the Schengen Border code in 2017 would be difficult to implement and might prevent border guards to perform proper profiling and tactical risk analysis.

At a more general level, a Member State noted that if concerns could rise in relation with specific instruments, this would be linked to the difficulties in the implementation and enforcement stages of EU measures. Another Member State drew the attention to the fact that the multiplication of initiatives could imply further burden for the competent authorities with a risk of "fatigue" with new EU tools. The multiplication of players dealing with similar issues was also signalled by a Member State as potentially making cooperation between Member States and agencies more complex. Also related to the multiplicity of instruments, a Member State drew the attention to the need for avoiding duplication of enrolment data, notably in the case of API related messages where it noted that air carriers would have to send the same message to different stakeholders and systems (Member States, eu-LISA, ETIAS) with a risk of mistakes which may lead to security gaps.

As regards issues related to specific instruments, two Member States mentioned some problems with the lack of consistency in the implementation of the Swedish Decision (in

relation to the pdf forms) as well as a possible lack of consistency with the use of some SIS II alerts.

There were some Member States as well as Agencies which expressed concerns on the negative effects and problems resulting from the ruling on the Data Retention Directive from the European Court of Justice in 2014.

On the other hand, there were also comments underlining the importance that limitations to fundamental rights meet the necessity and proportionality criteria. While measures could otherwise be challenged in court, unnecessary or disproportionate measures could also create adverse effects that undermine their actual objective of providing enhanced security.

Furthermore, attention should be paid to the practical application by Member States of the legislations or policies adopted at EU level so that they do not have unintended negative effects on fundamental rights. A sense of caution should also be applied to measures which could lead to the disproportionate targeting of minorities and discrimination due to ethnicity and/or religion. Still, agencies acknowledge that the PNR Directive adopted in 2016 addressed concerns raised in relation to the proposal of 2011. The practical application of measures supporting both immigration and security policy, such as Eurodac, SIS II and VIS, and the use of force in the fingerprinting process are raised as an issue.

Question 8

Has implementation of EU measures proven to be too costly? If so, which measures? How do you suggest the excessive cost could be reduced? Can you provide examples of quantitative/qualitative appraisal of implementation costs?

The views expressed by Member States and agencies as regards the implementation costs of the EU instruments were contrasted. Whereas some considered that none were too costly, others underlined that the implementation of certain initiatives, in particular new systems or data bases, is a burden on the Member States budgets which can be important. An agency insisted that training is a way to reduce costs as well-trained staff reduces implementation costs. Particularly online training is recognised as a very cost-effective tool.

Travel costs for meetings (participation to joint action days, coordination meetings, participation in acts of criminal proceedings abroad) are increasing substantially the costs of implementation of some measures.

A few Member States indicated that they do not engage in initiatives such as EU wide joint operations due to the excessive burden and costs which would then have to be assumed by a single administration. A Member State also emphasised the need to take care of avoiding overlapping operations.

There were different suggestions made to reduce the costs of the EU cooperation: a Member State suggested relying more frequently on videoconferences to reduce the costs of participation to trainings.

With a view to ensure cost effectiveness, a Member State suggested that actions to fight against radicalisation should include performance indicators.

A Member State suggested that future proposals could contain specific plans relating to funding options that Member States could make use of, giving at an early stage indications that could be factored in national planning. One agency recommends the scalability and ability to tailor the implementation of measures to reflect national contexts.

As regards information systems, a Member State asked for taking into account the human dimension of dealing with information they imply from their conception. In the context of the work to come on interoperability, it was also suggested that the EU ensures coherence of the exploitation systems of the different databases and ensure that all Member States use the same type of application. EU funds should take into consideration the need for "technological

harmonisation" as this will contribute to a better share of costs, while another proposed to consider ready-made IT solutions for all EU Member States. One agency also sees opportunities in the operational management level of information systems for more cost-effective and efficient approaches. Harmonised and more integrated approaches to the operational management of IT systems both at central and national level in order to optimise the costs and resources of designing, planning, building and operating systems are envisaged. Applying common standards and solutions, as well as using common procedures, such as common procurement, could help reducing the costs and efforts of implementation. The development of the European Search Portal solution, shared biometric matching service, whitelisting fingerprint devices for use with VIS, SIS II, Eurodac and the EES as well as an improved use of data analytics within systems could bring substantial financial savings. The Smart Borders technical proof of concept provides an example of the financial benefits to be leveraged through effective technical testing in advance of system rollouts.

Question 9

Please identify the instruments in each of the three areas (terrorism/radicalisation; organised crime, cybercrime), which you believe are no longer relevant in today's security environment. Which tools/policies/legislation are outdated/unhelpful and should either be upgraded or discontinued?

A few Member States considered that none of the EU instruments and tools present particular aspects to modify, and there was no suggestion to discontinue a specific instrument, with the exception of two Member States questioning the added value of the Swedish Framework Decision, without proposing to discontinue it though. A Member State was also critical on the Joint action days in the context of EMPACT, which were considered as burdensome with limited results for the services involved.

A number of Member States made various suggestions for upgrading existing tools. Overall, the views expressed were varied as regards measures to be updated and upgraded, and there was no particular convergence in the proposals made. However, various Member States concurred in considering that in a fast changing technological environment, judicial and police authorities' daily tools should be permanently reviewed. The internet's growing importance as a communications tool was identified by one agency as an area of priority for upgrading approaches and reviewing existing instruments to see if they are still fit for purpose.

On cyber-crime, according one Member State, legislation should be reviewed to fully cover cross border access to e-evidence. Another suggested that information channels should be improved, for example with a more efficient use of the European Judicial Cybercrime Network. One agency calls for an update of the Convention on Cybercrime 2001 and more specifically of the 2011 Directive on Combating the Sexual Abuse and Sexual Exploitation of Children and Child Pornography, the 2013 Directive on Attacks against Information Systems, and the 2001 Council Framework Decision on Combating Fraud and Counterfeiting of Non-Cash Means of Payment. Threats and trends are steadily evolving and instruments must be reviewed on this basis.

A few Member States noted that special techniques of telecommunication interceptions were evolving and should be covered by EU legislation. A Member State also suggested that in the field of asset recovery, measures concerning the deployment of covert investigators should be reviewed. One agency comments on the cooperation of EU Member States' Asset Recovery Offices and the need for review in the field of tracing and identification of proceeds from, or other property related to crime, namely the Council Decision 2007/845/JHA. The following measures would need to be reviewed and updated: the high threshold for evidence of the predicate offences, the problems of identifying beneficial owners, the probes of the abuse of the cash declaration system, the need for Centralized bank account registers (CBRs) and bank

statements in hard copies, reflecting the reviewed ML/AR regulations, urgent situations requiring precautionary freezing powers and mutual recognition of freezing and confiscation orders.

Two Member States proposed to update the EU strategy against terrorism. A Member State called for pursuing the work related to identification on the basis of biometric data due to the issues raised by the increasing capacity of ID fraud of terrorist organisations. As regards radicalisation, the improvement of the governance of RAN was seen as a priority by a Member State.

A Member State underlined the need to develop a true e-justice to increase the dematerialisation of procedures and foster the coherence of the new tools and the needs of operational services while another suggested that Member States should be encouraged to develop processes and methods within MLA in order to speed up execution of MLAs.

On the exchange of information, a Member State was in favour of updating the API directive, looking at synergies at with the Entry/Exit system and with ETIAS. A member state also proposed to review the Prüm framework set up and categories of data to consider new fields of cooperation (for example firearms, drugs, explosives). An agency suggested that Eurodac could be amended to better track the movements of asylum seekers and irregular migrants within Europe. Better appreciation of the movements of selected third country nationals within Europe by tracking secondary movements with this system and recording details about processing decisions and potentially return is seen as beneficial.

One agency sees the exclusion of law enforcement in the scope of the 2016 Network and Information Security Directive as problematic because it could create gaps in the investigation and prosecution of the incidents of criminal nature.

Question 10

Are there policy areas where you believe the EU should implement international standards and has not yet done so?

No such existing international standard was identified by Member States. In response to question 9 though, a Member State underlined the need to align definitions in the Framework Decision 2008/841/JHA on the fight against organised crime with the definitions in the UN Convention as well as to consider a review of the jurisdiction rules.

However, there were suggestions to progress in defining standards regarding data retention, security of connected objects, protection of European critical infrastructure and soft targets, decryption of devices and data, and for the identification of victims of child sexual exploitation.

According to one agency, international standards are beneficial in the area of large scale IT systems. Although international standards for fingerprint data formats already exist, further standardisation for fingerprint quality and structures such as biometric templates could be useful. Standardisation would have a positive impact on interoperability and could reduce vendor lock in.

Considering the increasing usage of automated border controls requiring fast document reading, an upgrade of EU passport standards in order to make use of high bit rate (VHBR) chips and LDS 2.0 structures should be envisaged according to one agency. The security measures and the scope of data within identification documents allowing the travel within the Schengen area appear to be the areas of priority of some agencies with regards to the above question. In this context, an agency states that opportunities provided by advanced passenger information and passenger name record should be exploited more systematically by EU Member States and Schengen Associated Countries in an interoperable manner.

Other areas suggested by agencies for the implementation of or improvement towards international standards are: Unmanned Aerial Vehicles, high risk pyrotechnics, pawn-shops and gold-stores, banning of "keyless go" technique tools for cars, Excise Movement Control System (EMCS) for monitoring the movement of excise goods under duty suspension in the EU, automated ballistic forensic standards (better identification of firearms), electronic evidence, security-by-design and privacy-by-design standards for goods and services provided in the EU.

An agency also underlined the need for international standards related to basic principles of human rights to be more explicitly reflected in EU legislation, for example those in the Geneva Convention relating to the status of Refugees.

Question 11

Are there areas where synergies between EU measures and/or EU actors should be further explored at EU level, and if so, which ones?

The great majority of Member States and agencies noted the importance of coherence between external EU security priorities and internal threats. In order to achieve a coherent approach in the field of security, Member States and various agencies called for a stronger link between the internal and external dimension and for looking at synergies between the internal security policy and the external action of the Union. Particularly a strengthened role for law enforcement agencies through intelligence gathering, including in conflict areas, was repeatedly mentioned by Member States. Secondary security checks are conducted by Europol Guest Officers deployed at hotspots are welcomed and collected information on returnees from conflict zones should be systematically shared with the ECTC in Europol and Member States via SIS. The strengthening of border management is perceived as a major challenge by some Member States.

Agencies also called for a better coordination between customs, border guards and police forces both at national level and at EU level. Both Member States and agencies also recognised the importance of cooperation between law enforcement agencies and customs. In this context, the distribution of competences between various authorities and its limits in cooperation must be clear. A stocktaking initiative on the distribution of competences between authorities could be a useful exercise.

In the field of data collection several Member States mentioned an interest in broadening the competence of law enforcement authorities for the collection of PNR data from other means of public transportation, notably maritime and rail. In this regard, the possibility to link different databases, such as ETIAS and PNR, was raised. The access of law enforcement to information systems such as VIS and Eurodac was also emphasised. Remote data access for the interception of new communication technologies is one of the suggested measures to be further explored. However, the creation of further information channels is not welcomed by Member States.

Synergies between EU agencies are also seen as beneficial regarding cost efficiency and continuity. Progress over the last years was acknowledged. Further improvements could be achieved, particularly between Europol, Eurojust, the European Border and Coast Guard Agency and OLAF.

The current work on interoperability was positively mentioned by a majority of agencies. Still, the increasing focus on internal security-related issues is an opportunity for further stepping up inter-Agency cooperation and information exchange to address EU policies and legislation in a comprehensive manner. Better integration of data gathering, reporting and analysis on drug precursors in Europe offers an opportunity for stronger synergies between bodies such as the EMCDDA, Europol and the European Commission.

An agency noted that an extension of the European Criminal Records Information (ECRIS) to cover third country nationals would increase agencies' capacities to coordinate investigations and prosecutions in the Member States in the most efficient way. The access to the envisaged secure online portal for electronic requests and responses concerning e-evidence was mentioned as beneficial for better judicial cooperation in criminal matters.

According to respondents, there is a general need for increasing the exchange of law enforcement information and criminal intelligence with relevant EU agencies by the Member States. Member States should make best use of SIENA. Cooperation between national law enforcement and administrative authorities should also be enhanced as noted by various Member States and agencies. The high-level expert group and legislative initiatives such as ETIAS, PNR, Eurodac etc. were considered as supporting agencies' information management capabilities.

Also the strengthening and coordination of cooperation between liaison officer networks is encouraged. In the fight against terrorism and radicalisation, synergies would result from a citizen centred approach with a focus on education and social inclusion as well as an administrative approach. The need for further initiatives aiming at raising public awareness on issues related to radicalisation, home-grown terrorism, and social polarisation factors are emphasised by the Member States. Further exchange between Member States on the issue of radicalisation with the aim to harmonise at European level the reporting of suspected radicalised persons was suggested.

With respect to cybersecurity and cybercrime, various Member States emphasised the need for enhanced cooperation with the private sector. Relations with cybersecurity organisations should be deepened. The interoperability of IT systems, online trade and e-evidence are issues to be further explored. An agency suggested that all EU agencies with cyber-related responsibilities should be included in the blueprint to handle large-scale cyber incidents at the EU level.

On CBRN-E, the centralisation of information on existing projects and programmes at EU level was recommended as well as further cooperation between military and law enforcement.

The strengthening of multidisciplinary cooperation, notably in the area of serious and organised crime and the promotion of an administrative approach both on EU level and national level have been suggested by several Member States.

On a more general note, Member States and agencies demand the "break of silos" to create a more integrated space for strategic analysis, policy development and operational tasking, due to the cross-cutting nature of issues related to terrorism, serious and organised crime and cybersecurity.

Question 12

In what areas do you believe that EU measures could contribute to better cross border cooperation at operational level, and how?

Most Member States focused on issues related to law enforcement and border authorities, the use of information exchange systems and access to EU databases. Electronic evidence, mutual legal assistance, data quality, cybercrime (online fraud, electronic payment fraud, virtual currencies, and anonymous services) were concrete issues mentioned for further improvement. Member States also generally called for full implementation and improvement of already existing systems/instruments rather than for new legislation. The optimisation of already existing instruments and the timely and efficient sharing of information should be the focus of the EU institutions. Concerns on constraints in law enforcement investigations due to a lack of access, data retention issues and encryption were also raised.

Analytical tools offered by Europol and the further development of existing tools for information exchange pursuing interoperable solutions are needed.

Various Member States also called for a more consistent approach regarding practices at the EU external border, particularly the identification of persons of interest (e.g. presenting a risk to security). To this end, the new Schengen Border Code was mentioned as a (possible) useful tool. An agency called for further exploring direct access to databases at the external borders (multi-databases cross-checks) and the interlinked and aligned elements both of border control, customs control, anti-terrorism measures and pure police collaboration. A Member States suggested to explore the possibility of interconnecting SIENA and Eurosur.

Numerous Member States refer to the continuous technological development and the challenges associated to it. This applies especially to data encryption. The potential of IT opportunities must be fully harnessed. Also the improved use of existing EU large-scale IT systems and more robust measures to ensure inclusion of high quality data is seen as an area for possible improvement by agencies.

A Member State suggested that further improvement of the functioning of SISII, bearing in mind the needs of the end user while increasing the automation of the process of entering a large set of data into SISII, for example by considering the possibility of entering only the first and the last series and numbers of stolen blankets of ID (blankets in between would be covered as well).

Several Member States and agencies were in favour of projects aiming at facilitating the exchange of expertise between law enforcement agencies, including third countries, as well as training projects to further improve cross border cooperation. Strengthening the cooperation with third countries is needed, more particularly in the field of border management and migrant smuggling.

With respect to EU funding procedures, various Member States asked for a smoother and faster process. In the context of the Policy Cycle, there were calls for an increased budget and reduced administrative burden, and a few Member States suggested an administrative procedure fully processed by Europol.

Sufficient resources (funding and staff) are an important pillar of cross-border operational cooperation. It was also suggested that funding for operational cooperation should not be limited to police forces, but enable multidisciplinary cooperation.

On cybercrime and cybersecurity challenges raised the lack of clear jurisdictions and issues such as e-evidence and encryption were repeatedly mentioned by Member States and agencies. The enhancement of practical measure in MLA was noted as a positive development. However, procedures for the retention and sharing of police and judicial-based information should be accelerated..

The process of Mutual Legal Assistance is criticised for being rather slow and Member States call for a simplified process. Common rules for the situations where Mutual Legal Assistance is not possible or a production order is not feasible (loss of location or emergency situation) are needed.

According to an agency the extension of secure communications services could contribute to current gaps limiting the capacity for law enforcement authorities to exchange information across borders during specific operations.

A few Member States refer to illicit arms trafficking as a priority objective which requires more focused attention on international and national level. There is a need for common technical standards for weapons, explosives and narcotics to counter trafficking across the Member States.

Question 13

Considering the evolving nature of the challenges faced by the EU, in what areas do you think that further action at EU level would be beneficial and what kind of action should be considered?

The majority of Member States and agencies agreed on a number of priority areas for further action. The most frequently mentioned areas were: cybercrime/cybersecurity (electronic evidence, information exchange, Mutual Legal Assistance, virtual currencies), cooperation with third countries, cooperation with the private sector (social media platforms and industry). As for previous questions, replies referred to the need to strengthen the link between internal and external aspects of security. Respondents also referred to the need for further focus on the protection of the external borders. The need for common security standards, training and capacity building for law enforcement and judicial authorities were seen as a key for policy instruments to perform successfully. An agency suggested to include training "by default" in new policy measures.

The benefits of interoperability across domains, and particularly interoperability of customs and border control systems were mentioned. Integrated Border Management requires increasing collaboration of all parties involved. Research was also mentioned among the areas needing improvement in the context of border security. An agency noted that research topics should be clearer, projects could be shorter and the allocation of budgets should be rethought. Systematic biometric checks upon entry at external borders against law enforcement information systems, particularly SISI II, were suggested by one agency.

Financial and digital investigations and the use of the internet require further development and implementation of horizontal instruments. Public Private Cooperation and Partnerships were mentioned in this context. Fighting organised crime requires enhanced financial intelligence.an agency proposed that the principles governing information exchange via TFTP/TFTS could be used in relation to organised crime.

Some Member States and agencies considered there was a need for stronger support at EU level in relation with technological development. Technical and financial assistance would be particularly needed in the area of decryption and data transfer. Differing national laws in the area of information exchange were perceived as strong constraints.

Overall, enhancing operational cooperation, inter sectorial cooperation, coordination and intelligence sharing (at both EU and international levels), streamlining and strengthening of existing legal frameworks and operational processes as well as overcoming existing boundaries between different EU and national institutions in the field of security were seen as essential by agencies and Member States to face the evolving nature of security challenges.

Strategic approaches, legal frameworks, the use of new technologies for monitoring and surveillance purposes, investment in the utilisation of forensic intelligence and the development of instruments for the systematic monitoring of Darknet markets and capacity building were considered to be beneficial. Moreover, the enhanced criminal use of new technologies requires providing law enforcement with the necessary powers and procedures to ensure security for the EU and its citizens.

Issues related to criminal finances, money laundering and asset recovery would benefit strongly from strengthened operational cooperation and legislative response.

In the area of cybercrime, most Member States agreed that closer collaboration with the industry and external players is necessary. Obtaining information from international communication service providers (social media platforms) is a challenge in a cybercrime investigation and Mutual Legal Assistance is too slow.

However, most of the Member States stressed that no new EU measures would be needed, but rather the full implementation should be pursued. More policy coherence could also be achieved, as noted by some agencies. The need for new legislative changes should be assessed in due time.

There were a few suggestions for legislative measures though, aiming at the harmonisation of law on securing e-evidence and remote access of law enforcement agencies to data or computer systems located outside of the country. A legal assistance model, matching the speed necessary for countering cross-border cybercrime would also be needed. In terms of electronic data retention, common standards and minimal requirements are demanded.

An agency suggested that the EU could consider developing mechanisms for the exchange of machine readable intelligence, potentially derived from big data techniques applied both locally and across networks.

The importance of electronic evidence and encryption, and the need to improve the access to the data required to be used as evidence was highlighted. The usage of encrypted communication by terrorists was mentioned as a major challenge, calling, as suggested by an agency, for a common approach by Member States and EU actors in order to change the paradigm in criminal investigations and in legal national frameworks. Further action is also needed to combat financing of terrorism, and data related to intra-EU financial transactions should be better accessed.

Some Member States point out the importance of the work in the area of trafficking in human beings and the necessity for more multidisciplinary training in this context. The involvement of businesses and NGOs would be important to tackle trafficking in human beings. Dialogues in priority countries, capacity building and close collaboration with local organisations are also important steps. Furthermore, work on modern slavery and wider forms of exploitation should be enforced according to one Member State. In the area of illegal immigrant smuggling, access to the Internal Security Fund for Eurojust for the benefit of the judicial authorities of the Member States is suggested by one agency.

A few Member States asked for more involvement of JHA actors in the decision-making process and planning process of CSDP missions both on the civilian and military side. Further development in the exchange of information between EU CSDP missions and Europol is welcomed.

Cooperation with third countries is widely welcomed by Member States and also agencies to improve the security situation and combat serious crime and terrorism. Sharing of knowledge and good practices on border security with African countries is envisaged to be beneficial by one agency. The Western Balkans are mentioned as a region of particular concern in the area of serious and organised crime as well as trafficking of weapons. Some Member States asked for further action at EU level for the trafficking of weapons in general.

A limited number of Member States called for a more unified and joint approach on foreign fighters coming from Syria and Iraq. In this regard the detection of travel movements, cooperation in criminal justice and gathering evidence, and the security risks and needs of children are the main concerns.

Work on PNR was a top priority for several Member States.

In the context of radicalisation and deradicalisation, the role of the Commission could be strengthened by enhancing cooperation through RAN Centre of Excellence. The detection of online-material propaganda, the monitoring of social media in cooperation with the private sector takes an important part in the fight against extremism and radicalisation. The development of a common terminology is considered to be useful.

On a general note, impact analysis and assessment as well as evidence-based policy is repeatedly part of the Member States' replies to this question.

Many respondents noted that the dynamic challenges in the field of security require a long-term but responsive strategy based on reliable data and a comprehensive approach including fundamental rights-oriented policies. Furthermore, promoting the values of tolerance, diversity and mutual respect in the dynamic communication and information environment to

enhance security, together with supporting the role of the civil society, should be part of the approach.