EUROPEAN
COMMISSION

Brussels, 9.7.2020
SWD(2020) 135 final

PART 1/2

# COMMISSION STAFF WORKING DOCUMENT

## Implementation of Home Affairs legislation in the field of internal security - 2017-2020

# INTRODUCTION

1. This document takes stock of the **implementation of Home Affairs legislation in the internal security field,** building upon the findings of the Comprehensive Assessment of EU Security Policy of July 2017[1].

The strategic framework in place during the period considered was set in the context of the Agenda on Security[2] as presented by the Commission in 2015. This overview focuses on four main fields of EU action in the area of internal security which are the key areas of EU action under that Agenda[3], as analysed in the Comprehensive Assessment: **(I) information exchange and operational cooperation, (II) counter-terrorism and radicalisation, (III) organised crime** and **(IV) cybercrime.**

2. To ensure the relevance, efficiency, coherence and EU added value of relevant activities, security policies and tools at EU-level are **regularly evaluated**. Assessing how the EU's action in the field of security is implemented is particularly necessary as security risks and threats evolve and the EU's response needs to be recurrently updated. The need for regular evaluation, as well as proper and effective implementation of legislation, is a shared institutional priority, frequently recalled notably by the European Parliament.

Furthermore, there is a direct link between security, democratic values, the protection of fundamental rights and the effectiveness of legal guarantees. The regular assessment of Home Affairs legislation and its implementation is necessary with a view to the protection of those values and rights as well as to ensure that citizens are protected effectively from security threats.

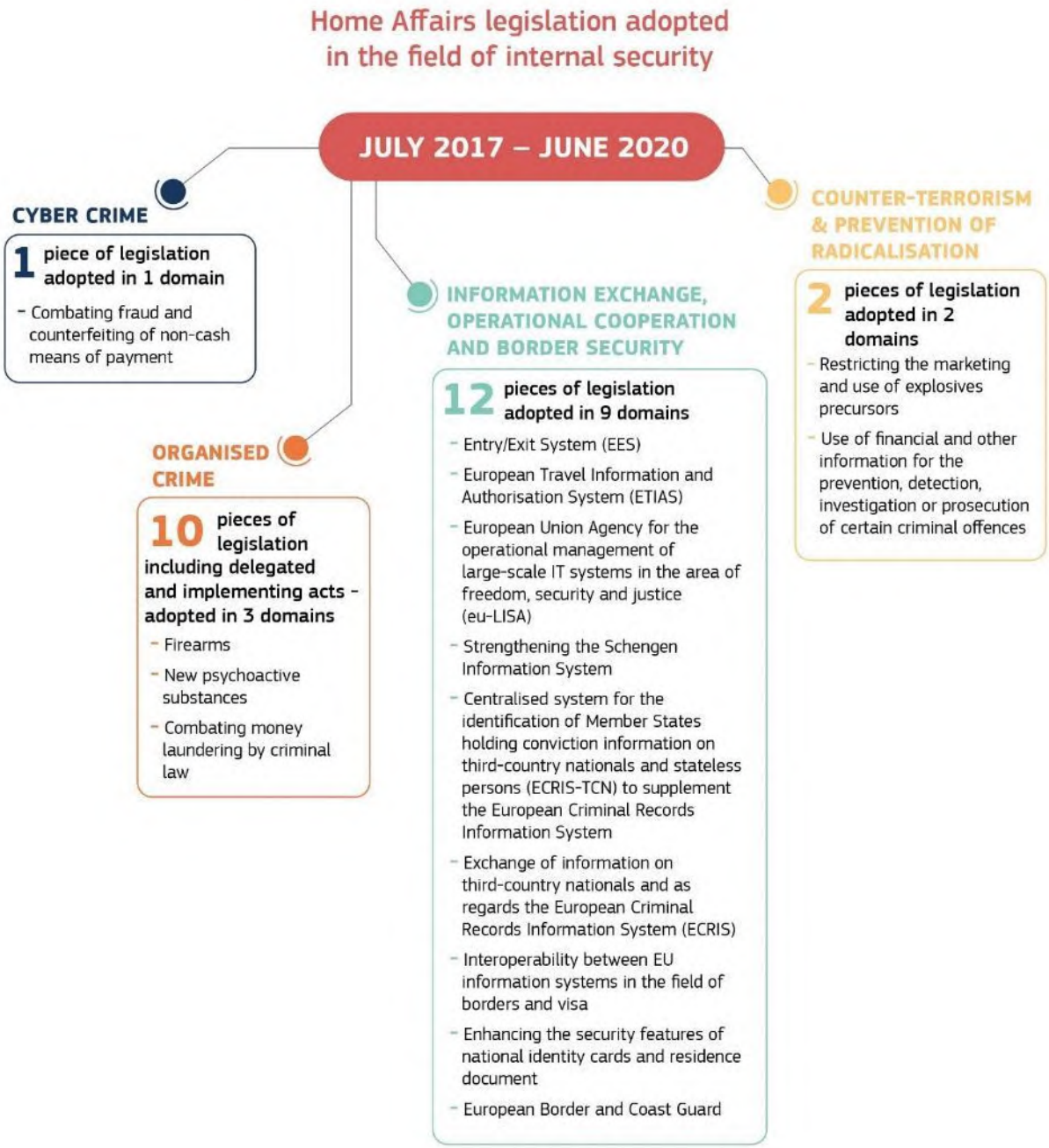
In the focus period of July 2017 to June 2020, 9 evaluations and 10 studies and impact assessments regarding legislative instruments (or proposals thereof) in the field of internal security policy have been carried out while numerous others are underway. These evaluations and studies provide valuable information on the specific instruments they relate to and their implementation. So did the Schengen evaluations carried out in the same period. Under this peer review mechanism, the Commission together with experts from the Member States and Schengen Associated Countries as well as observers from the relevant agencies, verify the quality of the implementation of the Schengen *acquis* which encompasses most of the legislation adopted in the area of Home Affairs (and when not encompassing it, closely relates to it). The present document aims to draw

---

1 Comprehensive Assessment of EU Security Policy, 26.7.2017, SWD (2017) 278.
2 The European Agenda on Security, 28.4.2015, COM (2015) 185 final.
3 This Staff Working Document takes equally into account the evolution of the policy framework - notably as regards the development of an effective and genuine Security Union since 2016 - as well as other relevant policy and institutional developments.

on the results of such evaluations, studies and quality control mechanisms to take stock of the implementation of internal security policies, in a cross cutting way.

3. The Commission has deployed significant means to **support effective and timely transposition and implementation of new Home Affairs legislation** in the internal security field drawing on all available expertise and resources including where appropriate those of Justice and Home Affairs Agencies. Indeed, internal security has



been a top priority for the Commission in the last years, which has conducted to a significant number of policy initiatives being developed in this area. Since 2017, 25[4] legislative instruments have been adopted by the co-legislators in this area many of which have entered into force or are in the process of being transposed. This report refers to numerous technical and legal support actions, including seminars, workshops and training programmes organised by the Commission to support Member States to this effect.

4. As appropriate, this report considers the development of **non-legislative instruments** including standards, codes of conduct and other relevant supporting measures- including "soft law". The European Union indeed mobilises a vast array of non-legislative means in support of Member States' action e.g. through the action of relevant Justice and Home Affairs (JHA) agencies and networks, research and innovation, international cooperation and financing activities. Therefore, while the present working document focusses on the implementation of internal security legislation, it also refers to some of the key non-legislative activities.

5. The Union has provided significant **budgetary and financial means** to support internal security policies under several internal security specific programmes - Internal Security Funds (police and borders and visa), Justice, Hercule III and Fiscalis programmes as well as through the budgets of the relevant agencies such as Europol or CEPOL. These were complemented by several other programmes relevant for internal security, such as the "secure societies" strand of Horizon 2020.

The Internal Security Fund (ISF) is composed of two separate instruments: the instrument for financial support for **police cooperation, preventing and combating crime, and crisis management**[5] (ISF-P) and the instrument for financial support for **external borders and visa**[6] (ISF-BV). The ISF was set up to contribute to ensuring a high level of security in the Union through different means. The police cooperation instrument ISF-P supports crime prevention, combating cross-border, serious and organised crime including terrorism, and reinforcing coordination and cooperation between law enforcement authorities and through enhancing the capacity of Member States and the Union for managing effectively security-related risks and crises. The external borders and visa instrument ISF-BV facilities legitimate travel, through applying a uniform and high level of control of the external borders and the effective processing of Schengen visas.

---

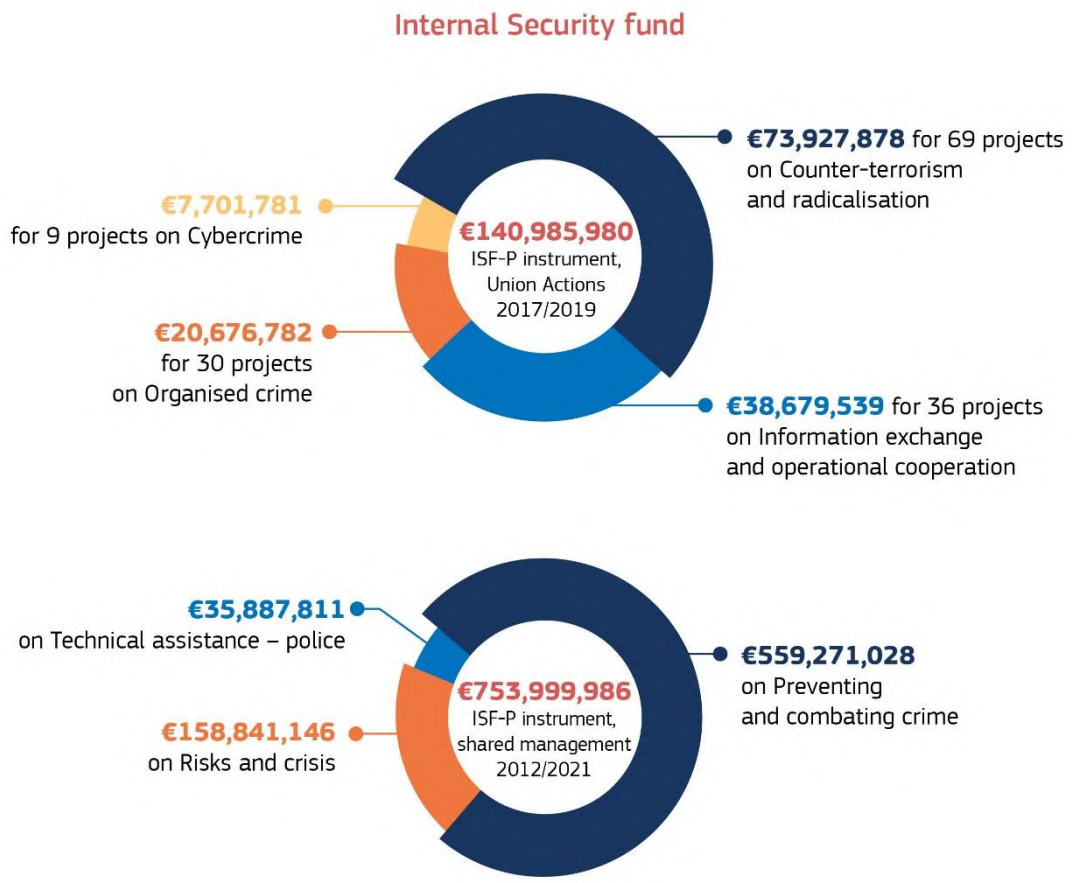
4 Including seven delegated or implementing acts, cf. Annex 1.

5 Regulation (EU) No 513/2014 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.

6 Regulation (EU) No 515/2014 of 16 April 2014 establishing, as part of the Internal Security Fund, the instrument for financial support for external borders and visa and repealing Decision No 574/2007/EC.

The financial resources of ISF-P were initially set at EUR 1 004 million[7] divided into two parts: (i) EUR 662 million to be managed by Member States through national programmes and (ii) EUR 342 million to be managed by the Commission under Union actions and emergency assistance. However, in response to the unforeseen security threats in recent years, this budget was increased through a top-up of EUR 70 million to support Member States in implementing the Passenger Name Record directive and another top-up of EUR 22 million for developing information exchange and interoperability tools bringing the allocation for national programmes up to EUR 754 million[8].

The financial resources of ISF-BV were initially set at EUR 2 760 million[9] divided as follows: (i) EUR 1 551 million for the national programmes of Member States, (ii) EUR 791 million for developing IT systems, based on existing and/or new IT systems, (iii) EUR 154 million for the Special Transit Scheme (for Lithuania) and (iv) EUR 264 million for Union actions and emergency assistance. Emergency assistance has been crucial to address the changing needs caused by the security/migration crisis.

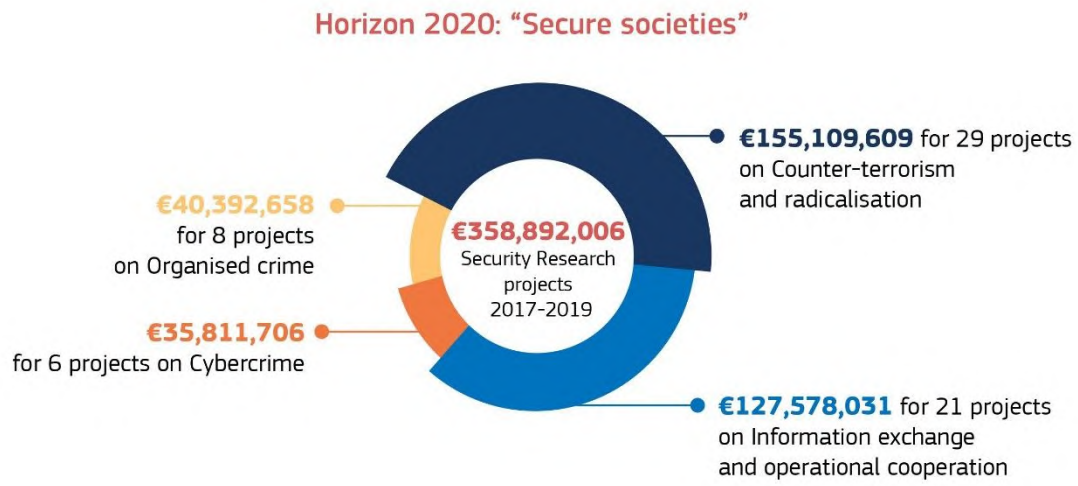



[7] More detail in Annex 3.
[8] More detail in Annex 3.
[9] More detail in Annex 3.

6. EU **Security Research**, funded through the "Secure societies" societal challenge of Horizon 2020 (the current EU Framework Programme for Research and Innovation), is a strategic instrument that significantly contributes to the overall Security Union objectives. Addressing a number of different dimensions, the investment under EU Security Research is supporting innovation in technologies and knowledge crucial for developing capabilities to enable police forces, border guards and first responders to have state of the art tools to do their work today while allowing them to prepare for the new security challenges that will be coming up in the next years. Moreover, EU Security Research also aims to boost the competitiveness of companies and research organisations in the EU civil security sector, thereby strengthening the EU's technology and industrial base in this sector. Compared to other fields, EU funding is of crucial importance to security research since it represents around 50% of all public funding for security research at EU and national level.

Since the inception of security research at EU level in 2007, the EU has contributed more than EUR 2 800 million in funding over 600 projects, supporting all top policy priority areas in the domain of security and delivering in domains such as airport scanners, advanced forensics, tools to deal with online radicalisation, methods for gathering electronic evidence in criminal cases, and technologies for first responders. Future technological trends such as Artificial Intelligence, cognitive systems and data analytics are also constantly addressed through security research projects.

Within the period 2017-2019, EUR 471 million of EU contribution were invested in 87 projects covering five EU Security Research areas, of which 64 projects corresponding to EUR 358 million of EU contribution are contributing to the four security policy areas explicitly referred in this document. The remaining projects and amounts address other security relevant matters such as natural disasters.



## MAIN DEVELOPMENTS

- As regards **Information exchange and operational cooperation** EU agencies' mandates were strengthened, including that of the EU Agency for the operational management of large scale IT systems (eu-LISA). Existing information systems – the Schengen Information System and Passenger Name Records – were reinforced through new regulatory frameworks. Three new systems were launched and were further developed with a view to deployment within the coming two years – the Entry/Exit System, the European Travel Information and Authorisation System and the European Criminal Records Information System for Third Country Nationals. The entry into force of two dedicated regulations will enable achieving full interoperability of EU information systems for borders migration and security by 2023. A new European Border and Coast Guard Regulation extended the Frontex mandate, including on internal security matters.

- On **counter-terrorism,** besides the transposition and implementation of the new Counter Terrorism Directive adopted in March 2017, a Regulation was proposed to prevent the dissemination of terrorist content online. The recommendations made in the Comprehensive Assessment as well as evaluations and external assessments were important to this effect. The EU legal framework to combat and track terrorist financing was reinforced in 2019 with a new Directive facilitating the use of financial information. The EU legal framework for the security of explosives was also strengthened through a new Regulation on marketing and use of explosives precursors.

- *S*everal legislative texts were further implemented **on organised crime**. The 2018 directive on combating money laundering by criminal law provided a harmonised and strengthened response to those offences. The capacities of law enforcement authorities, Asset Recovery Offices and Financial Intelligence Units' to access financial information have been strengthened by the 2019 Directive on the use of financial information to fight serious crime. The fight against firearms trafficking was pursued through the implementation of the 2017 Directive on the control of the acquisition and possession of weapons. As regards the fight against drugs trafficking, a legislative package on new psychoactive substances became fully applicable at the end of 2018.

- In the field of **cybercrime,** the EU cybersecurity strategy – also covering law enforcement aspects and the proposal on combating fraud and counterfeiting of non-cash means of payment was adopted in 2017. In addition, the Commission focused on providing Member States with the necessary support to ensure full transposition of the Directive regarding sexual abuse and sexual exploitation of children and child pornography, and the Directive on attacks against information systems. New legislation was proposed and adopted to combat fraud and counterfeiting of non-cash means of payment. In order to give authorities the right tools to investigate crime in

the digital age, practical measures and legislative proposals were put forward to improve cross-border access to electronic evidence in criminal investigations.

## I. INFORMATION EXCHANGE, OPERATIONAL COOPERATION AND BORDER SECURITY

**Information exchange and operational cooperation** are two pillars of EU action as identified in the European Agenda on Security and key horizontal tools for an effective Security Union.

In a context marked by the foreign terrorist fighters' phenomenon, stakeholders involved in the Comprehensive Assessment highlighted the importance of **security at borders**, and considered the potential of border checks as a means to combat terrorism, fight criminality and address irregular migration. They also insisted on the importance of better implementation, and better coordination of tasks amongst actors (customs, border guards, police, etc.).

In order to further information exchange, the Comprehensive Assessment of July 2017 identified as necessary the interoperability of EU databases. It also called for the simplification and streamlining of the Policy Cycle.

### 1. Transposition and implementation of legislation

#### 1.1. *Overview*

The 27 Schengen evaluations carried out between 2015 and 2019 on the implementation of the Schengen acquis in the field of police cooperation in the 26 Schengen States and Croatia indicate that the evaluated States achieved overall good compliance with the Schengen acquis in the field of police cooperation and law enforcement information exchange. Likewise, the 42 Schengen evaluations carried out in this period on the implementation of the Schengen acquis in the field of the management of the external borders in the 26 Schengen States and Croatia demonstrated that the evaluated States are to a large extent adequately carrying out systematic checks against the relevant data bases on all persons.

While the abovementioned external border Schengen evaluations have found clear progress in the implementation of Council Directive 2004/82/EC on the obligation of carriers to communicate advanced passenger information (API)[10], the ongoing evaluation of the Directive has identified a number of areas for improvement in the field of API.

[10] Information concerning the passengers whom carriers will transport to an authorised border crossing point through which these persons will enter the territory of an Schengen Member State, which carriers are obliged to transmit, by end of check-in, at the request of the authorities responsible for carrying out checks on persons at external borders.

The Commission has started preparing an impact assessment to look into ways to harmonise the way API data is used in the EU, to ensure consistency with new IT systems (notably EES and ETIAS), to facilitate the use of API data for law enforcement purposes and to streamline the use of API data and PNR data.

The 32 Schengen evaluations carried out between 2015 and 2019 on the implementation of the Schengen acquis in the field of SIS in the 26 Schengen States, Croatia and the UK demonstrated that most of the evaluated countries have generally incorporated and integrated well the use of SIS into the working procedures of the competent national authorities.

The evaluations carried out over the reporting period also indicate that, overall, the evaluated countries have already addressed the deficiencies identified or are actively working on remedying them. They also confirmed the importance of the Swiss, Norwegian, Icelandic and United Kingdom's contribution to internal security in the European Union.

### 1.2. *Information systems and interoperability*

At the time of the Comprehensive Assessment, stakeholders noted their overall satisfaction with the tools available at EU level. Yet, among the concerns raised for the full effectiveness of the tools, were the lack of interoperable systems (implying multiple checks by officers on the ground and possibly duplication of information stored), and the limited use by competent authorities of some of the EU instruments, such as the **Prüm decision** and the **Swedish initiative**. The evaluation of the Visa Information System in 2016 also showed a fragmented access to data for law enforcement purposes across Member States.

As a first step towards improving EU information systems, in June 2017, the Commission proposed to strengthen the mandate of the **EU Agency for the operational management of large scale IT systems** (eu-LISA). Eu-LISA's establishing regulation was repealed and replaced by Regulation (EU) 2018/1726 with effect from 11 December 2018. This regulation strengthened the mandate of the Agency and increased its responsibility in finalising the development of new large-scale information systems[11] as well as in the implementation of the interoperability of those systems.

In June 2019, two new regulations on the interoperability of information systems entered into force, with an aim to close information gaps and blind spots.

For example, the interoperability Regulations provided for access by police authorities to limited sets of data on hit no-hit basis, in case law enforcement access is needed for

[11] Entry/Exit System, European Travel Information and Authorisation System and European Criminal Records Information System for Third Country Nationals.

investigation, in order to establish if the data related to given person were registered in one of the connected systems Following the entry into force, the Commission immediately prepared and submitted proposals for the necessary implementing legislation - implementing and delegated acts – to enable the new components to be developed in line with the new and existing systems.

The Commission also launched initiatives to support Member States in the implementation process, including with funding, where needed, and exchanges of expertise and best practice. The implementation process has started with a view to its finalisation and full interoperability of EU information systems by end of 2023. The Commission has started preparing the necessary secondary legislation. eu-LISA has launched the process of developing the technical aspects. Member States are still in the preparatory phases.

Moreover, an expert group has completed a preliminary assessment of the interoperability with customs systems which recommends in particular a linkup of the Schengen Information System and the Europol data system with the customs Import Control System (ICS2) that will be deployed in three phases between 2021 and 2024

### 1.3. *Entry-Exit System*

The Regulation (EU) 2017/2226 establishing **an Entry/Exit System** (EES) was adopted on 20 November 2017, together with targeted amendments to the Schengen Border Code as regards the use of the EES (Regulation (EU) 2017/2225). It entered into force on 29 December 2017. EES, the entry into operation of which is planned for the first half of 2022, will record external border crossing by third country nationals visiting the EU for a short stay, and will thus contribute to the correct implementation of the short stay rule and help preventing identity fraud. The development and the implementation of the EES system has started and is progressing.

### 1.4. *European Travel Information and Authorisation System*

The Regulation (EU) 2018/1240 establishing a **European Travel Information and Authorisation System** (ETIAS) was adopted on 12 September 2018 and entered into force on 9 October 2018. Once in operation, the system will close an information gap by requesting visa exempt third country nationals intending to visit the EU for a short stay to apply for a travel authorisation prior to starting their travel. The Commission has well advanced its work on numerous implementing and delegated acts necessary for adoption before eu-LISA can start system development. The legislator has, however, specified in the ETIAS Regulation (Article 11 of ETIAS) that amendments necessary for the establishment of ETIAS interoperability with other information systems, inducing the corresponding access rights, need to be part of separate legal acts. Without such amendments, ETIAS cannot enter into operation (Article 88 of ETIAS Regulation).

In January 2019, following this legal obligation, the Commission submitted two legislative proposals[12]. The inter-institutional process is ongoing, the Council adopted a negotiation mandate for inter-institutional negotiations in May 2019, the European Parliament has not yet reached that stage. The current planning for entry into operation of ETIAS by the end of 2022, as well as related overall planning for the entry into operation of interoperability components is conditional on the proposals being adopted and entering into force in a timely manner.

### 1.5. *Schengen Information System*

Three new Regulations[13] on the establishment, operation and use of the **Schengen Information System** (SIS) were adopted on 28 November 2018. The new SIS regulations widened the scope of application and functionalities of SIS, as follows:

- new categories of alerts and more possibilities afforded by existing alert categories;
- extension of categories of data in SIS alerts;
- new technical possibilities;
- new biometric capabilities;
- wider access to SIS alerts at national and European level.

The new provisions are being implemented in different phases:

(1) **implementation phase I** (started in late 2019): Europol and members of the teams deployed by the European Border and Coast Guard Agency are allowed to access all categories of alerts in SIS. Europol access in SIS is already fully operational. The European Border and Coast Guard Agency is in the process of rolling out the system to its teams;

(2) **implementation phase II** (to be ready for entry into operation by end 2020): all Member States are able to use the Automated Fingerprint Identification System (AFIS) for searches on the basis of fingerprints in SIS (19 States were already connected at the end of 2019);

---

[12] COM (2019) 4 final and COM (2019) 3 final.

[13] Regulation (EU) 2018/1860 of the European Parliament and of the Council of 28 November 2018 on the use of the Schengen Information System for the return of illegally staying third-country nationals OJ L 312, 7.12.2018, p. 1;Regulation (EU) 2018/1861 of the European Parliament and of the Council of 28 November 2018 on the establishment, operation and use of the Schengen Information System (SIS) in the field of border checks, and amending the Convention implementing the Schengen Agreement, and amending and repealing Regulation (EC) No 1987/2006 OJ L 312, 7.12.2018, p. 14; Regulation (EU) 2018/1862 of the European Parliament and of the Council of 28 November 2018 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 and repealing Council Decision 2007/533/JHA, and repealing Regulation (EC) No 1986/2006 of the European Parliament and of the Council and Commission Decision 2010/261/EU OJ L 312, 7.12.2018, p. 56.

(3) **implementation phase III** (to be ready for entry into operation by end 2021): full implementation of all provisions of the new SIS regulations.

All stakeholders have made significant progress towards achieving implementation of the new SIS regulations in accordance with the defined milestones[14]. No significant implementation shortcomings have been identified so far.

### 1.6. *Visa Information System*

In May 2018, the Commission presented a proposal to strengthen the existing **Visa Information System** (VIS), providing for more thorough background checks on visa applicants and closing information gaps through better information exchange between Member States on long stay documents and their holders, ensuring full interoperability with other EU-wide databases. Inter-institutional negotiations are ongoing. Another aspect of the VIS legislation relates to the access to the Visa Information System for law enforcement purposes[15]. The Schengen evaluations found in a few occurrences that this access was not properly implemented. The Council issued recommendations to remedy such non-compliant deficiencies. The evaluated States took action on this basis and these provisions are now reported to be implemented.

### 1.7. *ECRIS-TCN*

The Regulation (EU) 2019/816 establishing a centralised system for the identification of Member States holding conviction information on third-country nationals and stateless persons (ECRIS-TCN) was adopted on 17 April 2019, together with Directive (EU) 2019/884 amending Framework Decision 2009/315/JHA as regards the exchange of criminal records information on third country nationals via European Criminal Records Information System (ECRIS). They entered into force, respectively, on 11 and 27 June 2019.

ECRIS-TCN is a centralised system that, once in operation, will allow the Member States' central authorities to identify which Member States hold criminal records on the third country nationals or stateless persons being checked. They can then use the existing ECRIS system to address requests for conviction information only to the identified Member States. Also Eurojust, Europol and the EPPO will have access to ECRIS-TCN for fulfilment of their statutory tasks.

The Commission is now in the process of adoption of the implementing acts necessary for implementation and development of the system by eu-LISA. The current planning for entry into operation of ECRIS-TCN by the end of 2022 is conditional on the interrelated acts being adopted and entering into force in a timely manner.

---

[14] See Report on the state of play of preparations for the full implementation of the new legal bases for the Schengen Information System (SIS) - COM(2020) 72 final.

[15] Council Decision 2008/633/JHA (23.6.2008).

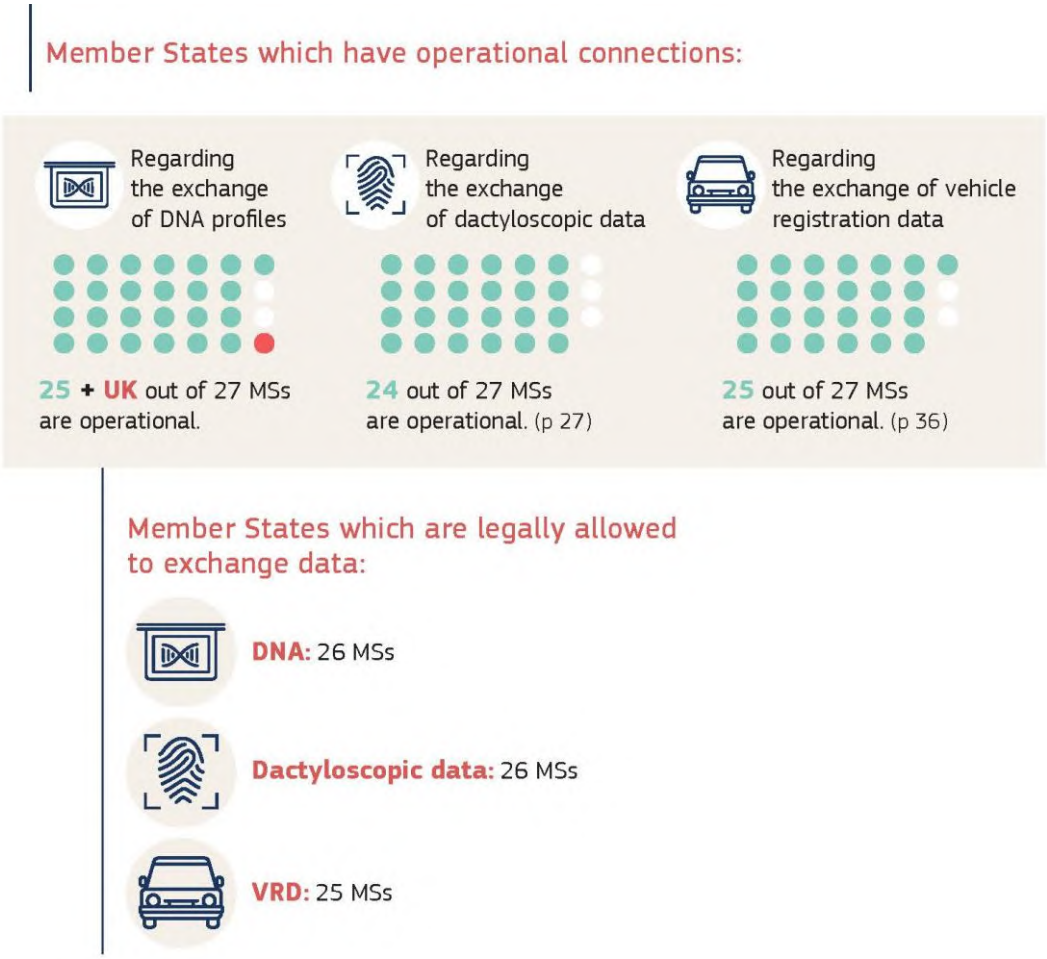
| INFORMATION SYSTEM | AUTHORITIES WITH ACCESS | PURPOSE OF ACCESS | TYPE OF DATA ACCESSIBLE |
|---|---|---|---|
| **Common Identity Repository (Interoperability Regulations)** | Member State police and law enforcement authorities | Identification of third country nationals in the territory of the Member States<br><br>Prevention, detection and investigation of terrorist offences or other serious criminal offences | Identity data, travel document data and biometric data |
| **ECRIS-TCN** | Member States' central authorities, Eurojust, Europol and the EPPO | Judicial cooperation and other legitimate purposes in accordance with national law | Identity data, biometric data and a reference to the Member State holding the criminal records of the third country national |

The existing ECRIS system is operational since 2012 and allows for an electronic and decentralised exchange of criminal records information between the central authorities of the Member States on persons convicted in the EU. The information can be requested for the purpose of criminal proceedings and for any other purposes foreseen by national law. The system not only ensures that the adequate responses can be given to crimes already committed, but also plays an important role in crime prevention. In 2019, the total of 4,2 million of messages have been exchanged via ECRIS, where half of all requests for information concerned other purposes than criminal proceedings. On average, one reply in four reveals previous criminal convictions of the checked person. So far only 8% of requests concerned TCN.

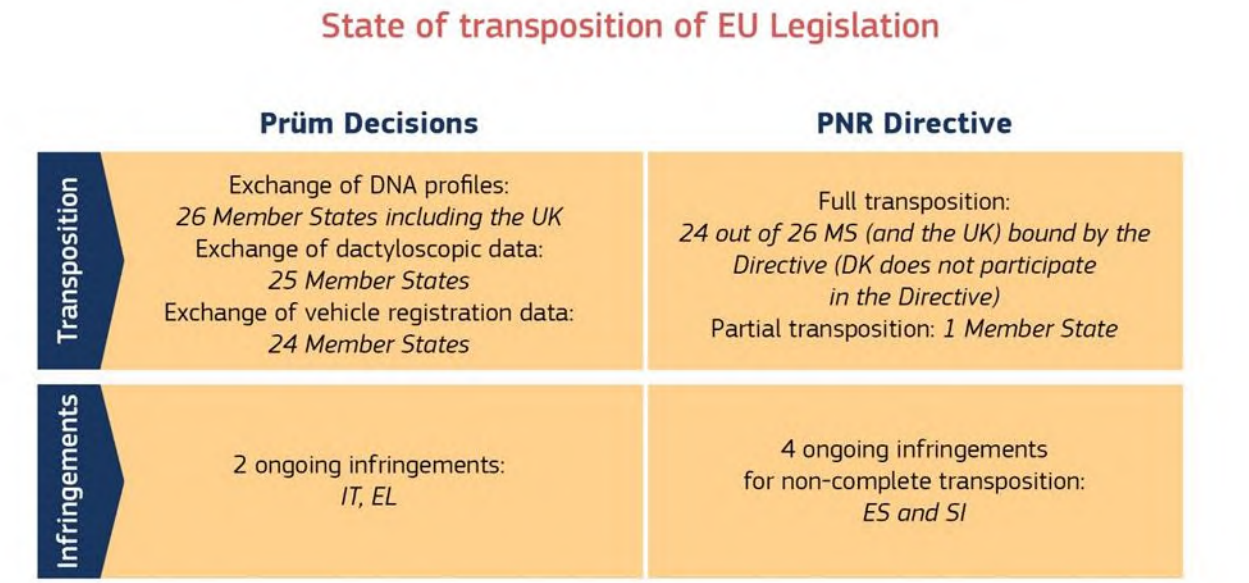
### *1.8. Law enforcement information exchange*

The Comprehensive Assessment confirmed the high value and relevance of the EU tools facilitating law enforcement information exchange, notably the **Prüm Decisions** and the **Swedish Framework Decision**. The Assessment also emphasised the importance of using these instruments to their full potential. The Schengen evaluations conducted in the field of police cooperation found some instances of lack of awareness on the potential of the Swedish Framework Decision. As a result, in such instances, recommendations were made by the Council for improving the level of awareness. The interested evaluated States have all reported adequate remedial actions. In 2017, the Commission conducted a compliance assessment of the Swedish Framework Decision, which confirmed the overall adequate level of application and the practical added-value of the instrument, outlining the short delays in the responses received to requests and the few refusals.

Regarding the implementation of the Prüm Decisions, improvement has taken place since 2017, concerning both the number of participating Member States and the number of bilateral connections set up between the Member States.




In order to assess the possibilities for the improvement of the Prüm decentralised information system, the Commission launched a feasibility study in November 2018.




### *1.9. The Passenger Name Record Directive*

The deadline for the Member States to transpose the Passenger Name Record (PNR) Directive expired on 25 May 2018. The Commission is currently completing the review of the PNR Directive. The review report, accompanied by a staff working document, is scheduled to be adopted in summer 2020. In the meantime, the Commission has completed the compliance assessment of the national measures transposing the Directive in the 23 Member States that had notified full transposition by 10 June 2019. The findings of this assessment point to overall compliance with the Directive. In July 2018, the Commission launched infringement proceedings against 14 Member States that had failed to notify full transposition on time. Eight of these cases have been closed in light of the completeness of the notified measures. The Commission is currently considering further steps in relation to infringement proceedings for non-conform transposition of the Directive.

### *1.10 Schengen Borders Code*

Regulation 2017/458 amended the Schengen Borders Code to oblige Member States to carry out systematic checks against relevant databases on all persons, including those enjoying the right of free movement under EU law (i.e. EU citizens and members of their families who are not EU citizens) when they cross the external borders. The databases against which checks shall be carried out include the Schengen Information System (SIS) and Interpol's database on stolen and lost travel documents (SLTD). The checks aim to enable Member States to verify that those persons do not represent a threat to public policy, internal security or public health. This obligation applies at all external borders (air, sea and land borders), both at entry and exit.

## 2. Broader policy implementation

### 2.1. *Law enforcement cooperation*

**Operational cooperation between Member States** takes place on the basis of EU law and bilateral or multilateral/regional police cooperation agreements between Member


List of the Police Customs Cooperation Centres

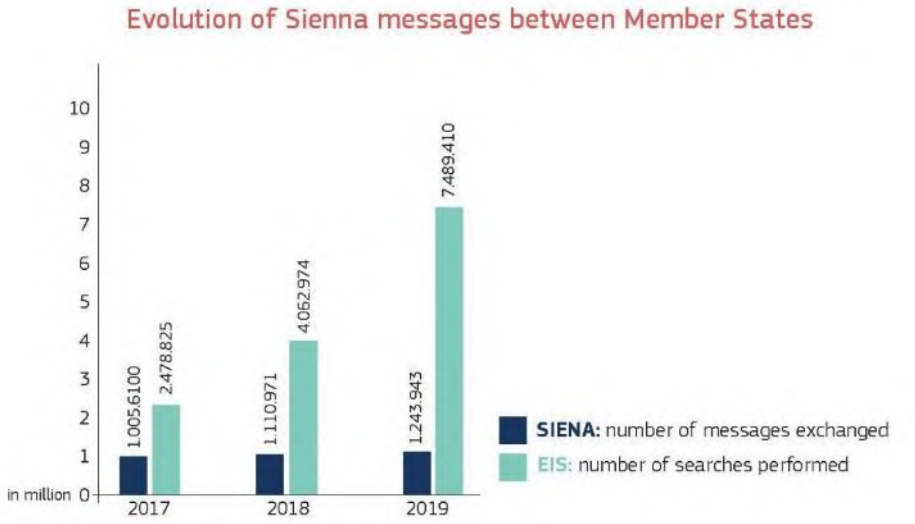
1. Artand
2. Dolno Blace
3. Kjafasan
4. Roszke
5. Barwinek
6. Drasenhofen
7. Kudowa
8. Satoraljaujhely
9. Basel
10. Galati
11. Luxembourg
12. Schaanwald
13. Batrovci
14. Genève
15. Melles Pont du Roy
16. Petrovice/Schwandorf
17. Bijaca
18. Giurgiu
19. Modane
20. Swiecko
21. Budzisko
22. Goch
23. Mohacs
24. Tabanovce
25. Canfranc
26. Gyueshevo
27. Nickelsdorf
28. Thörl-Maglern
29. Castro Marim
30. Heerlen
31. Oradea
32. Tournai
33. Caya
34. Hendaye
35. Padborg
36. Trebinje
37. Cenad
38. Hodonin
39. Passau
40. Trstena
41. Chiasso
42. Jarovce
43. Le Perthus
44. Tuy
45. Chotebuz
46. Kalotina
47. Porubne
48. Ventimiglia
49. Cunovo
50. Plav
51. Portile de Fier
52. Vermice
53. Darmoty
54. Kapitan Andreevo
55. Promachonas
56. Vilar Formoso
57. Dolga Vas
58. Kehl
59. Quintanilha

States, and between Member States and Schengen Associated Countries[16], sometimes with the involvement and support of Europol and Eurojust. EU agencies in the Home Affairs area are essential in supporting Member States to respond more effectively to security challenges. 2017 was the first full year when both Europol and CEPOL operated under their new mandates.

Europol supports cross-border investigations involving at least two Member States and targeting serious and organised crime, terrorism and crime affecting a common interest of the European Union. Europol's work in support of Member States includes producing strategic analyses and supplying evidentially valid analysis supporting cross-border criminal investigations.

Examples of **Europol** Agency's support to Members States in the referenced period include:

- 8266 **operational reports** in 2018 (8280 in 2017) of which 4636 on organised crime, 1837 on counterterrorism, 1033 on financial crime, and 889 on cybercrime;
- support to Member States in **operations** (1748 in 2018;1496 in 2017) with a focus on counter terrorism, followed by cybercrime;
- **mobile office deployment in Member States**, consisting of on-the-spot support deployed to fight migrant smuggling; drug labs to assist in the dismantling of illicit production sites and conduct of technical investigations on drug production equipment; forensic examinations of forged documents and counterfeit currencies; forensic jobs performed related to cybercrime investigations;
- more than 5000 investigations of a growing number of **international criminal groups;**
- facilitation of **bilateral cooperation between Member States**, e.g., through the SIENA system; and.




[16] The active involvement of relevant third countries in priority areas of the Policy Cycle is also pursued.

- maintaining and supporting **cooperation with third countries**[17].

**The European Union Agency for Law Enforcement Training (CEPOL)** focuses its activities on training needs assessment, training coordination, and training of law enforcement officials. Examples of its support in the referenced period include:

- In 2017 CEPOL launched several key initiatives such as the first **pilot EU-Strategic Training Needs Assessment** (EU-STNA). The EU-STNA looks at capability gaps that can be addressed by training on the basis of identified threats. Furthermore, two **pilot CEPOL Knowledge Centres** (CKCs)[18] were established in the priority areas of counter-terrorism and common security and defence policy (CSDP) missions;
- Number of officials trained in 2019: 34 723[19];
- The first **CEPOL European Joint Master Programme** was successfully completed in 2017 and 26 students graduated and received their Master Diploma in October 2017. In parallel, 30 new students were enrolled in the second edition of the Master Programme in 2018. Further to a critical finding of the IAS concerning the procurement procedure, the initiative had to be discontinued; CEPOL is currently considering a possible new programme, fully in line with the provisions in force;
- Strengthen the collaboration between law enforcement officers through its **Exchange Programme** with over 500 exchanges in 2017;
- Following the external audit completed in January 2017, in 2018 CEPOL was certified the Management System Standard ISO 9001:2015 by Lloyd's Register Quality Assurance;
- On 1 January 2018 CEPOL started implementing two external cooperation projects EU/MENA Counter Terrorism Training Partnership 2 (CEPOL CT2) financed by the foreign policy instruments and the Financial Investigation In-Service Training Programme, Western Balkan (CEPOL FI) funded by the Instrument of Pre-Accession Assistance (IPA). The MENA action has a budget of some EUR 6 million and a duration of 36 months; it operates with beneficiaries in the Middle East and North Africa, notably Algeria, Jordan, Lebanon, Morocco, Tunisia and Turkey, aiming to contribute to the international prevention of and fight against terrorism. The Western Balkans initiative had a budget of some EUR 2.5 million, a duration of 24 months and ended in March 2020; the action aimed at developing and sustaining the institutional capacity of the law enforcement agencies of the six beneficiaries in order to prevent, investigate and prosecute transnational organised crime and financing of terrorism;

[17] Although differences in third country data protection regimes pose obstacles to the development of Europol's international cooperation negatively impacting its effectiveness and internal security in the EU.

[18] In the meantime, the CKC on CSDP Missions is no longer operational MSs did not include this activity among their training priorities.

[19] For comparison that number had been 23000 in 2017.

- In 2018 CEPOL signed an agreement with ECBGA/Frontex in order to allow participants exercising border and coast guard duties in the CEPOL Exchange Programme; during that year 49 exchanges were financed by ECBGA/Frontex;
- By the end of December 2018, 98% of the available budget was committed;
- In 2018 CEPOL signed a Working Arrangement with UNODC and the Working Arrangement signed with Serbia in 2017 entered into force; also, the Working Arrangement with the European Network of Forensic Science Institutes was renewed.

On 27 March 2017, the Council decided to maintain the **EU Policy Cycle** for organised and serious international crime also known as "EMPACT"[20] for the period 2018-2021. Driven by EU Member States, with the support of EU institutions, agencies and bodies, and together with relevant third parties, "EMPACT" continued to enable the tailored design of joint operational action plans (OAPs), according to the criminal reality and based on the stakeholders' needs.


While undergoing a continuous streamlining, EMPACT kept delivering noticeable operational results in the fight

[20] EMPACT: European Multidisciplinary Platform A continuation of the EU Policy Cycle for organised 2021 (7704/17).

against organised crime.[21] Beyond the results herewith, based on 2018 activity, EMPACT increased the connection between law enforcement authorities of the Member States. The evaluation pointed out that one of the main added values of EMPACT was to bring people together, to create links between those working in that field. Early information on 2019 performance confirmed those trends. Amongst 2019's operational results, the following can be mentioned: more than 8000 arrests, more than 1400 victims of Trafficking in Human Beings (THB) and online child abuse identified, EUR 400 million in fraud prevented, more than 75 tonnes of drugs and chemicals seized, more than 350,000 cigarettes seized, more than 6,000 weapons & explosives seized and more than EUR 77 million in criminal assets and 1000 bank accounts seized or frozen.

Cooperation between law enforcement in the area of security research is supported through the Secure Societies strand of Horizon 2020. As of 2017, it is funded with a view to strengthen the agencies' capabilities to influence, develop and take up research and innovation that is useful, and thereby help them tackle current and upcoming challenges.

**Presentation of EU decentralised information systems**

| | Prüm Decisions | PNR Directive |
|---|---|---|
| Type of data | Automated exchange of DNA profiles dactyloscopic data vehicle registration data | PNR data, as defined in Annex I to the PNR Directive |
| Right to access | Authorities responsible for the prevention and investigation of criminal offences | Competent authorities, designated by Member States, among national authorities competent for the prevention, detection, investigation and prosecution of terrorist offences and serious crime |
| Purpose | Prevention and investigation of criminal offences | Prevention, detection, investigation and prosecution of terrorist offences and serious crime |

[21] https://www.consilium.europa.eu/en/infographics/fight-against-organised-crime-2018-results/

The Comprehensive Assessment highlighted that the use of **Passenger Name Records (PNR)** is a key part of cooperation with EU strategic partners on the fight against terrorism and serious crime. Following the European Court's Opinion of July 2017[22] on the envisaged PNR agreement between the EU and Canada, a new PNR agreement was negotiated. The agreement's finalisation is pending Canada's legal review[23]. Meanwhile, in August-September 2019, the Commission launched the combined joint review and joint evaluation of the PNR agreement with Australia as well as the joint evaluation of the PNR agreement with the United States. The results of these exercises will be presented to the European Parliament and the Council in the coming months. In addition, on 18 February 2020, the Council authorised the Commission to open negotiations for the conclusion of a PNR agreement with Japan[24]. Negotiations are planned to start still in 2020.

The EU also supported the work carried out by the International Civil Aviation Organisation (ICAO) to develop new international standards on the processing PNR data, in line with United Nations Security Council Resolution 2396 (2017).

### 2.2. *Security dimension of borders*

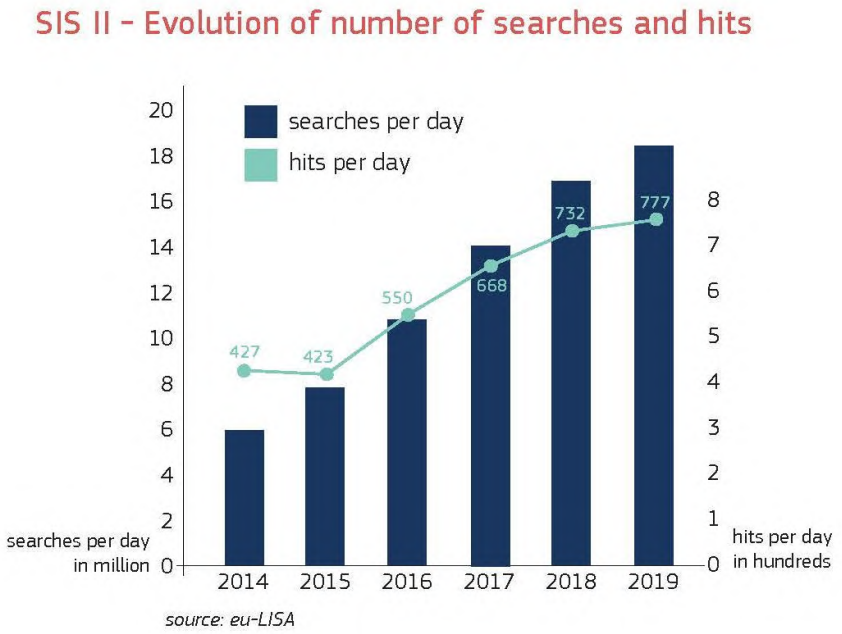
Maintaining a high level of security at the EU's external borders was essential to prevent the undetected movements of criminals and terrorists. The **new European Border and Coast Guard (EBCG) Regulation**[25], which entered into force on 4 December 2019, extended Frontex' mandate and significantly reinforced its financial and human resources. The full and rapid operationalisation of the new Regulation is a top EU priority. In particular, the efficient roll out of the standing corps bringing together the Agency's statutory staff as well as border guards and return experts seconded or deployed by Member States is central in EU action.

Following the evaluation of Regulation 1052/2013 establishing the European Border Surveillance System EUROSUR, this system has been integrated into the functioning of the European Border and Coast Guard. While EUROSUR continued to function as an integrated framework for the exchange of information and for operational cooperation within the European Border and Coast Guard, its scope has been extended from the surveillance of external land and sea borders to border checks at authorised border crossing points and to the surveillance of external air borders. Another novelty introduced by the new EBCG regulation was the possibility for the Agency to share

---

22 Opinion 1/15 of the Court (grand chamber), 26 July 2017.
23 EU-Canada Summit joint declaration, Montreal 17-18 July 2019.
24 Brussels, 4 February 2020, 5378/20.
25 Regulation (EU) 2019/1896 of the European Parliament and of the Council of 13 November 2019 on the European Border and Coast Guard.

operational personal data with law enforcement agencies and Member States law enforcement authorities.




The second generation of SIS (SIS II) became operational on 9 April 2013 in 28 Schengen states[26]. At present, already 30 Schengen states are connected to it[27]. Ireland and Cyprus can be expected to join SIS in the course of 2020 under certain conditions. Nineteen countries connected to SIS have successfully rolled-out the new SIS Automated Fingerprint Identification System (AFIS) at national level. SIS AFIS search functionality provided for a possibility to identify a person on the basis of their fingerprints. Eleven countries plan to roll-out the functionality in the course of 2020.

[26] Schengen states include EU Member States and Schengen Associated Countries that are non-EU Member States (Norway, Switzerland, Iceland and Liechtenstein).

[27] In addition to the 26 countries of the Schengen area, the UK, Bulgaria, Romania and Croatia are connected to SIS. Yet, certain restrictions apply to the UK and Croatia regarding the use of Schengen-wide SIS alerts for the purposes of refusing entry into or stay in the Schengen area.


Security **research and innovation** provided a significant contribution to the implementation of all these policies[28].

Following the adoption of Regulation 2019/1157, it was established that Member States will start issuing identity cards according to minimum common security standards as of August 2021. The regulation determines that security features of identity cards will be aligned with those of passports, as both types of travel documents will contain a highly secure contactless storage medium with the holder's facial image and fingerprints. The format of residence cards issued to third-country family members of EU citizens will be aligned with the existing uniform residence permit. This was intended to reduce criminals' possibility to use forged identity and residence documents whilst safeguarding the rights and freedoms of EU citizens.

The Commission has also negotiated **status agreements** with Albania, Montenegro, Serbia, Bosnia and Herzegovina and North Macedonia, which, once in force, allow for the deployment by Frontex of European Border and Coast Guard teams with executive power on their territory. Executive power may include one or more of the following

[28] Since 2017, through the Secure Societies societal challenge of Horizon 2020, the EU invested about 135 million euros in research related to border security. Research areas include: facilitated and more secure border check systems; improved border surveillance capabilities; automated management of customs checks and of the flows of goods, to secure and facilitate trade; future technology for the operations of the European border and coast guards (including the standing corps of the EBCGA); and fighting high-tech falsified documents. In the meanwhile, investments in border security research of the past decade, including EU-funded ones, contributed to innovations that are now being deployed: from automated border gates in airports to joint maritime border surveillance systems, from equipment for search-and-rescue at sea to technology to predict pressure at borders, to automatic detectors of drugs, weapons and illicit goods.

operational actions: identity control, consultation of databases, authorisation and refusal of entry, stamping of passports, patrolling the border, use of coercive measures including use of service weapons etc. The status agreement with Albania entered into force in May 2019 and a Frontex joint operation took place at its border with Greece.

## II. COUNTER-TERRORISM AND THE PREVENTION OF RADICALISATION

Although the number of terrorist attacks in the EU diminished in 2018 and 2019 as compared to previous years, Europe still faced a continued and evolving terrorism threat[29]. To address all dimensions of that threat, the Union's counterterrorism policy has relied on a wide range of instruments and tools, aiming at preventing terrorism and violent radicalisation, closing the space in which terrorists operate, protecting Europeans and increasing their resilience[30].

### 1. Transposition and implementation of legislation

#### 1.1. *Directive on combatting terrorism*

Horizontal instruments in the area of counter-terrorism, such as the 2017 Directive on combating terrorism[31], provided the EU with a general framework that the stakeholders involved in the Comprehensive Assessment found satisfying. It was, however, pointed out that the EU could benefit from a more extensive use of regular monitoring and assessment of risks and threats.

The Comprehensive Assessment emphasised that EU-wide definitions of terrorist and terrorist-related offences as provided by the 2017 Directive on combating terrorism were of clear added value for enhancing the security of the EU and the safety of EU citizens and people living in the EU.

The 2017 Directive on combating terrorism strengthened the **obligation to exchange information on terrorism** between Member States. The Comprehensive Assessment highlighted significant progress in the volume and quality of information exchanged through the legal provisions coupled with political commitment and increased awareness of the added value of enhanced information exchange among Member States and with EU Agencies. However, there remained room for improvement in the sharing of information with both Europol and Eurojust. The Commission has addressed information exchange issues in the workshops it organised on the transposition of the Directive on combating terrorism. It has also launched an assessment to what extent Member States have taken measures to comply with the information exchange provisions, including to

---

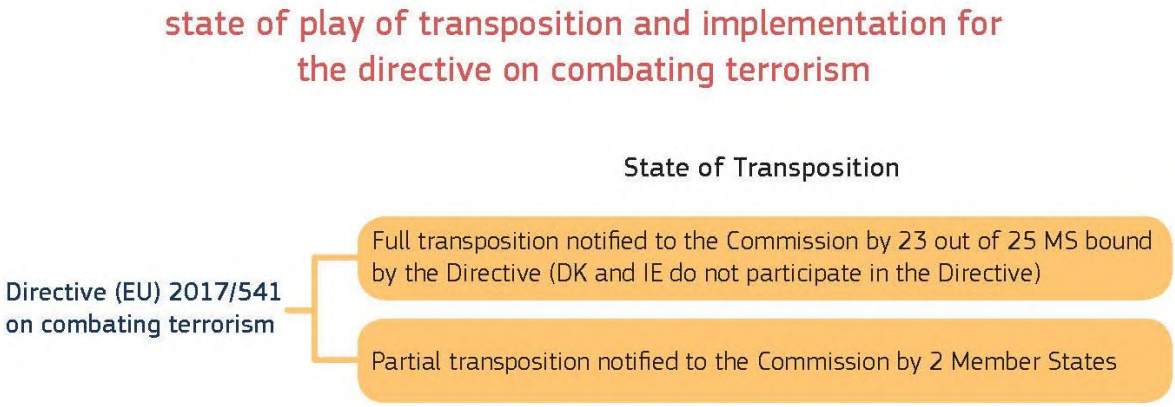
[29] Numbers of terrorist attacks in EU (Europol statistics) in recent years: 205 in 2017, 129 in 2018 and 118 in 2019. Those attacks cost the life of 68 people in 2017, 13 in 2018 and 10 in 2019.

[30] The action on the EU internal side has been accompanied by action and engagement on the EU external action, be it at bilateral or multilateral level. For example, sharing of battlefield information with external partners, such as the USA, was tackled with a view to identify terrorists entering the EU.

[31] 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.

what extent national legislation allows for the spontaneous exchange of information, as emphasised by the European Parliament[32].

The Directive had to be transposed before 8 September 2018, which eight Member States (out of 25 concerned Member States) did before the deadline. In November 2018, the Commission launched infringement procedures against 16 Member States for failing to communicate the adoption of national legislation, which fully transposes the Directive. Since then, an additional 15 Member States have declared the transposition to be complete.




### 1.2. *Explosives precursors Regulations*

The Comprehensive Assessment stressed the importance of the **explosives precursors'** regulation[33] in reducing the amount of explosives precursors available on the market, and enabling early investigations into suspicious incidents involving explosives precursors. In April 2018, the Commission carried out an evaluation of Regulation 98/2013. The evaluation noted that "as of March 2018, all Member States were in compliance with the requirements of the Regulation to set up national contact points (NCPs) for reporting suspicious transactions (Article 9(2)) and to lay down rules on penalties (Article 11)". All Member States have adopted either a prohibition, a registration regime or a licensing regime, or a combination of these options. There are no open infringements on Regulation 98/2013.

The evaluation demonstrated that the Regulation had achieved significant results, but also showed a number of limitations and challenges which were impacting its added

[32] Ibid, preamble.
[33] 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.

value and even aggravating security risks. On the one hand, the existing restrictions did not prevent explosives precursors from being misused for the manufacture of homemade explosives (HMEs), due to a lack of awareness in the supply chain and challenges for economic operators in identifying legitimate users and products falling under the regulation. On the other hand, economic operators were facing a number of obstacles in operating in the EU internal market, due to different regimes throughout the EU. Likewise, the European Parliament stressed that, despite Regulation 98/2013, some terrorists were still obtaining explosives precursors, and that ensuring stricter controls must be a key priority[34]. It also called on the Commission to consider establishing common criteria for licences and facilitating mutual recognition between Member States, and for a stricter monitoring of online purchases.

In August 2019, the EU adopted a new regulation[35], applicable as of February 2021, which tightens the rules on the marketing and use of explosives precursors. It prohibits additional chemicals, abolishes the registration regime, imposes training and awareness-raising obligations on national authorities and economic operators, and establishes certain common criteria for national authorities to consider when issuing a licence. The new regulation also explicitly applies to online marketplaces and obliges them e.g. to report suspicious transactions. In line with the regulation, the Commission started to work on practical guidelines in 2019 to support national authorities, economic operators and online marketplaces with the implementation of the new regulation, to increase awareness of the rules throughout the supply chain, and to help ensure better enforcement of the rules in the online sphere.

### 1.3. *Fight against Terrorism Financing*

The legal framework giving law enforcement access to, and capacity to exploit, financial information for counter-terrorism purposes, including cross-border, has been reinforced with the 2018 revision of the Anti-Money Laundering Directive[36] and the 2019 Directive facilitating the use of financial information[37]. The framework provided better access to information through centralised bank account registers and enhances cooperation between authorities at national and EU level, among other measures. In parallel, the Commission has been supporting the development of effective partnerships with the private sector under the Internal Security Fund (ISF), to ensure the exchange of valuable operational information and to keep apace of the evolution of trends, sources, and methods of terrorism financing.

---

[34] Report on findings and recommendations of the Special Committee on Terrorism (2018/2044(INI)), preamble.

[35] Regulation (EU) 2019/1148 of the European Parliament and the Council of 20 June 2019 on the marketing and use of explosives precursors.

[36] 5th AMLD, Directive (EU) 2015/849 as amended by Directive (EU) 2018/843 (, OJ L 156, 19.6.2018, p. 43.).

[37] Directive (EU) 2019/1153 of the European Parliament and of the Council of 20 June 2019 laying down rules facilitating the use of financial and other information for the prevention, detection, investigation or prosecution of certain criminal offences, and repealing Council Decision 2000/642/JHA.

## 2. Broader policy implementation

### 2.1. *Horizontal counter-terrorism measures*

**Respect for fundamental rights** was an essential part of all legislative initiatives on terrorism. The European Parliament has particularly insisted on that shared priority, calling on the Commission to examine the challenges in relation to fundamental rights that exist in the field of counter-terrorism policies[38].

**Gathering expertise** in cross cutting areas of internal security, particularly as regards risk analysis, multidimensional situation awareness and forecasting, contributed to the EU's information and analytical capability, and provided information and assessments, in particular on threats and vulnerabilities. The focus of situational awareness was on strategic information and assessments with a view to support policy development and implementation in the JHA area, as well as to feed in JHA aspects into other policy areas. EU risk assessment processes played a growing role in the European security landscape, notably in securing means of transport from terrorist attacks.

As regards **international cooperation in the area of counter-terrorism**, an important achievement in the period relates to the EU's engagement in the Western Balkans. A Joint Action Plan on counter-terrorism for the Western Balkans was agreed with six Western Balkan partners in October 2018. The Action Plan provided for a robust, joint framework for countering terrorism and called for ambitious and concrete actions to achieve five counter-terrorism objectives. In addition to the prevention and countering of radicalisation and the protection of citizens, the Action Plan called for effective information exchange and the combatting of terrorist financing. The European Commission has agreed to implement arrangements for tailor-made priority actions with each Western Balkans partner.

### 2.2. *Prevention of radicalisation*

**Preventing radicalisation** was one of the central pillars of the EU's security policy in the referenced period. The Comprehensive Assessment showed that various EU initiatives have laid a solid basis for more effective preventive work, while also identifying scope for improvement. It has underlined the need for a more structured exchange on preventive work among the relevant stakeholders. In terms of **coordination**, it pointed to the possibility of using the full potential of existing instruments and new ones while seeking complementarity and synergies between key stakeholders, initiatives and policy instruments, including on funding. In terms of **outreach**, the assessment suggested reaching out to smaller internet companies whose platforms were used by terrorist organizations and to develop partnerships with civil society actors and creative

[38] Report on findings and recommendations of the Special Committee on Terrorism (2018/2044(INI)), recommendation 6.

communications industry. Finally, in terms of **impact**, the assessment highlighted the need for more evidence-based policies, as well as targeted research and evaluations. It underlined the importance of "staying ahead of the curve" by identifying new trends and developing responses in a more anticipatory manner. The Court of Auditors confirmed those recommendations[39]. Furthermore, the European Parliament called for further developing long-term capacities within the Commission[40].

As to the need for a better **coordination**, the Commission set up in 2017 the High-Level Expert Group on Radicalisation (HLCEG-R), which identified recommendations based on thematic and structural priorities that have laid the ground for future actions at EU level[41]. As a follow-up measure to the main structural recommendation, in 2018, the Commission reinforced its support and coordination capacities in this area.

A "Steering Board on radicalisation"[42] was set up to define yearly Strategic Orientations[43] to be implemented jointly by Member States and the Commission through its main instruments, especially the Radicalisation Awareness Network (RAN). The Strategic Orientations contributed to deliver on the thematic recommendations according to Member States' priorities[44]. New forms of cooperation also helped to swiftly address unexpected challenges, such as the impact of COVID-19 on radicalisation processes and outline further action e.g. to counter the impact of extremist narratives online. To follow-up on the recommendations of the Comprehensive Assessment and the HLCEG-R, as of 2020, the Commission has further increased its coordination and steering role also by doubling the earmarked amount to strengthen the support to policy makers, practitioners and researchers[45]. The Commission also facilitated thematic-based collaborations amongst like-minded Member States (e.g. on prisons, ideologies, the local level etc.)[46]. These enhanced coordination and support activities are an important step towards the

---

39 https://www.eca.europa.eu/en/Pages/DocItem.aspx?did=45801

40 https://www.europarl.europa.eu/doceo/document/A-8-2018-0374_EN.html?redirect, notably rec. 27

41 Key areas identified in the HLCEG-R report are prisons and rehabilitation, communications and online propaganda, local dimension, sharing of knowledge about radicalisation phenomena and radicalisation pathways, ideology and polarisation, education and social inclusion, external dimension. https://ec.europa.eu/transparency/regexpert/index.cfm?do=groupDetail.groupDetailDoc&id=37474&no=1

42 Steering Board for Union actions on preventing and countering radicalisation, https://ec.europa.eu/transparency/regexpert/index.cfm?do=groupDetail.groupDetail&groupID=3626

43 2020 Strategic Orientations on a coordinated EU approach to prevention of radicalisation: https://ec.europa.eu/transparency/regexpert/index.cfm?do=groupDetail.groupDetailDoc&id=39835&no=1

44 For instance, on prisons and reintegration, different work-stands (including dedicated workshops and study visits of Member States and thematic meetings of the RAN) have led to an exchange of practices e.g. on multi-agency collaboration and specialized programmes for radicalized offenders and risk assessment. Via the RAN the Commission has trained not only prison staff, but also police and social and community workers to increase their preparedness. Amongst others, the RAN has drafted a manual on rehabilitation that is about to be published. It provides an overview of key insights and tackling also issues related to family acceptance.

45 Threshold for 2 framework contracts: 61 Mio EUR. The framework contract to support practitioners is already operational, the one targeting policy makers and researchers will be awarded in the course of 2020.

46 Member States have unanimously praised this format in an ad hoc assessment carried out by the Commission in the second half of 2019.

recommended goal to enhance the capacity of the Commission to build, pool and better disseminate expertise and know-how at EU level.

Along with an increased **outreach** to policy makers at national level, the Commission has strengthened also the dialogue with other partners. For instance, the initiative "EU Cities against Radicalisation" offered a platform to support and foster closer cooperation among cities. Communication and dissemination efforts targeted to practitioners have yielded considerable results - the number of RAN social media followers and the RAN website continues to grow in terms of traffic volume and is reaching new users. The Commission also supported efforts by civil society under the Civil Society Empowerment Programme for campaigns providing alternative narratives to terrorist propaganda and promoting fundamental rights and values[47].

Collaboration with the private sector, in particular in the framework of the EU Internet Forum to counter dissemination of terrorist content online has intensified by expanding engagement with numerous small and medium size companies. The Commission was also actively engaging with key partners such as the Global Internet Forum to Counter Terrorism. Work in this area has been complemented by legislative action, with a proposal for a Regulation to prevent the dissemination of terrorist content online[48] presented in 2018, on which negotiations are expected to be concluded in the course of 2020. Regarding the external dimension, the Commission increased its support to priority external partners, especially the Western Balkans[49].

The Commission was also taking a growing role in increasing the **impact** of its actions, building evidence-based knowledge and fostering mutual reinforcement between academia, policy and practice. Projects awarded under EU programmes, particularly Horizon 2020 and the Internal Security Fund were increasingly interconnected. Publicly available information on EU funds covering radicalisation[50] also contributed to achieve impactful actions. As of 2017, the EU has funded several projects within the Secure Societies strand of Horizon 2020 that tackled prevention of radicalisation and that have been regularly providing policy feedback on the matter[51].

---

47 The programme funded initiatives with a total volume of almost EUR 14 million.

48 https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX:52018PC0640

49 The Joint Action Plan on Counter Terrorism for the Western Balkans and the Regional Network of National P-CVE Coordinators (RNNC) provide a solid framework to engage in substantive work on preventing and countering violent extremism in the region. The development of RAN activities in the MENA region is also of particular interest for Member States.

50 https://ec.europa.eu/home-affairs/what-we-do/policies/counter-terrorism/funding-research-projects-radicalisation_en

51 The EU funded projects in that area for a total amount of 18 million EUR. At the beginning of 2020, a new call for proposals is launched that should build up on the results of these projects and ensure continuity of inputs to policy makers. Similarly, 15 million EUR have been invested in the security research projects on terrorist-content online, that provided input for the proposal on Preventing the dissemination of terrorist content online (COM(2018) 640 final), and a new call for proposals is launched in 2020 to ensure continuity of the topic being addressed through security research.

With the abovementioned legislative and policy developments, the Commission has aimed for systematic progress in terms of coordination, outreach and impact and has gradually developed its coordination and knowledge building capacities.

### 2.3. *Tracking terrorist financing*

**Tracking terrorist financing** was necessary to close the space in which terrorists operate. The Comprehensive Assessment acknowledged that, with its 2016 Action Plan for strengthening the fight against terrorist financing[52], the Commission had responded to the evolving challenges of terrorist financing. However, the assessment highlighted the need to ensure the final adoption and full implementation of the legislative and non-legislative instruments developed. Furthermore, the stakeholders involved in the assessment overall called for continued action in this field, in order to ensure that financial information can be used in the area of counter-terrorism, in full respect of fundamental rights.

The **EU-US Terrorist Financing Tracking Programme (TFTP)**, which contains financial transaction data with a link to geographical areas that are particularly at risk of terrorism, remained an effective counter-terrorism tool to provide timely, accurate and reliable information about activities associated with suspected acts of terrorist planning and financing. The Comprehensive Assessment suggested that the competent authorities make better use of the TFTP for counter terrorism investigation, and that Member States provide regular feedback on this tracking program data.

Member States have reported to the Commission that the TFTP has helped to identify and track terrorists and their support networks worldwide, and proved instrumental in moving forward specific investigations relating to terrorist attacks on EU soil. This included the investigations following the terrorist attacks in Stockholm on 7 April 2017, Barcelona on 17 August 2017 and Turku on 18 August 2017, as well as leads relating to several terrorist suspects, including foreign terrorist fighters travelling to or returning from Syria and the support networks facilitating or funding their movements and training.[53]

The TFTP Agreement provided a robust set of controls and safeguards, including an overseer appointed by the EU. The Commission's report on the fifth joint review[54], issued in July 2019, concluded that these controls and safeguards were implemented properly.

---

[52] Communication from the Commission to the European Parliament and the Council COM (2016) 50 final.

[53] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=SWD:2019:301:FIN

[54] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52019DC0342

With the aim of **improving access to financial information through the targeting of transactions by individuals with links to terrorism**, and in line with the recommendations issued by the Special Committee on Terrorism, the Commission has analysed the need for a complementary mechanism to the TFTP that would also cover, for example, intra-EU payments in Euro. The Commission considered the important balance between security and individual freedoms. In a report issued in July 2019[55], it determined that a measure involving the interconnection of the national centralised automated mechanisms on bank accounts, which under the 5th AMLD[56] must be set up in all Member States, would facilitate the cross-border cooperation of the competent authorities involved in the fight against money laundering, terrorist financing and other serious crimes[57].

### 2.4. *Protection against attacks and crisis management*

Ensuring protection and efficient crisis management contributed to improving resilience against attacks. The EU acted to protect against **explosive** and **chemical, biological, radiological and nuclear threats** (CBRN). The assessment showed that increased cooperation at EU level, including partnerships with the private sector, could enhance preparedness in that matter. The 2017 **Action Plan to enhance preparedness against chemical, biological, radiological and nuclear security risks[58]** called for Member States to nominate CBRN Security Coordinators, who form the CBRN Security Advisory Group ensuring the overall coordination of the CBRN policy. Europol continued the development of its CBRN Knowledge Hub. Over the past two years, progress has been made in most of the areas covered by the Action Plan. At the Commission's initiative, a consortium of national experts carried out an **analysis of the gaps in detection equipment** for around 70 different types of CBRN scenarios. The gap analysis report has been shared and discussed with Member States in order to guide future research needs, to inform decision making on detection strategies and devise operational measures to address the identified gaps[59].

Within the scope of the work on **chemical detection** – launched following the foiled 2017 Australia bomb plot – the Commission and interested Member States – developed a list of chemicals of concern. Currently the Commission works with manufacturers in order to see how the related detection equipment performance can be improved.

---

55 https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52019DC0372

56 https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32015L0849

57 Cf Action Plan for a comprehensive Union policy on preventing money laundering and terrorist financing, https://ec.europa.eu/finance/docs/law/200507-anti-money-laundering-terrorism-financing-action-plan_en.pdf

58 COM(2017) 610 final.

59 As a follow-up, the Commission – in cooperation with several Member States – organised a multi cross-border CBRN exercise Quinteto+ with mixed radiological and chemical scenario. It was an excellent opportunity to test information exchange and police cooperation in case of cross-border terrorist threat. Based on the lessons learnt, a guidance material with recommendations for Member States on how to deal with such cases has been released.

Training was an essential part of preparedness-raising. Apart from supporting Member States-led training projects, the Commission has itself organised such training. The **European Nuclear Security Training Centre (EUSECTRA)** in Karlsruhe offered a unique opportunity to train – among others – law enforcement including customs official using actual nuclear materials. In 2019 for the first time, the Commission launched a training campaign for the police officers with the focus on management of a contaminated crime scene.

In addition, **cooperation with third countries**, including through workshops and exchange of practices, has proved useful[60].

Since 2017, relevant **security research** has been undertaken through the Secure Societies societal challenge of Horizon 2020. Examples of actions in support of first responder operations, with effect on enhanced coordination among civil protection, police and military forces, enabled the development of integrated and adaptive responses to toxic emergencies in case of a CBRN incident or terrorist attack. In addition, CBRN-related actions contributed to the implementation of the Internal Security Strategy (in particular for disasters linked to terrorism) and of the CBRN Action Plan[61].

The all-hazards European Programme for **Critical Infrastructure Protection** (EPCIP)[62] consists of several pillars, including the European Critical Infrastructure (ECI) Directive (2008/114)[63]. Further to the findings of the Comprehensive Assessment of EU Security Policy and the recommendations[64] of the European Parliament's Special Committee on terrorism, which called inter alia for the revision of the ECI Directive, the Commission evaluated the ECI Directive in 2019. Although the evaluation[65] found that the Directive

---

60 These include in particular: the United States (workshop on Joint Criminal-Epidemiological investigation organised in cooperation with the Federal Bureau of Investigation and Centre for Disease Control and Prevention; workshop on security of radioactive sources organised in cooperation with the Office for Radiological Security of the Department of Energy; various agencies involved in the work on chemical threat) and Israel (two workshops in 2018 and 2019 as well as interactions in the context of the EU CBRN Centres of Excellence which cover more than 60 third countries.

61 Research focused on solutions, methods, tools covering different types of (natural or man-made) disasters and related resilience and security issues, the objectives of which were to reduce the loss of human life, environmental, economic and material damage, including from extreme weather events, crime and terrorism threats. Research inputs in this area directly or indirectly contributed to the implementation of international (e.g. the Sendai Framework for Disaster Risk Reduction) and EU Disaster Risk Reduction policies tackling natural and man-made threats (either accidental or intentional), in particular the Union Civil Protection Mechanism (UCPM).

62 Communication from the Commission on a European Programme for Critical Infrastructure Protection (COM (2006) 786 final), revised by Commission Staff Working Document on a new approach to the EPCIP - Making European Critical Infrastructures more secure (SWD (2013) 318 final).

63 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.

64 report on findings and recommendations of the Special Committee on Terrorism (2018/2044(INI)) recommendation 174:

65 SWD (2019) 310 final.

had brought overall added value, it revealed some deficiencies as well as the need to address new and evolving threats and align the critical infrastructure protection policy with the Network and Information Systems (NIS) Directive and other sectoral measures. The deficiencies included the limited sectoral scope (only covering transport and energy), the lack of focus on resilience and interdependencies, and the heterogeneous approach of Member States in designating European critical infrastructures. In November 2019, the Commission launched a feasibility study aimed at identifying possible options to enhance the EU critical infrastructure protection policy, which is due to be completed in summer 2020. A legislative proposal on additional measures for critical infrastructure protection is part of the Commission Work Programme 2020.

Significant results were achieved in the research and innovation on critical infrastructures under the Secure Societies strand of Horizon 2020.[66]

In order to ensure an efficient **protection of public spaces**, the assessment suggested raising awareness and fostering cooperation at EU level, and called for a comprehensive approach including a risk assessment methodology, taking into account insider threats, detection capacity, citizen training, public awareness, as well as engagement with private stakeholders. The 2017 Action Plan to support the protection of public spaces[67] aimed to support Member States' law enforcement authorities and local authorities in enhancing the protection of public spaces through dedicated funding, fostering the exchange of best practice through networks and providing guidance material. Different fora served to support the communication and cooperation with the stakeholders. Under the Urban Agenda for the EU, a partnership on security in public spaces has been set up for cooperation with local and regional authorities. Good practices have been collected and laid down in a Commission Staff Working Document to support the protection of public spaces.[68]

Places of worship with their symbolic value were a particularly vulnerable target, thus the Commission took steps to support the protection of these sites by fostering the exchange between different faith associations and Member States as well as by providing funding.

---

66 The EU has allocated funding of around 91 million EUR for projects enhancing the protection of infrastructures. Areas of research included combined cyber and physical threats, improved and fast response to incident and better information sharing. Specific attention has been dedicated to emerging threats and technologically complex scenarios, like combined attacks making use of digital instruments, Unmanned Aircrafts Systems or insiders. Security research on protection has ensured a close collaboration between the different actors, most notably between operators, security authorities as well as industry and academia. Knowledge and results created in projects are also used for the preparation of the upcoming proposal for additional measures on Critical Infrastructure Protection.

67 COM (2017) 612 final.

68 SWD (2019) 140 final.

Research projects under Horizon 2020 were contributing to the objectives defined in the Action plan to support the protection of public spaces[69].

The EU has been making significant investments in security research projects in this area for years, and the output of these projects was regularly taken into consideration in legislative and policy developments, such as the impact assessment of the Regulation on the marketing and use of explosives precursors.[70]

As regards **Crisis Management** the conduct of exercises reinforced the interaction and synchronisation among the crisis mechanism among the Member States and the Union's institutional actors. An example of best practices in the field were the PACE exercises jointly conducted with NATO in 2017 and 2018[71], were designed to address hybrid security threats. However, there is more room for improvements in future similar exercises, particularly throughout strengthened cooperation, coordination and exchange of information with NATO.

[69] Under a Secure Societies topic specifically dedicated the challenge of protecting public spaces in Horizon 2020, 16 million EUR were allocated in 2019 with an aim of addressing cyber-physical threats to public spaces and provide tools for faster identification of dangerous situations and well as supporting efficient response.

[70] SWD (2018) 104 final.

[71] As stated in the 08.07.2016 Joint Declaration by the President of the European Council, the President of the European Commission, and the Secretary General of the NATO cooperation on exercises, among other areas is a strategic priority. Based on that priority Paralleled and Coordinated Exercises took place during 2017 and 2018.

## III. ORGANISED CRIME

Stakeholders consulted in 2017 identified **organised crime** as an important threat to security in the European Union, bearing major human, social and economic costs, and requiring a comprehensive approach on EU level. However, the Comprehensive Assessment showed that EU actions so far were crime-specific (commodity approach), rather than tackling this phenomenon in a comprehensive way. It stressed the need for a more horizontal approach.

### 1. Transposition and implementation of legislation

#### *1.1. Framework Decision 2008/841 on the fight against organised crime*

In terms of horizontal instruments against organised crime, the Comprehensive Assessment in 2017 showed that the legal standards of Framework Decision 2008/841 on the fight against organised crime[72] appeared quite low. It considered that one possibility would be for the EU to focus on a **more intensive use of soft law measures** to assist Member States in implementing existing EU laws, such as the framework Decision.

With the objective of supporting Member States in **fully implementing framework Decision 2008/841 on the fight against organised crime** and exploiting its full potential, the Commission has engaged in discussions with Member States on the way they implement it, including regarding the definition of the term "criminal organisation". In September 2019, the Commission organised a meeting with Member States' experts on this topic. A majority of participants called for an EU strategy on organised crime. Many also stressed that one of the main challenges in cross-border investigations is a lack of harmonisation of the offence of participation or membership in a criminal investigation. The Commission has started an assessment implementation of the Framework Decision in the context of an external study. The Commission also supported Member States' efforts in the fight against organised crime in a variety of ways, for example through financial support for operational projects to tackle serious and organised crime groups in cross-border settings or via dedicated funding proposals for certain crime priorities such as organised property crime.[73]

[72] Council Framework Decision 2008/841/JHA of 24 October 2008 on the fight against organised crime.

[73] Calls on organised property crime were published in the ISF-P Annual Work Programme 2017 and 2019. Direct grants have been awarded under the ISF-P Annual Work Programme 2017 for the Anti-Money Laundering Operational Network (AMON) and for the @ON Network on mafia-type organised crime groups.

### *1.2. Directive 2018/1673 on combating money laundering by criminal law*[74]

This 2018 Directive complemented the preventive framework on anti-money-laundering established by the 4th Anti-Money Laundering Directive[75] and by the 5th Anti-Money Laundering Directive[76]. It did so by harmonising the definition of the criminal offence of money laundering and related penalties for money laundering, ensuring that dangerous criminals and terrorists face equally severe penalties for their crimes across the whole EU. The crime was defined comprehensively, covering all serious crimes, at least those defined in EU law, including cybercrime. The Directive set out a maximum term of imprisonment of at least four years, which can be extended in aggravating circumstances, and introduced liability of legal persons. Furthermore, under this Directive, Member States must ensure the availability of effective investigative tools for the investigation and prosecution of money laundering offences. This strengthened the criminal response to money laundering aimed to cut off sources of finance as well as counter the financial incentives that drive crime. The Directive entered into force in December 2018 and Member States have until December 2020 to transpose it.

### *1.3. Directive 2019/1153 on the use of financial information to fight serious crimes*[77]

This Directive was adopted in July 2019 and granted law enforcement authorities and Asset Recovery Offices direct access to the national centralised bank account registries for the purposes of fighting serious crime. The Directive also aimed to improve cooperation between law enforcement authorities and Financial Intelligence Units (FIUs), and to facilitate the exchange of information between FIUs. Member States are obliged to transpose the provisions of the Directive in national law by August 2021.

In 2019, the European Commission issued a staff working document analysing Member States' non-conviction based confiscation regimes[78]. This analysis followed the call by the European Parliament and the Council to analyse the feasibility and possible benefits

---

74 Directive (EU) 2018/1673 of the European Parliament and of the Council of 23 October 2018 on combating money laundering by criminal law; PE/30/2018/REV/1; OJ L 284, 12.11.2018, p. 22.

75 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, amending Regulation (EU) No 648/2012 of the European Parliament and of the Council, and repealing Directive 2005/60/EC of the European Parliament and of the Council and Commission Directive 2006/70/EC, OJ L 141, 5.6.2015, p. 73.

76 Directive (EU) 2018/843 of the European Parliament and of the Council of 30 May 2018 amending Directive (EU) 2015/849 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, and amending Directives 2009/138/EC and 2013/36/EU, OJ L 156, 19.6.2018, p. 43.

77 Directive (EU) 2019/1153 of the European Parliament and of the Council of 20 June 2019 laying down rules facilitating the use of financial and other information for the prevention, detection, investigation or prosecution of certain criminal offences, and repealing Council Decision 2000/642/JHA, OJ L 186, 11.7.2019, p. 122.

78 SWD (2019) 1050.

of introducing further common rules on the confiscation of property deriving from criminal activities in the absence of a conviction of a specific person or persons for these activities[79].

In 2018/2019 the Commission carried out its assessment of the implementation of Directive 2014/42/EU on the freezing and confiscation of instrumentalities and proceeds of crime[80]. Based on the assessment, reasoned opinions for the failure to communicate transposing measures were sent to three Member States.[81] The results of the assessment have fed into the Commission's report on **asset recovery and confiscation**: ensuring that crime does not pay, which was adopted on 2 June 2020[82]. The report also followed the Commission staff working document on the analysis of non-conviction based confiscation[83]. It also provided the formal reply of the Commission to the co-legislators concerning their request[84] to analyse the feasibility and possible benefits of introducing additional common rules on non-conviction-based confiscation. In addition, the Commission has launched further analysis of asset recovery in the context of an external study that should be finalised mid-2020.

### *1.4 The Directive on the control of the acquisition and possession of weapons[85]*

This Directive was adopted in May 2017 and the deadline for its transposition expired on 14 September 2018. On 25 July 2019, the Commission sent reasoned opinions to 20 Member States for failing to notify full transposition of the Directive. So far, 17 Member States notified full transposition[86].

The Commission adopted on 5 March 2018 the Implementing Regulation on **deactivation standards and techniques** for ensuring that deactivated firearms are rendered irreversibly inoperable. On 16 January 2019, the Commission adopted the related Implementing Directive and Delegated regulation. This Implementing Directive established technical specifications for the marking of firearms and their essential components laying down technical specifications for alarm and signal weapons and blank-firing guns. The Delegated Regulation laid down the detailed arrangements for the

---

79 Council doc. 7329/1/14 REV 1 ADD 1.

80 Directive 2014/42/EU of the European Parliament and of the Council of 3 April 2014 on the freezing and confiscation of instrumentalities and proceeds of crime in the European Union, OJ L 127, 29.4.2014, p. 39.

81 Luxembourg, Romania, Bulgaria.

82 COM(2020) 217 final of 2.6.2020

83 Commission Staff Working Document 'Analysis of non-conviction based confiscation measures in the European Union', 12.4.2019 SWD(2019) 1050 final.

84 Council doc. 7329/1/14 REV 1 ADD 1.

85 Directive 2017/853.

86 Austria, Bulgaria, Germany, Denmark, Ireland, Greece, Estonia, France, Croatia, Italy, Latvia, Lithuania, Malta, Netherlands, Portugal, Romania, Finland.

systematic exchange, by electronic means, of information relating to the transfer of firearms within the Union in the Internal Market Information System.

In December 2017, the Commission adopted a report on the evaluation of the application of Regulation (EU) No 258/2012 on **import and export of firearms**[87]. The evaluation concluded that the Regulation had broadly achieved its assigned goals, but that it faced a number of challenges. Those challenges were notably related to unsatisfactory exchanges of information between national authorities when granting export authorisations, unclear provisions (notably with respect to the use of a single procedure for exports of both military and civilian firearms) and outdated definitions. In April 2018, the Commission adopted a Recommendation, which calls for strengthening of the European Union rules to improve traceability and the security of export and import control procedures of firearms and the cooperation between authorities in the fight against firearms trafficking[88].

### *1.5. Legislative package on new psychoactive substances*

On the basis of a new Commission proposal, the **legislative package on new psychoactive substances** (NPS) was adopted in autumn 2017 by the co-legislators. The legislation[89] entered into force in November 2017, and became fully applicable in November 2018. The majority of Member States took the necessary measures to transpose the Directive. However, letters of formal notice were sent to 11 Member States in January 2019 and, on 2 July 2020, reasoned opinions were sent to 4 of these. In application of the transitional provisions of the new legislation, a delegated act[90] was adopted to include the substances, which were put under control at the proposal of the European Commission between the adoption of the legislation and its full applicability[91], into the annex of the revised Council Framework Decision.

---

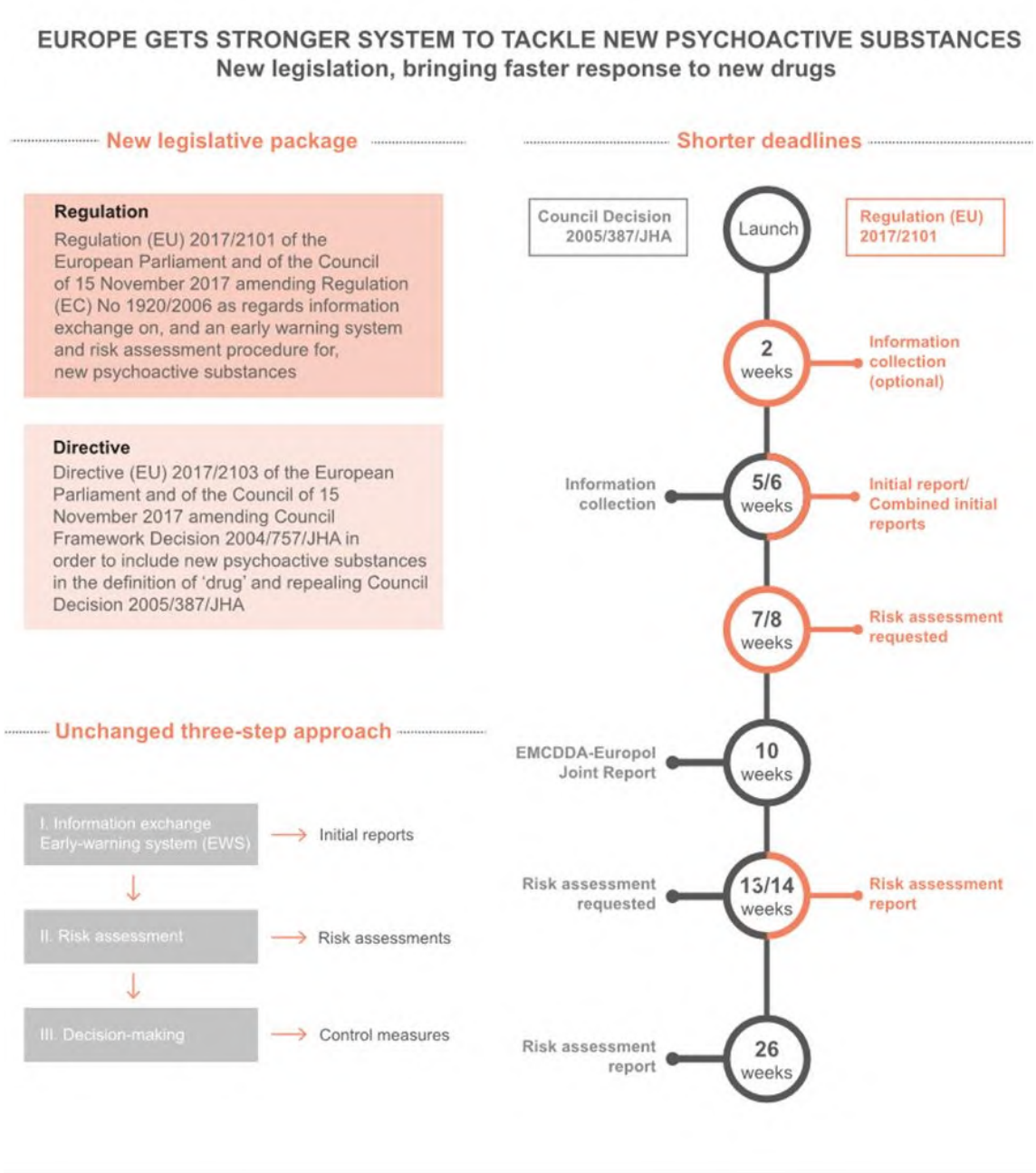
87 COM(2017) 737 final, 12.12.2017.

88 C(2018) 2197 final, 17.4.2018.

89 Regulation (EU) 2017/2101 of the European Parliament and of the Council of 15 November 2017 amending Regulation (EC) No 1920/2006 as regards information exchange on, and an early warning system and risk assessment procedure for, new psychoactive substances, OJ L 305, 21.11.2017, p. 1; Directive (EU) 2017/2103 of the European Parliament and of the Council of 15 November 2017 amending Council Framework Decision 2004/757/JHA in order to include new psychoactive substances in the definition of 'drug' and repealing Council Decision 2005/387/JHA, OJ L 305, 21.11.2017, p. 12.

90 Commission Delegated Directive (EU) 2019/369 of 13 December 2018 amending the Annex to Council Framework Decision 2004/757/JHA as regards the inclusion of new psychoactive substances in the definition of 'drug', OJ L 66, 7.3.2019, p. 3.

91 This concerns the following substances and acts: Furanylfentanyl (Council Implementing Decision (EU) 2017/2170 of 15 November 2017 on subjecting *N*-phenyl-*N*-[1-(2-phenylethyl)piperidin-4-yl]furan-2-carboxamide (furanylfentanyl) to control measures; OJ L 306, 22.11.2017, p. 19); ADB-CHMINACA (Council Implementing Decision (EU) 2018/747 of 14 May 2018 on subjecting the new psychoactive substance *N*-(1-amino-3,3-dimethyl-1-oxobutan-2-yl)-1-(cyclohexylmethyl)-1*H*-indazole-3-carboxamide (ADB-CHMINACA) to control measures; OJ L 125, 22.5.2018, p. 8); CUMYL-4CN-BINACA (Council Implementing Decision (EU) 2018/748 of 14 May 2018 on subjecting the new psychoactive substance 1-(4-cyanobutyl)-*N*-(2-phenylpropan-2-yl)-1*H*-indazole-3-carboxamide (CUMYL-4CN-BINACA) to control measures; OJ L 125, 22.5.2018, p.10); cyclopropylfentanyl and




## 2. Broader policy implementation

### *2.1. Horizontal measures against organised crime*

Since 2016, the Commission has increased its support for the **European Crime Prevention Network** (EUCPN) to increase the network's output. The EUCPN has aligned its activities with the EU Policy Cycle and actively contributed to Operational

methoxyacetylfentanyl (Council Implementing Decision (EU) 2018/463 of 28 September 2018 on subjecting the new psychoactive substances *N*-phenyl-*N*-[1-(2-phenylethyl)piperidin-4-yl]cyclopropanecarboxamide (cyclopropylfentanyl) and 2-methoxy-*N*-phenyl-*N*-[1-(2-phenylethyl)piperidin-4-yl] acetamide (methoxyacetylfentanyl) to control measures; OJ L 245, 1.10.2018, p.9).

Actions in the crime priorities Organised Property Crime, Trafficking in Human Beings, Child Sexual Exploitation and Environmental Crime. The Commission has launched an evaluation of the EUCPN in 2019 with results expected at the end of 2020.

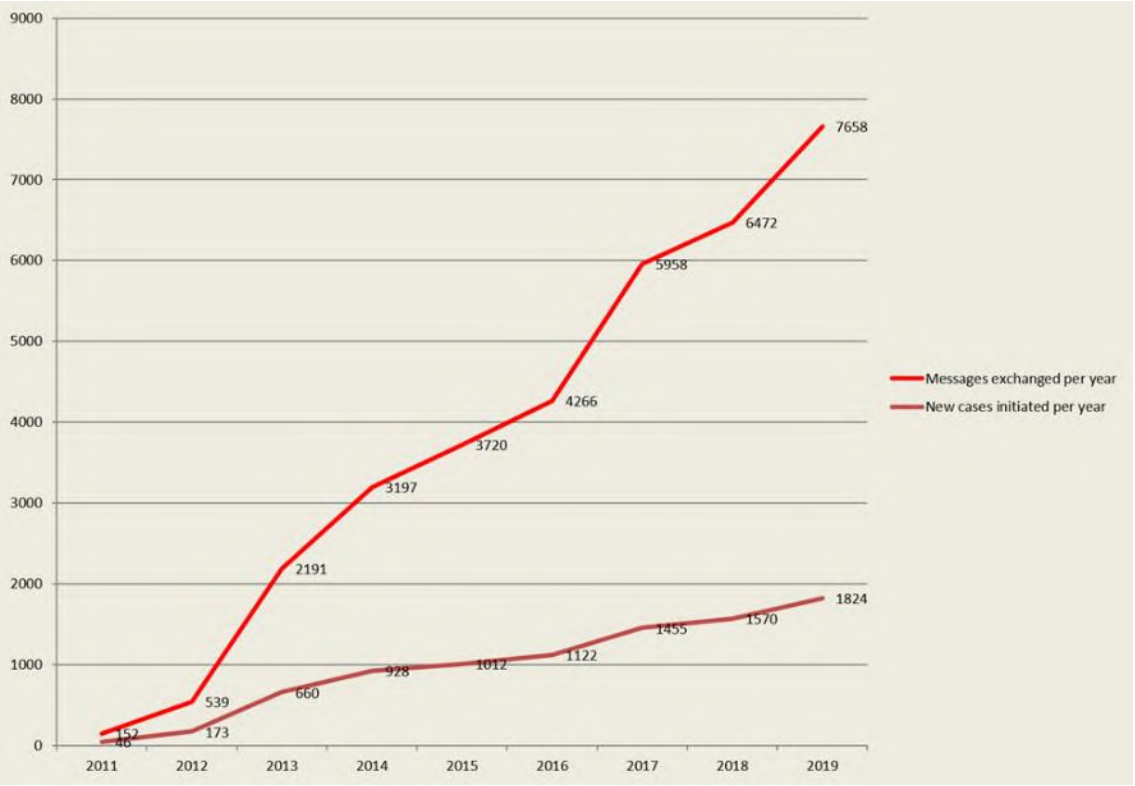
### *2.2. Money laundering, asset recovery and financial crime*

On money laundering, asset recovery and financial crime, the Comprehensive Assessment found that the EU legal framework was well developed, but could still be further improved. In some instances, better and more effective implementation of existing laws was needed. In that regard, the Comprehensive Assessment proposed several measures to improve the work of **Asset Recovery Offices**, such as granting them access to additional databases, facilitating information exchange between offices and with national authorities, providing investigators with specialized training or increasing cooperation with customs and Financial Intelligence Units (FIUs). The assessment further suggested the possibility of mapping out investments made by organized crime groups on high-risk sectors – to better detect the infiltration of organised crime in the economy.

The Commission funded a study completed in 2018, which provided a model to **map the risk of serious and organised crime infiltration in legitimate businesses** across European territories and sectors. This aimed at mapping out investments made by organised crime groups and infiltration of organised crime in the legal economy. This model is currently being further developed and applied to all criminal markets identified as priorities by the current EU Policy Cycle by means of a follow-up study by an external contractor to be finalised mid-2020.

Over the course of the past three years, the operational exchanges between the **Asset Recovery Offices** continued to increase. The Commission continued to chair and convene the EU Asset Recovery Office Platform - five meetings of the Platform and four meetings of the sub-groups on asset management and virtual currencies took place since the adoption of the Comprehensive Assessment of EU security policies. During the May 2019 Platform meeting, the Asset Recovery Offices highlighted the importance of providing them with swift access to a minimum set of databases and registers. They also pointed to the need to exchange information via SIENA in order to enable the swift and secure communication of crime-related information, the necessity to enhance their powers as well the need to set fixed and strict time limits within which an Asset Recovery Office must respond to a request by a counterpart. The Commission also continued to support financially the Camden Asset Recovery Inter-Agency Network (CARIN) of asset recovery practitioners.

**Number of exchanges of Asset Recovery Offices via SIENA 2011-2019**




A new priority, Criminal Finances, Money Laundering and Asset Recovery, was included as a priority crime area in the EU Policy Cycle 2018-2021 to increase cooperation among law enforcement agencies on financial investigations.

Since its adoption in 2016, the EU has constantly updated and adapted its list of "high-risk third countries", i.e. countries with strategic deficiencies in their Anti-Money Laundering/Counter Terrorist Financing regimes, which consequently pose significant threats to the financial system of the Union. A further amendment, including of the underlying methodology, was adopted on 7 May 2020.

As regards **the impact of the COVID-19 pandemic**, organised crime was highly adaptable and has been quick to seize opportunities to engage in new criminal activities offered by the current situation in order to generate profits. As reported by Europol, organised crime groups were increasingly trading counterfeit and sub-standard goods, on both the surface web and dark web. The distribution of counterfeit medical equipment, sanitisers/disinfectants and pharmaceuticals was particularly threatening to the health and safety of medical staff and the general public. Organised crime groups were likely to take advantage of persistent conditions of economic hardship for infiltrating the legal economy. The pandemic offered greater opportunities for the money to be laundered into

"ordinary, sound companies" in urgent need for cash after the sudden loss of income suffered during lockdowns.

### *2.3. Trafficking of firearms*

As regards firearms trafficking, the Comprehensive Assessment stressed that it should remain a high priority in security policies. As such, any inconsistency in implementation of the current legislation should be effectively resolved. Furthermore, the assessment pointed out that further **capacity building**, better cooperation between bodies (public authorities such as customs services as well as private sector and their networks), and **cooperation with third countries**[92] had proven useful. It could thus be further expanded to the fight against firearms trafficking. In order to gain a better intelligence picture on firearms trafficking, it was suggested that the EU develops a systematic harmonized data collection on firearms seizures for all Member States.

The Joint Communication of the Commission and the High Representative of the Union for Foreign Affairs and Security Policy on "Elements towards an EU Strategy against illicit Firearms, Small Arms and Light Weapons and their Ammunition"[93] was endorsed by the Council of the EU in 2018[94]. On 27 June 2019, the Commission also published its "Evaluation of the 2015-2019 action plan on firearms trafficking between the EU and the south-east Europe region"[95]. The assessment demonstrated the benefits of European cooperation by improving cooperation and networking between law enforcement officials in the region as well as the exchange of operational information between the EU and Western Balkans. It also demonstrated that further efforts were still required by all partners to put in place efficient national coordination centres on firearms (focal points), to establish a more effective penal chain that leads to convictions and deterrent sanctions for firearms trafficking as well as to improve exchange of information and intelligence between EU and Western Balkan partners. Harmonising the collection of data on firearms' seizures and standardising the reporting were identified as key operational priorities for future work.

The Commission, through the Internal Security Fund - Police - financially supported several studies such as the FIRE[96] and SAFTE[97] research programmes, to improve knowledge on the illicit trafficking of firearms covering inter alia online trafficking and the diversion of legal trade. The Commission financed the UNODC's Global Firearms

---

92 Cooperation with the Western Balkans in that matter can be refered as a successful example.
93 JOIN(2018) 17 final, 1.06.2018.
94 Council conclusions of 19 November 2018 – Document 13581/18.
95 COM (2019) 293 final, 27.06.2019.
96 *Fighting Illicit Firearms Trafficking Routes and Actors at European Level*, eds. Ernesto U. Savona, Marina Mancuso, Transcrime – Università Cattolica del Sacro Cuore, 31.03.2017.
97 Triggering Terror: Illicit Gun Markets and Firearms Acquisition of Terrorist Networks in Europe, ed. Nils Duquet, Flemish Peace institute, 17 April 2018.

Programme to collect and analyse quantitative and qualitative information and data on trafficking in firearms.[98]

### *2.4. Drugs trafficking*

Drugs trafficking was another major security threat brought by organised crime. Yet, the Comprehensive Assessment pointed out that **Council framework decision from 2004**[99] setting up criminal offences and penalties in this field, while providing a common framework, needed to be reviewed, as it did not address a number of issues such as prevention or the development of an online market for drugs. The Assessment stressed the importance of **action on the international stage**, and of ensuring the implementation of the United Nations Special session of the General Assembly on the world drug problem (UNGASS) outcome document adopted in 2016 and the preparation of the 2019 review process on Drugs. As regard the growing number of new psychoactive substances, the assessment suggested amending the European Monitoring Centre for Drugs and Drug Addiction regulation. It also called for an **EU common approach to drugs trafficking**, especially of new psychoactive substances and a new legislative framework to adapt EU action to those new psychoactive substances.

The European Commission carried out the regular (every 6 years) **evaluation of the European Monitoring Centre for Drugs and Drug Addiction** (EMCDDA) in 2018/19.[100] The main conclusion of the evaluation is that the Agency overall worked well. The evaluation was positive as regards all five evaluation criteria (better regulation criteria), but it also identified further the need for improvements in several areas. The Agency was recognised as a hub of excellence and its information is considered factual, objective, reliable and robust. The EU added value of the work of the Agency was high. There was room for improvement as regards technological development, the availability of more forward-looking products, the relationship with the scientific community and general practitioners, and the general public awareness. The Agency could provide more information on drug supply issues and should work further on the comparability of data. Poly-drug use and the support to Member States in evaluating their national drug policies were areas where the Agency's contribution would provide added value. The evaluation was inconclusive on the potential future broadening of the scope of the Agency to other licit and illicit substance and addictive behaviours.

In 2019/2020, the European Commission carried out the final evaluation of the EU Drugs Strategy 2013-2020[101] and the EU Action Plan on Drugs 2017-2020[102]. Preliminary findings of the evaluations suggested that actions on drug supply and demand reduction

---

98 UNODC Global Firearms Study, 2019.

99 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.

100 COM (2019) 228; SWD (2019) 174.

101 https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2012:402:0001:0010:en:PDF

102 https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52017XG0705(01)&from=EN

needed to be strengthened and more integrated with the area of security, public health, environmental and social aspects.

On the **international stage**, the Commission actively participated in the 2019 review process on drugs and on the negotiations of the UN Ministerial Declaration[103], which was a follow-up to the 2016 UNGASS outcome document. The European Commission proposed Union positions for the voting at the Commission on Narcotic Drugs in 2018, 2019 and 2020[104] as regards the scheduling of new psychoactive substances. It also proposed positions in 2020 for the re-scheduling of cannabis and cannabis-related substances[105]. Furthermore, the European Commission proposed in 2018 to launch two new dialogues on drugs with China and Iran. Both dialogues were approved by the Council[106]. The Commission supported the conclusion of working arrangements by the EMCDDA with non-EU partners through the adoption of opinions on these working arrangements. Since July 2017, these concerned Albania, Kosovo*[107], Serbia and Ukraine (re-negotiation of an existing agreement).

Finally, the European Commission supported drug policy through the funding of the **Civil Society Forum on Drugs**, and many concrete projects, in particular through the drugs part of the Justice Programme and through the Internal Security Fund – Police[108].

### *2.5. Trafficking of human beings*

Under the comprehensive EU legal and policy framework[109], anti-trafficking actions have been victim centred, gender-specific and child-sensitive, focussing on the internal and external dimension, ensuring policy coherence and consistency across policy areas and with relevant stakeholders.

The Comprehensive Assessment identified the need to ensure the implementation of the Anti-trafficking Directive; to address the links between trafficking in human beings and other forms of organised crime; to protect and assist the most vulnerable and at the same time target the perpetrators; to address trafficking for sexual exploitation and child trafficking and also the links to the migration context; to improve data collections and ensure funding.

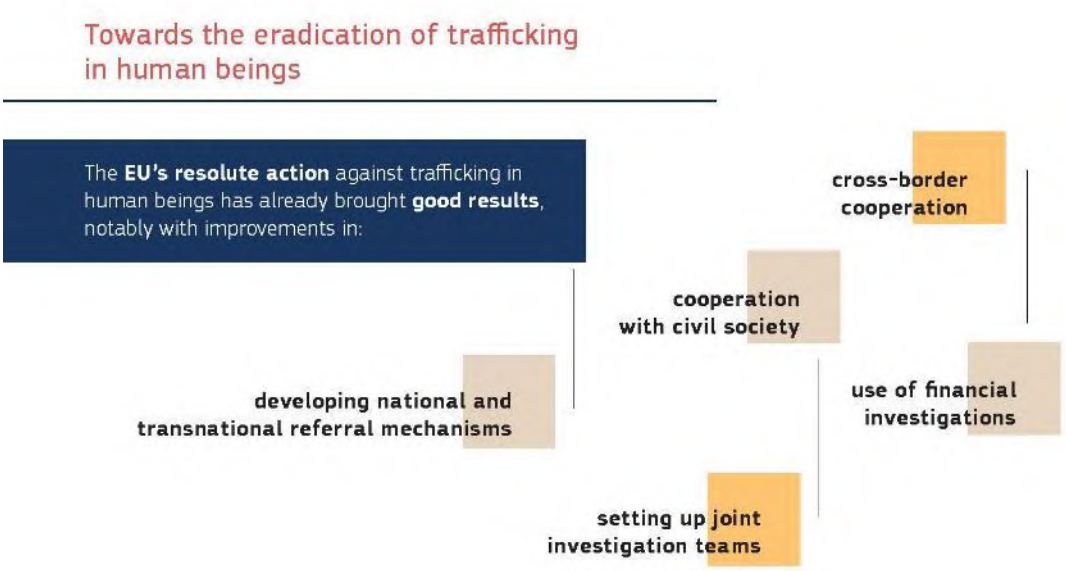
---

[103] https://www.unodc.org/documents/commissions/CND/2019/Ministerial_Declaration.pdf
[104] COM (2018) 31; COM (2018) 862 and COM(2019) 631.
[105] COM (2019) 624.
[106] The EU-China Summit of 16-17 July 2018 in Beijing resulted in an agreement to launch an annual EU-China Dialogue on Drugs. The modalities of the future dialogue were confirmed by COREPER on 30 October 2019. The Council approved the launch of a new EU-Iran dialogue on drugs on 5 March 2020.
[107] *This designation is without prejudice to positions on status, and is in line with UNSCR 1244/1999 and the ICJ Opinion on the Kosovo declaration of independence.
[108] Cf. Annex 2.
[109] Directive 2011/36/EU on preventing and combatting trafficking in human beings and protecting its victims ('Anti-trafficking Directive') and the EU Strategy towards the Eradication of Trafficking in Human beings 2012-2016.

EU actions followed from the 2017 Commission Communication "Reporting on the follow up to the EU Strategy towards the eradication of Trafficking in human beings"[110] for **stepping up the fight against organised criminal networks** by disrupting the business model and untangling the trafficking chain; by providing victims with better access to their rights; and by intensifying a coordinated and consolidated response, both within and outside the EU.

The two cross-cutting priorities focused on **widening the knowledge base** and on **ensuring funding**.

EU actions included: the joint statement of commitment signed by the heads of ten EU Agencies[111], the publication of European Institute for Gender Equality's (EIGE) report on gender-specific measures in anti-trafficking action (2018), the Fundamental Rights Agency's (FRA) Guide on Children deprived of parental care found in an EU Member State other than their own (2019), and the Commission's "Working together to address trafficking in human beings: key concepts in a nutshell (2018)"[112]. The Commission also launched two studies: one on "Reviewing the functioning of national and transnational referral mechanisms"; and another regarding the "Social, economic and human costs of trafficking in human beings", which are currently being finalised.




[110] COM (2017)728 final.

[111] CEPOL, European Asylum Support Office, Eurojust, Europol, eu-LISA, Frontex/EBCGA, European Institute of Gender Equalities, Eurofound, Fundamental Rights Agency, EMCDDA.

[112] Further information on EU anti-trafficking action since 2017 is available in the publication "EU anti-trafficking action 2017-2019: at a glance" and on the EU Anti-Trafficking Website, which has been revamped in the course of 2018 to improve accessibility and reorganise the resources in a more user-friendly format. Regular work is carried out on the website to update the content and improve accessibility.

The results of the latest EU-wide data collection were published in the 2018 Data study together with the Second Progress report of the Commission[113]. The report identified certain improvements to the overall framework, especially with regard to cross-border cooperation, cooperation with civil society, use of financial investigations, setting up joint investigation teams, and developing national and transnational referral mechanisms.

Trafficking in human beings remained a highly profitable crime characterised by impunity for the perpetrators and those who exploit the victims. Trafficking for sexual exploitation has consistently been the most common form of exploitation, largely targeting women and girls; while many victims are children[114]. The findings of the Transposition report on the Anti-trafficking Directive[115] showed that substantial efforts have been taken by the Member States to transpose it, nevertheless, there still remained significant room for improvement, in particular as regards to assistance, support and protection of victims and prevention. The Commission has been proactively monitoring the transposition and implementation of the Directive and requested the feedback of Member States in 2019.

The Commission has been encouraging Member States to criminalise the knowing use of services provided by the victims, which followed from the findings of the Commission's 2016 Users' report[116]. It was noted that the complete absence or inadequate criminalisation of the use of services of victims of trafficking in human beings, may foster the activities of the traffickers including through a culture of impunity. Such criminalisation was called for by the European Parliament[117].

### 2.6. Corruption

The 2017 Comprehensive Assessment highlighted **the link between organised crime and corruption**, which is a key enabler of organised crime. The Commission has prioritised fighting corruption in the European Semester of economic governance. By doing so, the Commission has ensured a continuous and streamlined monitoring of anti-corruption efforts and engaged with Member States in the area of major common interest. The annual European Semester country reports included detailed analysis of corruption risks and associated challenges. In relevant cases, these issues were also reflected in Country Specific Recommendations, endorsed each year by national leaders in the European Council.

---

[113] COM (2018) 777 final and SWD (2018) 473 final.

[114] Data collection on trafficking in human beings in the EU (2018, European Commission).

[115] European 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 final.

[116] European Commission's Users report : COM(2016) 719, http://ec.europa.eu/antitrafficking/sites/antitrafficking/files/report_on_impact_of_national_legislation_related_to_thb_en.pdf

[117] European Parliament resolution of 26 November 2019 on children's rights on the occasion of the 30th anniversary of the UN Convention on the Rights of the Child (2019/2876(RSP)).

In the 2019 Country Reports, the Commission focused its analysis on 15 Member States which present particular challenges[118]. Eight of these Member States[119], have received related Country Specific Recommendations. In addition to the Semester, Romania and Bulgaria received recommendations in this area in the framework of the Cooperation and Verification Mechanism (CVM). The analysis for the 2019-20 exercise showed that challenges remain in this area in most Member States covered by the analysis. Issues such as capacity and specialization to investigate and prosecute corruption crimes, inadequate conflict of interest regime, lack of comprehensive institutional framework, in particular dedicated national authorities to fight corruption, inadequate whistle-blowers legal framework, still needed to be addressed.

In July 2019, the EU became an observer to the **Council of Europe's Group of States against Corruption** (GRECO). The European Union's participation in GRECO as an observer brought added value to the cooperation between the European Union and the Council of Europe by facilitating joint work on capacity-building and implementing standards intended to strengthen the rule of law and the fight against corruption.

Council Framework Decision 2003/568/JHA of 22 July 2003 on **combating corruption in the private sector** aimed to ensure that both active and passive corruption in the private sector are criminal offences in all EU Member States. The third implementation report of the 2003 Framework Decision on Corruption in the Private Sector, published in 2018, assessed one of the core pieces of the EU anti-corruption acquis. That latest report showed that, overall, the level of transposition of the Framework Decision has improved compared to that in the 2011 implementation report. The level of penalties introduced in the national criminal codes was in line with the minimum thresholds of the Framework Decision in all Member States. They also have appropriate frameworks for the liability of legal persons. However, some of the provisions have been difficult to implement in some Member States and efforts need to extend to enforcing specific criminal measures. The Commission will continue to support Member States in transposing, implementing and enforcing EU legislation to a satisfactory level.

### 2.7. Environmental Crime

The 2017 Comprehensive Assessment found that the attention of Member States' law enforcement authorities on **organised environmental crime** was increasing, as evidenced by the fact that environmental crime had become a political priority under the new Policy Cycle to fight serious and organised crime for the period 2018-2021, with a special focus on illicit waste and wildlife trafficking. Wildlife trafficking was also the subject of a dedicated action plan[120] which still needs to be fully implemented[121].

---

[118] Hungary, Cyprus, Czech Republic, Bulgaria, Croatia, Greece, Italy, Latvia, Lithuania, Malta, Portugal, Romania, Slovakia, Slovenia and Spain.
[119] Cyprus, Czech Republic, Croatia, Hungary, Italy, Latvia, Malta and Slovakia.
[120] 2016 Action Plan against Wildlife Trafficking, COM (2016) 87 final.

The Commission supported **projects on environmental crime** with funding from the Internal Security Fund – Police. The funded projects have synergies with the Policy Cycle and address the need to gather intelligence on criminal activities, develop cross border cooperation and operational actions[122]. The Commission also supported and collaborated with EU networks of police officers, prosecutors, inspectors and judges specialised in combating environmental crime.[123]

Since 2017 and within the framework of the Secure Societies strand of Horizon 2020, the EU has been significantly investing in research projects that address organised crime and that provide their results both to policy and to practitioners (individual law enforcement agencies, their networks, and Europol). The key areas were: modelling of the processes that led to organised crime, nexus between organised crime and terrorism, investigation of mobile devices used by organised crime networks, online dimension (including darknet), such as multimedia analysis for organised crime prevention and investigation, advanced tools for fighting online illegal trafficking, money flows tracking (e.g., tools for investigation of transactions in underground markets), tools for discovering criminal networks and identifying their members, early warning and early action led policing in fighting organised crime, etc.

[121] Progress report on the implementation of the EU Action Plan against Wildlife Trafficking SWD (2018) 452 final.

[122] A call on environmental crime (€1.5m) was published under the ISF-P Annual Work Programme 2018 and a call for €2.5m was published under the ISF-P Annual Work Programme 2017.

[123] EnviCrimeNet. European Network of Prosecutors for the Environment (ENPE), IMPEL, EU Forum of Judges for the Environment (EUFJE).

## IV. CYBERCRIME POLICIES

While the stakeholders involved in the Comprehensive Assessment identified cybercrime as a major and evolving threat to EU security, they considered the **EU intervention insufficient given the dynamically changing landscape**. As such, the assessment called for more measures at all levels – strategic, legislative, and operational and pointed out the need for a more complete threat intelligence picture and greater coordination among all relevant actors.

The assessment suggested providing Member States with further **support for the transposition and implementation of all cybercrime related laws** – in particular those on child sexual abuse and attacks against information systems. The assessment of implementation of the 2011 directive on combating child sexual abuse[124] indicated that, while significant progress had been made, there was room for the Directive to reach its full potential by achieving a complete implementation by Member States. The areas in which efforts were still needed included prevention, substantial criminal law and assistance to child victims. In addition to monitoring the implementation of the Directive, the Commission has supported Member States by facilitating exchanges of best practices, for example through expert workshops, of which the Commission has organised six in the last two years.

### 1. Transposition and implementation of legislation

#### *1.1. Overview*

State of transposition of main directives in the cybercrimes area

| | Transposition deadline | Open non-communication infringements | Open non-conformity infringements |
|---|---|---|---|
| Directive 2011/93/EU on combating the sexual abuse and sexual exploitation of children and child pornography | 18/12/2013 | 0 | 23 |
| Directive 2013/40/EU on attacks against information systems | 04/09/2015 | 0 | 4 |

[124] Directive 2011/93/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.

Based on the information submitted by Member States of the measures taken to implement the Directive at national level, the Commission initiated formal exchanges on conformity of transposition of the Directive with 26 Member States[125] and it opened infringement procedures against 23 in 2019.

### *1.2. Directive on Attacks against Information Systems[126]*

In its 2017 report[127] on the implementation of the 2013 **Directive on Attacks against information systems**, the Commission acknowledged the major efforts undertaken by the Member States to transpose the Directive. However, it also concluded that there was still scope for the Directive to reach its full potential if Member States were to implement its provisions fully. The analysis suggested that some of the main improvements Member States could still achieve were to align definitions of offences in their national law and include common standards of penalties for cyberattacks. Other areas of attention included the implementation of practical measures that Member States could take to provide for appropriate channels for citizens to report cyberattacks to authorities, and for authorities to gather statistics on reports, prosecutions and convictions for cyberattacks to allow for a comparison at EU level. Therefore, the Commission committed to assisting Member States with the implementation of the Directive.

The Commission undertook a number of activities for that purpose, including the organisation of workshops in the area of operational points of contact and of collection of statistical information. In addition, following the assessment of the conformity of the transposition of the Directive by Member States, the Commission initiated infringement procedures against four Member States in July and October 2019, as it assessed the national implementing legislation notified by those Member States did not represent a correct transposition of the Directive[128].


## 2. Broader policy implementation

[125] All Member States at the time except Denmark, which is not bound by the Directive, and the UK.
[126] Directive 2013/40/EU.
[127] COM(2017) 474 final.
[128] Bulgaria, Italy, Portugal and Slovenia.

As regards the **means for EU level operational cooperation**, several existing tools could be improved. While the joint cybercrime action task force (J-CAT) hosted by Europol's Cybercrime Centre has been praised for its efficiency, the assessment noted that too few Member States could afford to join it, calling for actions to facilitate participation. Currently, J-CAT's membership spans 16 countries, with five new countries joining since 2017[129]. To boost awareness and collaboration at the national, regional and local level, a number of roadshows were organised in 2018 and 2019. The roadshows were an opportunity to reach out to 580 law enforcement and judiciary practitioners from the current J-CAT countries, and a further 580 participants from over 30 countries, who followed through CEPOL webinars. The assessment suggested establishing a joint centre of excellence for cyber forensics and encryption, in order to complete EU action in that matter.

Further to the calls by the JHA Council in December 2016 and the European Council in June 2017, the Commission gathered information from Member States and experts in the private sector, based on which it published in the 11th Security Union Progress Report in October 2017 six practical measures addressing the issue of **encryption in criminal investigations**:

- Supporting Europol in further developing its capability to deal with encryption: funding of EUR 5 million for Europol and the Joint Research Centre to procure the necessary equipment and set-up the platform to gain access to data on seized devices;
- Establishing a network of centres of encryption expertise: the network has met several times and has started working on:
    - the toolbox of alternative measures;
    - training for law enforcement authorities: the European Cybercrime Training and Expert Group (ECTEG) has received a grant to develop training modules and deliver pilot courses – the first module is currently under peer-review;
- Establishing an observatory for legal and technical developments: Europol and Eurojust published already two observatory reports[130];
- Holding a structured dialogue with industry and civil society organisations: a plenary session and several sub-group sessions were held.

[129] Romania, Poland, Sweden, Norway and Switzerland.

[130] https://www.europol.europa.eu/sites/default/files/documents/final_report_of_the_observatory_function.pdf and https://www.europol.europa.eu/sites/default/files/documents/second_observatory_function_report.pdf

In addition to the above-mentioned measures, the Commission continued its work on the challenges posed by encryption in criminal investigations, in particular by looking into how law enforcement can deal with end-to-end encrypted information when encountered during investigations.

The 2017 assessment also suggested setting up swift investigation measures across borders and effective judicial cooperation. This suggestion was addressed through the measures proposed as part of the **cybersecurity package** adopted in September 2017, with the Joint Communication "Resilience, Deterrence and Defence: Building strong cybersecurity for the EU"[131]. The package included a comprehensive set of measures addressing the emerging cyber threats by reinforcing EU's cyber resilience, by creating a single market for cybersecurity, and by effectively building an EU cyber deterrence and strengthened international cooperation.

One of the aims of the package was to improve the legal framework across the EU to ensure that cybercrimes can be investigated and prosecuted. Stemming from the package were two initiatives aimed at improving the response to cybercrime: the Directive on combatting fraud and counterfeiting of non-cash means of payment[132], adopted by co-legislators in 2019, and the commitment to improve cross-border access to electronic evidence for criminal investigations.

In 2018, the Commission adopted two legislative proposals (for a Regulation on European Production and Preservation Orders for electronic evidence in criminal matters [133] and a Directive on the appointment of legal representatives for the purpose of gathering evidence in criminal proceedings [134]). On the basis of these proposals, the Council adopted its general approach in December 2018 and March 2019 respectively, whereas the European Parliament has yet to adopt its position before the co-legislators can enter into discussions.

In 2018, the Commission also provided funding under its Foreign Policy Instruments (FPI) for the activities of the SIRIUS project by Europol and Eurojust to support the cooperation between authorities and service providers to obtain e-evidence in the context of the existing legal framework[135]. In February 2019, the Commission also adopted two

---

[131] Joint Communication to the European Parliament and the Council Resilience, Deterrence and Defence: Building strong cybersecurity for the EU JOIN/2017/0450 final.

[132] Directive (EU) 2019/713 of the European Parliament and of the Council of 17 April 2019 on combating fraud and counterfeiting of non-cash means of payment and replacing Council Framework Decision 2001/413/JHA.

[133] Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on European Production and Preservation Orders for electronic evidence in criminal matters COM(2018) 225 final - 2018/0108 (COD).

[134] Proposal for a DIRECTIVE OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL laying down harmonised rules on the appointment of legal representatives for the purpose of gathering evidence in criminal proceedings.

[135] Foreign Policy Instrument (FPI), grant agreement No PI/2017/391-896.

Recommendations for Council Decisions to open negotiations at international level to improve cross-border access to electronic evidence, i.e. to open negotiations for an EU-US agreement on e-evidence[136] and to participate in the ongoing negotiations for a Second Additional Protocol to the Council of Europe 'Budapest' Convention on Cybercrime[137]. On the basis of these recommendations, the Council adopted Decisions in June 2019 to authorise the Commission to open and participate in these negotiations on behalf of the Union[138].


The creation of a European Cybercrime Centre (EC3) at Europol in 2013 has been conducive to enhancing cooperation at EU level. It also furthered international cooperation with several international partners and through its partnership with Interpol's Global Complex for Innovation (IGCI). EC3's model relied extensively on multi-agency collaboration and trust-based partnerships with the relevant non-law enforcement entities. Six years after its establishment, it has made a significant contribution to the European Union Member States' efforts to thwart cybercrime through an agile crime-fighting model. The ever-increasing number of requests for operational, strategic and forensic support by the MS' competent authorities, the growing network of Public-Private-Partnerships and the large number of successful innovative initiatives have been indicative of the relevance of the model adopted by EC3.

At multilateral level, the EU continued to support actions aiming at ensuring that international law, including international conventions such as the Council of Europe Convention on Cybercrime (Budapest Convention) and relevant conventions on international humanitarian law and human rights, were upheld in the cyberspace.

Cybercrime issues have been receiving particular attention and investment within the Secure Societies strand of Horizon 2020 and have been well aligned with policy requirements. As a result, the funded security research projects have been providing a

[136] COM(2019) 70 final.
[137] COM(2019) 71 final.
[138] Council documents 9114/19 and 9116/19.

significant input both to policy developments and to practitioners (law enforcement authorities, their networks, Europol), notably in the areas of fighting child sexual exploitation online, digital forensics, encryption, financially motivated malware and electronic evidence. Regarding the latter, results of security research were also used as a source of information for the impact assessment of the corresponding proposal[139].

Furthermore, the Comprehensive Assessment pointed out the absence of a harmonized legal framework on data retention of communication metadata. In 2014, the Court of Justice of the European Union (CJEU) invalidated[140] the 2006 Data Retention Directive[141] because of its incompatibility with the fundamental rights to privacy and data protection.[142] Data retention is an important tool for the investigation and prosecution of criminal offences, particularly because of the use of communication technologies to commit cyber and cyber-enabled/dependent crime. Complex cases, such as child sexual abuse or organised crime investigations, require sufficient time to enable law enforcement to conduct the resource-intensive analytical work and enrich the intelligence. National data retention frameworks are currently being assessed against the standard set by the ECJ, casting doubt on the admissibility of evidence in court proceedings based on access to retained data. Different national rules and a lack of harmonisation also limit opportunities for cross-border cooperation and information exchange as data may not be available by the time law enforcement need it.The crucial value of a data retention framework is, therefore, the guarantee that communications data will be readily available to law enforcement upon request, subject to robust legal, procedural and fundamental rights safeguards as required by EU law.
In this context, the Commission has been participating in the reflection process in the Council to discuss the way forward on data retention to ensure that critical information necessary to conduct investigations is available to police and judicial authorities. The Commission has also conducted stakeholder consultations and launched a fact-finding study in response to the request from the Council, which is expected to deliver results in summer 2020. The European Court of Justice is currently considering a number of cases dealing with key questions on national data retention frameworks, and its judgments in these cases, expected in the course of 2020, should provide further guidance on the possible scope of a harmonised data retention legal framework.

**The outbreak of COVID-19** showed how quickly criminals take advantage of a changed environment: cybercriminals have been particularly swift and industrious in exploiting the fears and anxieties of citizens by deploying phishing and malware attacks to extract payment card information and extort victims. They have adapted social engineering techniques as part of these pandemic-themed campaigns and attempts to carry out Business E-mail Compromise (BEC). From an infrastructure perspective, criminals have

[139] COM (2018)225.
[140] Judgment in Joined Cases C-293/12 *Digital Rights Ireland* and C-594/12 *Seitlinger et al,* 8 April 2014.
[141] Directive 2006/24/EC.
[142] Articles 7 and 8 of the EU Charter of Fundamental Rights.

been very active in registering domain names that have a reference to or contain words like corona or COVID. This domain name registration has been a backbone for many of their other criminal activities, which are linked to the current crisis. On the dark net, vendors focused their efforts on selling counterfeit versions of legitimate goods, such as medical supplies or cleaning material[143].

[143] Cf reports on all these topics on https://www.europol.europa.eu/activities-services/staying-safe-during-covid-19-what-you-need-to-know.

## CONCLUSION

At the light of the present review of the Union's action in the area of internal security, and specifically of the stocktaking of the implementation of Home Affairs legislation in this field, most of the findings and recommendations of the Comprehensive Assessment of EU Security Policy of July 2017 have been acted upon to different degrees and with generally positive effects.

Although most Member States were able to ensure timely and full transposition of most new EU legislation into their national legislations, challenges remained during the period in this regard. Reasoned opinions were issued and infringement procedures were necessary in cases of failure by individual Member States to communicate in due time the adoption of national legislation fully transposing legal acts.

There was a significant increase in the number of evaluations and reports on policies and instruments in the field of internal security. The same is true as regards studies and impact assessments. While all policies and instruments evaluated during this period have shown EU added-value, there was progress in reflecting critical findings of such evaluations as regards changes in policy implementation or the modification of legislative framework both through changes to existing instruments and, where required, through the establishment of new ones. Moreover, the establishment of two High-level expert groups - on information systems and interoperability, and on radicalisation – have proven successful as regards e.g. ex-ante evaluation and stake-holders engagement[144].

The Schengen evaluation and monitoring mechanism implemented by the Commission together with the Schengen States and Associated countries has provided regular quality control on the implementation of the Schengen *acquis* relevant to internal security. The deficiencies detected were subject to recommendations by the Council and to a close follow up of the Member States remedial action plans by the Commission services, resulting in a relatively high degree of compliance.

The articulation between the external dimension of internal security and foreign policy improved, also with enlargement, neighbourhood and development cooperation policies and a deepening of the internal-external security nexus, notably in the Western Balkans and Mediterranean regions. Furthermore, this report shows a closer alignment of sectoral security policies with those of support instruments such as Horizon 2020's research programme "secure societies" strand.

[144] This is also the case as regards two other high-level expert groups relevant for internal security, respectively on Artificial intelligence and on Fake news and online disinformation.