Council of the European Union

Brussels, 22 April 2021
(OR. en)

8085/21

COSI 65
ENFOPOL 143
CRIMORG 31
CYBER 105
ENFOCUSTOM 55
IXIM 71
CORDROGUE 17
CT 51
FRONT 149
CATS 29
COPEN 190
DROIPEN 78
JAIEX 46
JAI 422

COVER NOTE

From:	Secretary-General of the European Commission, signed by Ms Martine DEPREZ, Director
date of receipt:	19 April 2021
To:	Mr Jeppe TRANHOLM-MIKKELSEN, Secretary-General of the Council of the European Union
No. Cion doc.:	COM(2021) 170 final
Subject:	COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS on the EU Strategy to tackle Organised Crime 2021-2025

Delegations will find attached document COM(2021) 170 final.

Encl.: COM(2021) 170 final

EUROPEAN
COMMISSION

Brussels, 14.4.2021
COM(2021) 170 final

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

on the EU Strategy to tackle Organised Crime 2021-2025

{SWD(2021) 74 final}

Introduction

Hidden from public view due to the opaque nature of its activities, organised crime is a significant threat to European citizens, business, and state institutions, as well as to the economy as a whole. As highlighted in the latest **European Union Serious and Organised Crime Threat Assessment** (2021 EU SOCTA)[1], organised crime groups are present across all Member States. The organised crime landscape is characterised by a networked environment where cooperation between criminals is fluid, systematic and driven by a profit-oriented focus. Organised crime groups use their large illegal profits to infiltrate the licit economy and public institutions, including via corruption, eroding the rule of law and fundamental rights and undermining people's right to safety as well as their trust in public authorities. Criminal revenues in the nine main criminal markets in the European Union amounted to €139 billion in 2019[2], corresponding to 1% of the Union's Gross Domestic Product. As underlined in the Security Union Strategy[3], action taken at EU level to support Member States in the fight against organised crime must be continued and enhanced.

The complexity of the business model of organised crime groups was, in particular, exposed in 2020 in the joint investigation, led by French and Dutch authorities with the support of Europol and Eurojust, to dismantle **EncroChat**, an encrypted phone network widely used by criminal networks. The EncroChat case has so far led to more than 1,800 arrests and more than 1,500 new investigations. In addition, it displayed the extent to which organised crime groups operate transnationally and online across all criminal markets in a networked environment, using increasingly sophisticated modi operandi and new technologies. In March 2021, another joint operation following the cracking of Sky ECC, an encrypted network to which many former EncroChat users had migrated, led to the prevention of more than 70 violent incidents, the seizure of more than 28 tons of drug substances and the arrest of more than 80 suspects involved in organised crime and drugs trafficking in Belgium and the Netherlands. More than 400 new investigations against high risk organised crime groups have been initiated.

The use of violence by criminals involved in organised crime is on the rise in the EU, as is the threat from violent incidents due to the frequent use of firearms or explosives in public spaces[4]. The agility of organised crime groups to adapt to and capitalise on the changes in the environment where they operate was confirmed during the Covid-19 pandemic. Criminal

[1] Europol, 2021 European Union Serious and Organised Crime Threat Assessment (EU SOCTA), 12 April 2021, https://www.europol.europa.eu/activities-services/main-reports/european-union-serious-and-organised-crime-threat-assessment.The EU SOCTA is a comprehensive organised crime threat analysis identifying high priority crime areas produced every four years by Europol, on the basis of Member States' contributions.

[2] Illicit drugs, trafficking in human beings, smuggling of migrants, fraud (MTIC fraud, IPR infringements, food fraud), environmental crime (illicit waste and illicit wildlife), illicit firearms, illicit tobacco, cybercrime activities, organised property crime – Study on Mapping the risk of serious and organised crime infiltration in legitimate businesses, March 2021, DR0221244ENN, https://data.europa.eu/doi/10.2837/64101.

[3] Commission Communication on the EU Security Union Strategy, COM(2020) 605 final, 24.7.2020.

[4] Europol, 2021 EU Serious and Organised Threat Assessment Report (EU SOCTA), 12 April 2021, https://www.europol.europa.eu/activities-services/main-reports/european-union-serious-and-organised-crime-threat-assessment.

groups have exploited the pandemic to expand online crime activities[5] and to engage in fraud including in counterfeit medical products. The sustained high demand for Covid-19 vaccines makes for an attractive pursuit for criminals seeking to engage in the production and supply of counterfeit vaccines or in fraud schemes targeting individuals or public authorities. EU governments have so far detected attempts of scams and fake offers by fraudsters trying to sell over 1.1 billion vaccine doses for a total price of over €15.4 billion[6]. The economic crisis resulting from the pandemic increases the risks of organised crime activities and that these further infiltrate society and the economy.

The transnational threats and evolving modi operandi of organised crime groups operating offline and online call for a coordinated, more targeted and adapted response. While national authorities operating on the ground are on the frontline in the fight against organised crime, action at Union level and global partnerships are paramount to ensure effective cooperation as well as information and knowledge exchange among national authorities, supported by a common criminal law framework and effective financial means. Furthermore, organised crime is emblematic of the link between internal and external security. International engagement on countering organised crime, including further steps to develop partnerships and cooperation with countries in the immediate neighbourhood and beyond, is needed to address this transnational challenge.

Both the European Parliament[7] and the Council[8] have stressed that organised crime causes enormous damage and highlighted the importance of strong EU action to counter all forms of organised criminal activity.

This Strategy builds on past achievements, identifies priority work strands to better protect citizens and the economy from organised crime groups and puts forward concrete medium and long-term actions, which will be developed in full respect of fundamental rights. It constitutes the first dedicated Strategy on organised crime since the entry into force of the Lisbon Treaty[9].

---

[5] In an international operation supported by Europol and the European Anti-Fraud Office (OLAF) between March and December 2020, law enforcement authorities of 19 Member States and eight third countries seized almost 33 million fake medical devices, including face masks, tests and diagnosis kits, 8 tonnes of raw materials and 70 000 litres of hygiene sanitizers.

[6] Information reported by governmental authorities to OLAF. Law enforcement authorities together with Europol and OLAF are cooperating to thwart these attempted frauds.

[7] https://www.europarl.europa.eu/doceo/document/TA-9-2020-0378_EN.pdf. In October 2016, the European Parliament, adopted also a report specifically focussing on the fight against corruption, https://www.europarl.europa.eu/doceo/document/A-8-2016-0284_EN.pdf.

[8] Council Conclusions on Internal Security and European Police Partnership, 13083/1/20 REV 1, 24 November 2020.

[9] Organised Crime has been a priority of the EU since the middle of the 1990s, as shown in the Tampere Programme (that launched the first multi-annual strategic objectives of the EU in the field of Justice and Home Affairs and the subsequent multi-annual programmes on Justice and Home Affairs, such as the 2004 Hague Programme, the 2009 Stockholm Programme, the 2015 EU Agenda on Security, and the recently adopted 2020 EU Security Union Strategy. The last dedicated strategy on organised crime dates from 2005, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52005DC0232&from=EN.

1. Boosting law enforcement and judicial cooperation

Today's organised crime is an international enterprise. 65% of the criminal groups active in EU Member States are composed of members of multiple nationalities[10]. Transport routes of drugs, firearms or counterfeit products span across all continents through a global supply chain. Mobile organised crime groups engaged in organised property crime move quickly across multiple jurisdictions to carry out their crimes. By operating across different jurisdictions, criminal groups avoid detection and exploit the differences of the applicable national laws.

1.1.Smooth exchange of and timely access to information

In an area of freedom, security and justice, where there are no internal border controls, a high level of security can be ensured through robust police and judicial cooperation across Member States. Timely access to information, in full respect of fundamental rights and in particular data protection, is essential for the fight against all forms of organised crime. The European Union has provided law enforcement with a wide range of tools to facilitate exchange of information that has proved crucial in uncovering criminal activities and networks.

The **Schengen Information System (SIS)** has enabled frontline officers to quickly detect and locate persons and objects involved in organised crime and to take action accordingly. The information in this shared database can help officers arrest a person, seize an object or establish the travel movements of persons involved in an investigation. In 2020 alone, the Schengen Information System was searched almost 4 billion times resulting in more than 200,000 hits. The 2018 review of the SIS framework[11] considerably reinforced the system's functionalities and introduced a number of new tools, allowing national authorities to enter alerts on persons at risk of abduction or trafficking in human beings or to request inquiry checks of a suspect. The reform also grants Europol access to SIS alerts and to the exchange of supplementary information and makes more effective use of biometric data, by introducing the possibility of using facial images for identification purposes and of including DNA profiles to facilitate the identification of missing persons. The implementation of these novelties is moving ahead at full speed so that the new system is fully operational by the end of 2021, with the implementing acts and technical documentation completed, work on the

[10] Europol, 2021 EU Serious and Organised Threat Assessment Report (EU SOCTA), 12 April 2021 https://www.europol.europa.eu/activities-services/main-reports/european-union-serious-and-organised-crime-threat-assessment..

[11] 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, 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, and Regulation 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.

technical development of SIS well underway and with the first steps undertaken to develop a SIS handbook and training activities for SIS users.

The potential of SIS in combatting organised crime will be further enhanced through the new framework for **interoperability** between EU information systems in the area of justice and home affairs[12]. It is crucial to devote all efforts to achieving full interoperability by the end of 2023. This will facilitate law enforcement access to relevant information in the EU centralised information systems and allow the detection of multiple identities, essential to combat identity fraud often used by criminals to commit crimes or escape justice. Within the interoperability framework, a **multiple-identity detector** functionality is being developed which, by checking data across these systems, will help to effectively address the fraudulent use of identities.

Investigators working in isolation in one Member State are often not able to establish the involvement of an organised crime group behind a specific crime. The 2008 **Prüm** framework[13] allows law enforcement authorities, in the course of their investigations, to search for DNA and fingerprints in the databases of other Member States on a hit-no-hit basis through bilateral connections, and to search for vehicle registration data. While the Prüm framework has proven instrumental in solving many crimes in Europe, its decentralised nature has resulted in many bilateral connections between Member States' national databases not being established due to the technical complexity and the important financial and human resources entailed. Furthermore, it may take weeks or even months for authorities to share the personal data behind a hit. To enhance the efficiency of criminal investigations and reinforce the automated exchange of information on criminals, the Commission will propose to modernise the **Prüm framework to address the operational needs** of law enforcement authorities, in compliance with fundamental rights and the requirements of necessity and proportionality, and to align the data protection provisions with the Law Enforcement Directive[14]. The Commission is exploring options to ensure the connection of relevant databases between all Member States and to **speed up the exchange of information** following a hit. The Commission is also assessing the need to exchange **additional data**

[12] The interoperability framework covers the SIS, the Visa Information System (VIS), Eurodac, Entry-Exit System (EES), the European Travel Information and Authorization System (ETIAS) and the European Criminal Records Information System on third country nationals (ECRIS-TCN). Regulation (EU) 2019/817 of the European Parliament and of the Council of 20 May 2019 on establishing a framework for interoperability between EU information systems in the field of borders and visa and amending Regulations (EC) No 767/2008, (EU) 2016/399, (EU) 2017/2226, (EU) 2018/1240, (EU) 2018/1726 and (EU) 2018/1861 of the European Parliament and of the Council and Council Decisions 2004/512/EC and 2008/633/JHA, OJ L 135, 22.5.2019, and Regulation (EU) 2019/818 of the European Parliament and of the Council of 20 May 2019 on establishing a framework for interoperability between EU information systems in the field of police and judicial cooperation, asylum and migration and amending Regulations (EU) 2018/1726, (EU) 2018/1862 and (EU) 2019/816, OJ L 135, 22.5.2019.

[13] Council Decision 2008/615/JHA on the stepping up of cross-border cooperation, particularly in combating terrorism and cross-border crime and Council Decision 2008/616/JHA on the implementation of Decision 2008/615/JHA, OJ L 210, 6.8.2008.

[14] Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by national authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA, OJ L 119, 4.5.2016.

categories relevant for criminal investigations, such as facial images, driving licences, police records and ballistics, under the Prüm framework, and to add Europol as a new partner to that framework.

Given the cross-border and international dimension of organised crime, **travel information** is of the essence to identify high risk travellers who are not otherwise known to law enforcement agencies, and to establish links between members of criminal groups. The processing of **Passengers Name Record (PNR)** data assists relevant authorities in identifying persons involved in criminal activities committed by organised groups. To ensure this tool is used to its full potential, the Commission will continue to monitor full and effective implementation of the Passenger Name Record Directive[15] and support cooperation and exchange of PNR data between Member States, in particular by exchanging best practices, training and developing the necessary capabilities[16]. **Advanced Passenger Information (API)**, biographic data of passengers collected by air carriers during check-in, is equally highly valuable[17], also due to its complementarity with Passenger Name Record data. A revision of the current legal framework[18] would allow for a variety of improvements, notably on data accuracy and data completeness. More importantly, the Commission will analyse the potential use of API data to systematically query Europol data for countering organised crime and possibly extending its use to Intra-Schengen movements and waterborne carriers and coaches. With this objective, the Commission will make a proposal to revise the Advanced Passenger Information Directive in the first half of 2022, based on an Impact Assessment where these options and its impacts will be further explored.

1.2.Advanced cooperation frameworks

Major parts of law enforcement cooperation across the EU are based on the 1990 Convention implementing the Schengen agreement. This bedrock is complemented by other EU instruments, such as the Council Framework Decision 2006/960/JHA on simplifying the exchange of information and intelligence between law enforcement authorities of EU Member States or by chapters 4 and 5 of the Council Decision 2008/615/JHA of 23 June 2008 on the stepping up of cross-border cooperation, particularly in combating terrorism and cross-border crime (Prüm).

---

[15] Directive 2016/681 of the European Parliament and of the Council of 27 April 2016 on the use of passenger name record (PNR) data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime, OJ L 119, 4.5.2016.

[16] Such as the ones referred to in the Staff Working Document accompanying the Commission Report on the review of the PNR Directive, SWD(2020) 128 final, 24.7.2020, pp. 7-8.

[17] Reiterated calls for an increased use of advanced passenger information from the United Nations - see UNSCR 2178(2014), UNSCR 2309(2016), UNSCR 2482 (2019), and the commitment by participating states of the Organization for Security and Co-operation in Europe to set up advanced passenger information systems, confirm the importance of these data. In addition, since February 2018, the establishment of national advanced information systems is a standard of the International Civil Aviation Organization, making it mandatory for all contracting states to the Chicago Convention.

[18] Council Directive 2004/82/EC on the obligation of carriers to communicate passenger data, OJ L 261, 6.8.2004 ('Advanced Passenger Information Directive' or 'API Directive').

Member States have complemented this framework with a complex set of bilateral and multilateral agreements. As a result, the level of cooperation between Member States is uneven, creating operational obstacles preventing effective cross border cooperation.

The Commission will prepare a legislative proposal for **an EU Police Cooperation Code.** This will draw on the results of an ongoing external study and will be based on a thorough consultation process, taking into account the competence of Member States. The aim is to streamline and develop the various instruments for law enforcement cooperation including relevant EU legislation, Council guidelines, and Member States' good practices from bilateral and multilateral agreements into a coherent and modern rulebook that also covers investigative tools.

Furthermore, in order to address potential obstacles to cross-border cooperation specifically against organised crime structures, the Commission has launched an external study to assess whether the 2008 **Council Framework Decision on Organised Crime**[19] is still fit for purpose.

Europol plays an important role as the **EU criminal information hub**, supporting police cooperation and information exchange and producing, every four years, the **European Union Serious and Organised Crime Threat Assessment** (EU SOCTA) report[20]. In order to address pressing operational needs, such as cooperation with private parties or the processing of large sets of data, the Commission proposed in December 2020 to strengthen Europol's mandate[21]. The new competences and tools foreseen in the proposal will enable Europol to step up its support to fighting organised crime. Both the European Parliament and the Council are working on their mandates for the upcoming inter-institutional negotiations that are expected to start later this year. The Commission will facilitate the negotiations and aims at a swift agreement by co-legislators by the end of 2021.

[19] Council Framework Decision 2008/841/JHA of 24 October 2008 on the fight against organised crime, OJ L 300, 11.11.2008.

[20] The EU SOCTA is produced every four years by Europol, on the basis of extensive input provided by Member States and other relevant stakeholders. It identifies key crime threats in the EU and proposes EU crime priorities for the next four years. The EU SOCTA is the first step of each EMPACT cycle, and is used as a basis upon which the Council adopts EU crime priorities to concentrate on in the next four years.

[21] Proposal for a Regulation of the European Parliament and of the Council amending Regulation (EU) 2016/794, as regards Europol's cooperation with private parties, the processing of personal data by Europol in support of criminal investigations, and Europol's role on research and innovation, COM(2020) 796 final, and Proposal for a Regulation of the European Parliament and of the Council amending Regulation (EU) 2018/1862 on the establishment, operation and use of the Schengen Information System (SIS) in the field of police cooperation and judicial cooperation in criminal matters as regards the entry of alerts by Europol, COM(2020) 791 final, 9 December 2020.

One of the key tools to implement the present Strategy and to step up efforts against organised crime structures through coordinated operations is the **European Multidisciplinary Platform Against Criminal Threats (EMPACT)**. Since 2010, EMPACT enables Member States to identify the EU priority crime threats where collective action is needed[22] and to tackle these criminal threats through a structured cooperation at EU level between law enforcement, customs, tax authorities, magistrates, European institutions and agencies and, where relevant, third countries, international organisations and the private sector[23].

Through EMPACT, Member States and their partners carry out over **200 joint operational actions every year**, aimed at fighting organised crime, for instance developing a criminal intelligence picture on EU crime priorities, building law enforcement capacities to target specific crimes, reinforcing cooperation with international partners, carrying out prevention activities, joint investigations against specific crime phenomena or specific criminal groups, and addressing the methods of these criminal groups to launder money, commit crimes online or obtain fraudulent documents. Although EMPACT already delivers significant operational results, for instance in terms of drugs seized or criminals arrested, it is currently not used to its full potential. Its complexity, lack of awareness among frontline officers and insufficient funding do not always ensure the ownership and active involvement of Member States and external partners, and hamper the development of more complex operations that would more significantly harm organised crime groups.

The Commission will work, together with all relevant EMPACT stakeholders to put in place a number of measures, outlined in detail in the Staff Working Document accompanying this Strategy, in order to use EMPACT to its full potential, and turn it into a true EU flagship instrument for **multidisciplinary and multiagency operational cooperation** to fight organised crime at EU level.

The Commission will also assess the feasibility of casting the EMPACT mechanism into EU legislation. This would firmly establish EMPACT as a key EU instrument for Member States and relevant EU agencies and bodies to cooperate operationally in the fight against organised and serious international crime. It would make EMPACT the permanent vector of structural cooperation between European and national crime strategies and actions, with a harmonised methodology and approach, as a legal foundation for ad hoc joint partnerships based on operational needs. The Commission will also seek to significantly reinforce the funding of EMPACT, to enable it to develop more complex operations. The Commission will also explore, together with all relevant stakeholders, the possibility to streamline the current EMPACT along four modernised and upgraded pillars[24], complemented by guiding principles

[22] For the period 2018-2021: Cybercrime, Drugs trafficking, Facilitation of illegal immigration, Organised property crime, Trafficking in human beings (for all forms of exploitation, including sexual and labour exploitation as well as all forms of child trafficking), Excise and MTIC fraud, Illicit firearms trafficking, Environmental crime, Criminal finances and money laundering & Document fraud.

[23] The "EU Policy Cycle for organised and serious international crime" used to define the cooperation framework for setting common priorities, "EMPACT" being the operational platform enabling cooperation between practitioners. "EMPACT" has now become the sole name to designate the two concepts.

[24] Renovated four-pillar sequence: 1/ observe, detect & orient. 2/ decide & plan together. 3/ fight, prevent & disrupt, 4/ hold learn & repeat.

against organised crime. Furthermore, it will aim to increase the role of European networks and expert groups in supporting EMPACT actions. Finally, the Commission, together with the European External Action Service, will promote the increased association of third countries to EMPACT activities, and promote the development of the EMPACT methodology outside the EU, tailored to operational needs.

In order to bring criminals to justice, law enforcement and judicial authorities need to work hand in hand: an effective response to organised crime requires further steps to reinforce further judicial cooperation. The recommendations of the Parliament[25] and Council Conclusions[26] call for improvements of the practical operation of the **European Arrest Warrant**[27]. The Commission is therefore enforcing the correct implementation, following the Commission's report on the implementation of the European Arrest Warrant[28], and will provide guidance in an updated handbook.

Moreover, to avoid parallel investigations on those criminals operating across several jurisdictions, common rules could be necessary to allow Member States to transfer criminal proceedings to another Member State, for example the Member State of nationality of the suspect, taking into account the Framework Decision for the prevention of conflicts of jurisdiction[29]. The Commission is currently further studying this issue to explore the need for EU action in this area. The Commission is also looking into problems arising with regard to the collection, transfer and use of evidence in cross-border proceedings and possible ways forward[30].

The communication and sharing of information within Joint Investigation Teams is essential and the Commission will therefore work on developing a Joint Investigation Teams collaboration platform and on stepping up Eurojust cooperation with third countries. Moreover, as announced in the Communication on the digitalisation of justice in the EU[31], the Commission will present by the end of 2021 a proposal to enable the secure electronic communication and exchange of information and documents between courts, national authorities, and justice and home affairs agencies where relevant. The Commission will also support modernising Eurojust's case management system to help Eurojust provide feedback to national authorities and develop judicial links between ongoing investigations. This should enable Eurojust to work efficiently with its partners, in particular Europol and the EPPO,

[25] https://www.europarl.europa.eu/doceo/document/TA-9-2021-0006_EN.html.
[26] https://data.consilium.europa.eu/doc/document/ST-13214-2020-INIT/en/pdf.
[27] Cf. Handbook on how to issue and execute a European arrest warrant, OJ C 335, 6.10.2017: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52017XC1006(02)&from=DA.
[28] Report of 2 July 2020 from the Commission to the European Parliament and the Council on the implementation of Council Framework Decision of 13 June 2002 on the European arrest warrant and the surrender procedures between Member States, COM(2020) 270 final, 2.7.2020.
[29] Council Framework Decision 2009/948/JHA of 30 November 2009 on prevention and settlement of conflicts of exercise of jurisdiction in criminal proceeding, OJ L 328, 15.12.2009.
[30] A study on the "Cross-border use of evidence" has been launched in March 2020.
[31] Commission Communication on the Digitalisation of justice in the European Union - A toolbox of opportunities, COM(2020) 710 final, 2.12.2020.

helping to coordinate investigations at national level and avoid parallel investigations with the aim of ensuring effective prosecutions.

1.3. International cooperation

Law enforcement cooperation beyond the Union is necessary to disrupt global criminal networks and transport routes. It is essential to step up international cooperation including through the activities of the relevant justice and home affairs agencies, in particular in relation to the neighbourhood and enlargement countries.

There is an urgent need to further develop serious and organised crime intelligence at Europol and enhance information exchange and investigative actions with third countries and regions constituting major hubs for high-risk organised crime affecting EU Member States, including via Member States' bilateral Liaison Officers seconded to these critical areas. The Commission has received directives for negotiating international agreements with third countries to exchange personal data with Europol[32] and to enable judicial cooperation with Eurojust[33] and it will strive to make progress in these difficult negotiations.

Furthermore, EU international cooperation programmes and projects are relevant to build trans-continental law enforcement and criminal justice networks. The Commission's support for such networks and to joint operations will continue to expand.

The EU approach to external security within the framework of the Common Foreign and Security Policy and the Common Security and Defence Policy remains an essential component of EU efforts to countering organised crime in order to strengthen stability and protect European security interests. The High Representative/Vice-President, supported by the European External Action Service, will continue to play a key role in enhancing strategic and operational cooperation with third countries and international organisations, by making full use of its external tools, such as the High Level Dialogues, the network of Counter-Terrorism/Security experts in EU Delegations and, where relevant, Common Security and Defence Policy missions and operations. Moreover, the Commission and the European External Action Service will continue to prioritise capacity building projects in third countries and in particular the neighbourhood and enlargement countries, both to support operational cooperation with EU Member States and agencies and to equip partners with the tools allowing them to root out complex criminal structures potentially affecting the EU.

Interpol is another key actor when it comes to international cooperation against organised crime. Interpol's 18 databases contain over 100 million law enforcement records, including on wanted criminals, suspected terrorists, fingerprints, stolen vehicles, stolen and lost travel documents, weapons and firearms. These databases enable law enforcement and judicial authorities to identify links and thus facilitate investigations against transnational organised crime. The Commission is adopting alongside this Strategy **a recommendation to the**

[32] Algeria, Egypt, Israel, Jordan, Lebanon, Morocco, Tunisia, Turkey and New Zealand.
[33] Algeria, Argentina, Armenia, Bosnia and Herzegovina, Brazil, Colombia, Egypt, Israel, Jordan, Lebanon, Morocco, Tunisia and Turkey.

Council to open negotiations with Interpol on an EU-Interpol cooperation agreement in order to improve cooperation and address operational needs.

The main international instrument enabling cooperation and mutual legal assistance in organised crime investigations is the **United Nations Conventions against Transnational Organized Crime** (UNTOC), which the EU and Member States are party to. In 2021, the Commission will update the declaration of competence to bring it in line with the Lisbon Treaty changes[34] and to ensure that the **European Public Prosecutor's Office** (EPPO) can make use of UNTOC rules on international mutual legal assistance to cooperate with third countries' authorities. In addition, the Commission will explore the possibility of notifying the EPPO as a responsible authority in the context of existing Union-level cooperation agreements with third countries and, where necessary, will consider opening negotiations with selected priority third countries. As expressed in the Kyoto Declaration adopted at the 14th UN Congress on Crime Prevention and Criminal Justice, the Union and Member States are fully committed to strengthening the international framework promoting the rule of law, crime prevention and criminal justice, including through an active engagement in the ongoing processes to review the implementation of UNTOC and the United Nations Convention against Corruption (UNCAC).

Key actions:

The Commission will:

- Propose to strengthen **the Prüm framework** (Q4 2021);
- Propose the creation of an EU **Police Cooperation Code** (Q4 2021);
- Propose to revise the **Advanced Passenger Information** Directive (Q1 2022);
- Establish a **collaboration platform** for Joint Investigation Teams (Q4 2021);
- Work with all relevant stakeholders, to **streamline, expand and modernise** the European Multidisciplinary Platform Against Criminal Threats (**EMPACT**) and establish it as **the EU flagship instrument to fight organised and serious international crime** through a set of actions and a legislative proposal (2023);
- Significantly **reinforce funding** for EMPACT through the Internal Security Fund for the period 2021-2027;
- Start negotiations for agreements on **cooperation** between **Eurojust** and third countries;
- Step up negotiations on cooperation between **Europol** and third countries;
- Reinforce, jointly with the European External Action Service, **international cooperation** with third countries and international organisations.

[34] The entry into force of the Treaty of Lisbon on 1 December 2009 and the end of the transition period for former third pillar instruments on 1 December 2014 have changed the boundaries of EU powers relevant for implementing this Convention. The EU acquired new competences under Title V of the TFEU (Articles 82 and 83), and has exercised its competence by legislating in relevant policy areas. Further, the UNTOC review process should be based on an updated declaration of competence.

The European Parliament and the Council are invited to:

- Advance in the legislative negotiations on the **Revision of the Europol Regulation**, including the amendments to the Schengen Information System Regulation, with the aim of reaching a **swift agreement**.

The Council is invited to:

- Adopt the recommendation to open the negotiations with **Interpol** on an EU-Interpol cooperation agreement.

2. Effective investigations: disrupting organised crime structures and tackling high priority crimes

2.1. Stepping up efforts on tackling organised crime structures

The focus of law enforcement investigations should not stop at the seizure of illegal items or the arrest of low-level criminals, but target actors and networks which are the backbone of criminal ecosystems.

With most criminal organisations structured around a core group or in a hierarchical way[35], the organised crime landscape is characterised by a networked environment where different groups and individuals systematically cooperate through 'joint ventures' within loose and fluid criminal networks. Criminal organisations orchestrating the supply chains in international criminal markets cooperate with smaller groups specialised in certain activities and with individuals in pivotal roles providing services to criminals such as document fraud, legal advice, encrypted communications or transportation. The capacity of the criminal groups to link each other undermines law enforcement efforts, since each segment of the criminal chain can be easily replaced in case of law enforcement intervention.

Against this landscape, it is crucial to scale up the **dismantling of organised crime structures**, targeting those groups that are a higher risk to Europe's security and the individuals in the higher echelons of criminal organisations. To this effect, some Member States have established structures at national level or specialised bodies in law enforcement and the judiciary against mafia-style organisations. These experiences have proven effective in spurring a strategic approach promoting efforts leading towards the disruption of criminal infrastructures. Moreover, the establishment of dedicated police units or judicial bodies would facilitate greater cross-border cooperation. The Commission will promote the exchange of best practices to facilitate the replication of such models across Member States, adapted to national specificities.

[35] According to the 2021 EU SOCTA report, 43 % of the organized crime groups are structured around a core group, 40 % are hierarchically structured and 17 % are loose networks.

At European level, the operational cooperation against mafia-style organised crime groups carried out through the **@ON Network**[36] facilitates the on-site deployment of specialised investigators across Member States to assist in investigations into cross-border organised crime groups. Another important milestone is the work carried out by Europol together with Member States to identify and carry out intelligence and investigative activities against selected **High Value Targets**[37], namely suspected members of criminal organisations posing a particularly high risk to two or more Member States.

To step up action against criminal organisations, further structural cooperation is highly needed. Developing **common criteria** for all Member States **to identify High-Value Targets** and facilitating real-time operational cooperation and information exchange would enable more joint and systematic investigations on those persons having a key role in a criminal network. The current @ON Network should be reinforced by incorporating all Member States and developing best practices, as well as through a closer link to EMPACT in its work against criminal networks.

A greater emphasis on organised crime investigations also requires a more robust **intelligence picture of the organised crime groups** that are at the heart of the complex web of organised crime networks. Europol and Member States should continue their work to develop intelligence-led strategic and tactical pictures on those groups that pose a greater threat to Europe's security, including through the development of ad hoc reports that complement the EU Serious and Organised Crime Threat Assessment (SOCTA). The exchange of strategic information with other actors, including Common Security and Defence Policy missions and operations can be beneficial in this regard. In addition, a better overview of the dimension of criminal activities and the actions taken by Member States is needed. Given the opaque nature of organised crime, it is difficult to measure and quantify these activities, and the data and statistics available to the European Union are fragmented, collected mainly through reporting obligations scattered around various legislative acts. Building on the outcome of a comprehensive study already carried out[38], the Commission will assess the need for a more systematic collection of statistics in this area.

2.2. A tailor-made response to specific forms of crime

According to the 2021 EU SOCTA, organised crime groups active in Europe are involved in a variety of criminal activities, with most criminal groups involved in drugs trafficking, organised property crime, followed by fraud (including customs, excise and VAT fraud), migrant smuggling and trafficking in human beings. While some groups are specialised in a particular criminal market, others are increasingly **poly-criminal**, using the profits of one

[36] Currently 16 Member States participate in the @ON Network which exists since 2014.
[37] Since 2018, this initiative has led to the arrest of 75 High Value Targets and 2529 of their associates, and to the seizing of assets worth €310 million.
[38] Study on the "Availability, Comparability and Consistency of Administrative Statistical Data on Recorded Crime and on the Stages of the Criminal Justice Process in the EU", March 2021, DR0121067ENN, https://data.europa.eu/doi/10.2837/065004.

criminal activity to finance their expansion into other crime areas. Specific forms of crime require a dedicated response from a legislative and policy perspective.

The EU has set out rules in relation to serious crimes such as migrant smuggling[39], and to detect and prohibit new psychoactive substances[40], to control the possession and trade of firearms and to prevent the reactivation of neutralised weapons[41]. Drugs trafficking remains a major source of income for organised crime groups and the EU set out the priorities for the next five years in the **EU Drugs Strategy 2021-2025**, which was adopted by the Council in December 2020[42]. The discussions on the related **Action Plan on Drugs** are continuing in the Council, while the Commission is preparing the first initiatives to implement the Strategy and the Action Plan[43].

Firearms are a key enabler of the increasing violence by criminal groups, allowing them to intimidate their opponents and exert control over their members and markets. In order to limit the availability of firearms in the hands of criminals, the Commission started the implementation of the new 2020-2025 EU Action plan **against firearms trafficking**. It will publish the application report of the Firearms Directive, identifying initial means of improving the legal framework.

Migrant smuggling remains a key activity for organised crime groups that endangers migrants and damages the migration management objectives of the EU. The Commission will adopt in 2021 a **new Action Plan against migrant smuggling** to combat criminal networks involved in this crime, support law enforcement and inter-agency cooperation and stimulate cooperation with third countries, as well as with Common Security and Defence Policy missions and operations wherever relevant.

Trafficking in human beings, a particularly abhorrent form of crime, is often committed by organised crime groups, which increasingly recruit their victims online, forge identity documents and work permits and exploit them for sexual purposes, forced labour, forced criminality or begging. While the priorities and actions of this Strategy cover trafficking in human beings, the Commission is also proposing alongside this Strategy a dedicated EU Strategy on Combating Trafficking in human beings 2021-2025 to address the specificities of this crime.

Cybercrime is becoming more aggressive and confrontational. The rapidly progressing digitalisation of society, which has seen a surge with the Covid-19 pandemic, creates new vulnerabilities that can be exploited by criminals involved in cyber-dependent crime.

[39] Council Framework Decision 2002/946/JHA of 28 November 2002 on the strengthening of the penal framework to prevent the facilitation of unauthorised entry, transit and residence, OJ L 328, 5.12.2002.
[40] Regulation (EU) 2017/2101 of the European Parliament and 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.
[41] https://ec.europa.eu/home-affairs/what-we-do/policies/organized-crime-and-human-trafficking/trafficking-in-firearms_en.
[42] Council Conclusions on the EU Drugs Strategy 2021-2025, 14178/20, 18 December 2020.
[43] https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12854-Alternatives-to-coercive-sanctions-for-drug-using-offenders.

Cyberattacks such as the creation and spread of malware, hacking to steal sensitive personal or industry data, or denial of service attacks, have increased over the last year both in number and degree of sophistication[44].

The **European Cybercrime Centre at Europol (EC3)**, which was established in 2013, has played a key role in tracking the exploitation of the Covid-19 pandemic by organised crime, and creating awareness raising materials and reports for the information of Member States and the public, as well as supporting investigations into online scams perpetrated by organised crime groups. In addition, it has published its regular **Internet Organised Crime Threat Assessment** (IOCTA) reports, which provide an important source of information for priority setting in operations and policy[45].

In line with the 2020 EU Strategy for a more effective fight against child sexual abuse and the EU Comprehensive Strategy on the Rights of the Child (2021-2025), in 2021 the Commission will propose legislation to improve the protection of children against **child sexual abuse**, including by requiring relevant online services providers to detect known child sexual abuse material and to report that material to public authorities[46]. The legislation will also ensure consistency with other legislative initiatives, in particular with the proposal on the Digital Services Act[47]. The Commission also continues to support the European Parliament and the Council in reaching an agreement as soon as possible on the proposal for a regulation regarding voluntary efforts by certain service providers in the fight against child sexual abuse online[48]. In parallel, Europol has been supporting the expansion of its successful "Trace an Object" campaign, which crowdsources information on individual objects in images showing child sexual abuse that can help narrow down the geographic location of an abuse and therefore eventually contribute to the identification and rescue of victims.

The move towards cashless economies, further accelerated by the pandemic, has created increased opportunities for fraud and counterfeiting of **non-cash means of payment** such as credit cards and online payment tools[49], which poses a serious threat to the EU's security. They provide an important source of income for organised crime and enable criminal activities such as drug trafficking and trafficking in human beings. The EU adopted stricter

---

[44] See the 2020 Internet Organised Crime Threat Assessment (iOCTA) at https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment, as well as Europol's other reports on https://www.europol.europa.eu/activities-services/staying-safe-during-covid-19-what-you-need-to-know.

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

[46] Commission Communication on an EU strategy for a more effective fight against child sexual abuse, COM(2020) 607 final, 24.7.2020.

[47] Proposal for a Regulation of the European Parliament and of the Council on a Single Market For Digital Services (Digital Services Act) and amending Directive 2000/31/EC, COM(2020) 825 final, 15.12.2020

[48] Proposal for a Regulation of the European Parliament and of the Council on a temporary derogation from certain provisions of Directive 2002/58/EC of the European Parliament and of the Council as regards the use of technologies by number-independent interpersonal communications service providers for the processing of personal and other data for the purpose of combatting child sexual abuse online, COM(2020) 568 final, 10.9.2020.

[49] https://www.europol.europa.eu/newsroom/news/beyond-pandemic-what-will-criminal-landscape-look-after-covid-19.

rules in 2019[50], which Member States have to implement by 31 May 2021. The Commission will closely monitor progress to ensure the full effectiveness of the new rules.

Fraud, including customs, excise and VAT fraud, is another area of crime that is becoming increasingly appealing for organised crime. In addition to current efforts by Europol and Eurojust in this area, the **EPPO** will investigate and prosecute offences regarding participation in a criminal organisation, if the focus of the criminal activity of such a criminal organisation is to commit offences affecting the Union budget, including serious cross-border VAT fraud.

Counterfeiting of products is a high impact crime. Counterfeit products represent 6.8% of EU imports[51] and are a significant source of income for organised crime groups. Medical, healthcare and sanitary products constitute a considerable and increasing share of counterfeiting, a phenomenon that has alarmingly increased with the Covid-19 pandemic. Organised crime has engaged in the production and supply of counterfeit protective equipment, test kits and pharmaceuticals, and there is a risk that organised crime groups try to exploit opportunities arising in the EU from the high demand for vaccines. Law enforcement authorities together with Europol and the European Anti-Fraud Office are successfully conducting important operations leading to significant arrests and seizures of counterfeit products, including medical products, toys, food and beverages[52]. However, more needs to be done to reinforce operational cooperation to address counterfeiting. Organised crime groups are increasingly involved in crimes such as counterfeiting of pesticides and fraudulent use of the EU organic logo. Building on its official controls and enforcement framework, the Commission will keep stepping up its efforts to tackle food fraud, and will work to empower national authorities, create a zero-tolerance policy and increase prevention, controls, deterrence as well as effective sanctions.

To this end, in November 2020, the Commission adopted the Intellectual Property Action Plan, and in 2022 it will establish an **EU Toolbox against counterfeiting** setting out principles for joint action, cooperation and data sharing among law enforcement authorities, right holders and intermediaries[53]. Given that counterfeiting of medical products mostly occurs in third countries, it is important to reinforce global governance, notably through the accession to and ratification by EU Member States, and possibly the Union itself, of the Council of Europe Convention on the **counterfeiting of medical products** (Medicrime

[50] Directive (EU) 2019/713 of the European Parliament and of the Council on combating fraud and counterfeiting of non-cash means of payment, OJ L 123, 10.5.2019.
[51] OECD/EUIPO (2019), Trends in Trade in Counterfeit and Pirated Goods, Illicit Trade, OECD Publishing, Paris/European Union Intellectual Property Office. https://doi.org/10.1787/g2g9f533-en.
[52] See for example operations Pangea XIII (medical items), LUDUS (toys) and Opson IX (food and beverages). During the Europol Coordinated Operation Shield, concluded in September 2020, almost 33 million COVID-19-related counterfeited medical devices were seized: this included 8 tonnes of raw materials, face masks, tests and diagnosis kits.
[53] Commission Communication Making the most of the EU's innovative potential. An intellectual property action plan to support the EU's recovery and resilience, COM(2020) 760 final, 25.11.2020.

Convention), which has been signed by fourteen Member States, out of which only six have ratified it[54].

Environmental crime deserves particular attention due to its harmful effects on biodiversity and on the environment, health and social cohesion within the EU and in third countries. All kinds of wildlife – plants, animals and derived products – as well as companion animals continue to be traded illegally, often on a large scale and sometimes with potential devastating consequences. Illegal waste management and shipments undermines the legitimate waste treatment and recycling industries. The EU has adopted legislation to regulate the legal trade of wildlife[55] and of waste[56] and required Member States to criminalise and set penalties on a broad range of environmental offences[57]. These legislative tools have been complemented with the 2016 Action Plan against Wildlife Trafficking and the 2018 Action Plan on Environmental Compliance and Governance. The European Anti-Fraud Office has significantly developed its operational activities in the fight against illicit trade of goods putting at risk the environment.

Despite these efforts, inspection, law enforcement and judicial authorities often lack the capacity and resources to effectively detect, investigate and prosecute environmental crime. This is particularly the case in Member States where there are no specialised enforcement or prosecution bodies and no established strategic approach to combating environmental crime. There is a need to strengthen the enforcement capacity at national and EU level. Sanctions imposed are not sufficiently dissuasive and the coordination and exchange of information within and across Member States, particularly between administrative authorities and law enforcement bodies, is insufficient[58]. The Commission is reviewing the **EU Waste Shipments Regulation** and the **Action Plan against Wildlife Trafficking**. The **Environmental Crime Directive** will be revised to clarify the scope of environmental crime offences, provide more precision with regard to sanctioning and facilitate the use of effective investigative tools and promote cross-border cooperation and information sharing. In addition, cooperation through the European environmental enforcement networks will be enhanced. Finally, since the international dimension of wildlife trafficking is crucial, the Commission will promote the adoption of an additional protocol under the UNTOC.

---

[54] Convention CET nº 211. The Convention has been ratified by Belgium, Croatia, Spain, France, Hungary and Portugal. It was signed but not yet ratified by Austria, Cyprus, Germany, Denmark, Finland, Italy, Luxembourg and Slovenia. In addition to the Medicrime Convention, Directive 2011/62/EU of the European Parliament and of the Council of 8 June 2011 amending Directive 2001/83/EC on the Community code relating to medicinal products for human use, as regards the prevention of the entry into the legal supply chain of falsified medicinal products, OJ L 174, 1.7.2011, establishes rules and mechanisms to strengthen the verification requirements applicable to the manufacturer of the medicinal product for that purpose.

[55] https://ec.europa.eu/environment/cites/legislation_en.htm.

[56] See article 50 of Regulation 1013/2006 of the European Parliament and of the Council of 14 June 2006 on the shipments of waste, OJ L 190, 12.7.2006.

[57] Directive 2008/99/EC of the European Parliament and of the Council on the protection of the environment through criminal law, OJ L 328, 6.12.2008 (Environmental Crime Directive).

[58] Evaluation of the Directive 2008/99/EC of the European Parliament and of the Council of 19 November 2008 on the protection of the environment through criminal law (Environmental Crime Directive), SWD(2020) 259 final, 28.10.2020.

Trafficking of **cultural goods** has a devastating impact on countries' cultural heritage and it provides means of financing for criminal organisations and it is instrumental for money laundering. Improved monitoring and information exchange, reinforced law enforcement and customs cooperation, enhanced Justice and Home Affairs-Common Security and Defence Policy cooperation in the field and drawing on the expertise of different public and private actors are needed for an effective response to this crime. Rapid access to archaeologists and art historians can be greatly contribute to investigations into the trafficking of cultural goods. In order to tackle this unique form of crime, the Commission will continue to support capacity building amongst cultural heritage experts, including a network of such experts that Member States could use in the EMPACT framework. Their structured cooperation with law enforcement will be supported so as to facilitate investigations as well as the funding of projects on trafficking in cultural goods. Furthermore, the Commission will examine other necessary actions to address this phenomenon including through the improvement of the online and offline traceability of cultural goods in the internal market, the cooperation with third countries where cultural goods are looted. To this end, the Commission will propose an Action Plan on tackling the illicit trade in cultural goods in 2022.

Key actions:

The Commission will:

- Propose amendments to the **Environmental Crime Directive** (Q4 2021);
- Strengthen the provisions on enforcement against illegal shipments of waste as part of its proposal amending the **waste shipment regulation** (Q2 2021);
- Establish an **EU Toolbox against counterfeiting** setting out principles for joint action, cooperation and data sharing among **law enforcement authorities**, right holders and intermediaries (2022);
- Propose an **Action Plan on trafficking of cultural goods** (2022);
- Explore the possibility for the Union to accede to the Council of Europe **Medicrime Convention**.

Member States are urged to:

- **Join and strengthen the @ON Network** on mafia type organised crime groups and explore a more structured integration of a **targeted approach against criminal networks into EMPACT**;
- Establish or further develop coordination structures at national level or **specialised bodies** in law enforcement and judiciary authorities focused on tackling organised crime structures;
- Accede and ratify the Council of Europe **Medicrime Convention**.

Member States and Europol are urged to:

- Develop common identification criteria to select and investigate **High Value Targets**

and prioritise investigations against individuals and criminal networks posing the highest security risk in the EU;

- Develop a strategic and tactical **intelligence picture** on high-risk organised crime groups;
- Reinforce strategic and operational **cooperation** in the fight against **counterfeiting of medical products**, including with the European Anti-Fraud Office and the European Union Intellectual Property Office and at global level.

3. Eliminating profits generated by organised crime and preventing infiltration into the legal economy and society

3.1. Reinforcing asset recovery and anti-money laundering measures, promoting financial investigations

Organised crime in the EU fundamentally relies on the ability to launder vast amounts of criminal profits. While three fourths of criminal organisations still use basic methods to hide their illicit gains, such as investing in real estate or other high-value goods, others rely on increasingly sophisticated methods, with the assistance of white-collar money launderers[59]. The financial trail that criminals leave behind is a key indicator of their activity, providing useful leads for investigators and invaluable evidence to incriminate perpetrators. Therefore, tackling criminal finances is crucial to uncover criminal activities, to deter crime, and to prevent infiltration in the legal economy and society.

Despite the development of the anti-money laundering and asset recovery legal frameworks, only a minor share of money laundering activities is detected, and only 1% of criminal assets is confiscated[60]. This has been aggravated by the increasing use of financial channels with more limited oversight than the banking sector, such as **virtual currencies**.

The fight against criminal finances needs to be reinforced. As highlighted in the 2020 Anti-Money Laundering Action Plan[61], the EU anti-money laundering framework needs to be significantly improved to address major divergences in the way it is applied and serious weaknesses in the enforcement of the rules. Financial investigations are not being used to their full potential, partly due to the insufficient capacity in law enforcement to carry out these complex and burdensome enquiries.

In addition, the ability to deprive criminals from their illegally obtained assets is further hindered by the narrow scope of the confiscation legal framework in terms of assets and criminal activities covered. Moreover, Asset Recovery Offices currently face challenges when

[59] Europol, 2021 EU Serious and Organised Threat Assessment Report (EU SOCTA), 12 April 2021, https://www.europol.europa.eu/activities-services/main-reports/european-union-serious-and-organised-crime-threat-assessment.
[60] Europol, Does crime still pay? Criminal Asset Recovery in the EU – Survey of statistical information 2010-2014, 2016, available at: https://www.europol.europa.eu/publications-documents/does-crimestill-pay.
[61] Communication from the Commission on an Action Plan for a comprehensive Union policy on preventing money laundering and terrorist financing, C(2020) 2800 final, 7.5.2020.

tracing assets as they are lacking, for example, temporary freezing powers in order to prevent the dissipation of assets or direct and immediate access to certain public registers such as central land registers or central company registers[62]. Moreover, the recovered assets are also not always managed in an efficient manner and are not sufficiently used to compensate victims or to benefit society.

As announced in the 2020 Anti-Money Laundering Action Plan, ensuring effective implementation of the existing anti-money laundering framework is a priority. In addition to ongoing efforts to ensure adequate implementation, the Commission is preparing legislative proposals aimed at reinforcing and developing the **EU Anti-Money Laundering Framework** by proposing in the second quarter of 2021 to establish a directly applicable single rule book, to strengthen EU-level supervision and to establish an EU coordination and support mechanism for Financial Intelligence Units.

It is equally necessary to further promote a culture of **early financial investigations** in all Member States and to build up investigators' capacity to tackle the financial dimension of organised crime. The 2020 Council Conclusions on enhancing financial investigations[63] call on Member States to ensure that financial investigations form part of all kinds of criminal investigations regarding organised crime. Moreover, through the establishment of the European Financial and Economic Crime Centre, Europol has stepped up its capacities to support Member States in conducting financial investigations.

It is equally essential to step up **freezing and confiscation** efforts through a further reinforced legal framework at EU level and stronger operational capacities of **Asset Recovery Offices**. Non-conviction-based confiscation measures should be explored as they can contribute to increasing the amount of confiscated assets when, for example, it is not possible to link the obtained assets to a criminal conviction[64]. To provide for a stronger confiscation regime and equip national Asset Recovery Offices with a more effective mandate, the Commission will propose in 2022 a revision of the 2014 **Confiscation Directive** and of the 2007 Council Decision on **Asset Recovery Offices**[65] to expand the scope of criminal offences covered, introduce more effective rules on non-conviction based confiscation; ensure effective management and social reuse of confiscated assets and compensation of victims of crime and reinforce the capacity of Asset Recovery Offices to trace and identify illicit assets[66].

Moreover, the Commission will consider possible options regarding the **systematic launching of financial investigations** and post-conviction financial investigations. Swift

[62] See Council Conclusions on enhancing financial investigations to fight serious and organised crime, 8927/20, 17 June 2020.
[63] Council Conclusions on enhancing financial investigations to fight serious and organised crime, 8927/20, 17 June 2020.
[64] See also the Analysis of non-conviction-based confiscation measures in the European Union, SWD(2019) 1050 final, 12.4.2019.
[65] https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12725-Freezing-and-confiscation-of-the-proceeds-of-crime.
[66] Report of the Commission to the European Parliament and to the Council, "Asset recovery and confiscation, ensuring that crime does not pay," COM(2020) 217 final, 2.6.2020.

access to financial information is essential for carrying out effective financial investigations and for successfully tracing and confiscating assets. The timely transposition by Member States of the **Directive on facilitating access to financial information,** which provides law enforcement authorities with access to centralised bank account registries and strengthens cooperation between law enforcement authorities and Financial Intelligence Units is therefore of outmost importance. The Commission will also revise the Directive along with the Anti-Money Laundering Framework in order to provide law enforcement authorities access to the future platform interconnecting bank account registries across the Union.

Simultaneously, it will be necessary to improve international cooperation on the repressive response to money laundering. Member States should make full use of the possibilities offered by the **Anti-Money Laundering Operational Network (AMON)**, an informal international network of law enforcement anti-money laundering unit, and the **Camden Asset Recovery Inter-agency Network (CARIN)**, an informal network of law enforcement and judicial practitioners specialised in the field of asset tracing, freezing, seizure and confiscation. The Commission will also propose the ratification, on behalf of the EU, of the Council of Europe **Warsaw Convention** on Money Laundering, Freezing and Confiscation.

3.2. Stepping up anti-corruption measures

Corruption is a central part of the modus operandi of organised crime groups. They bribe, intimidate and use force on public officials and personnel in key entities such as ports to stay off the radar, obtain information or to facilitate their activities. Under the current EU anti-corruption rules, Member States are required to criminalise both active and passive corruption of public officials, establish adequate sanctions and ensure that entrepreneurs corrupting officials are held criminally liable. However, these instruments do not cover certain corruption-related offences, such as trading in influence, abuse of power, illicit enrichment, misappropriation or other diversion of property by a public official. More recently, the Union introduced new legislation protecting whistle-blowers and requiring the creation of safe channels for reporting corrupt practices. The annual Rule of Law report examines the situation of Member States also in relation to anti-corruption policies.

In order to step up efforts at EU level, the Commission will **assess the existing EU anti-corruption rules**[67], which were adopted twenty years ago, to assess whether they are up to date with evolving criminal practices and to ensure that they cover all relevant corruption-related offences.

The various forms of corruption linked to organised crime in a transnational context also justify the need for improved sharing of expertise, best practices, data and information among Member States and with civil society. In order to effectively support criminal investigations through the exchange of data, it is crucial to have an overview and understanding of the risks and threats caused by corruption before they materialise into corruption-related crimes.

[67] Council Framework Decision 2003/568/JHA of 22 July 2003 on combating corruption in the private sector and the 1997 Convention on the fight against corruption involving officials of the European Communities or officials of Member States of the European Union, OJ L 192, 31.7.2003.

The Covid-19 pandemic adds another serious layer of corruption risks: the large-scale resource mobilisation to respond to the health and economic crisis has indirectly created new opportunities for corruption. It is necessary to reinforce national authorities' capacity to address highly complex corruption cases related to organized crime, in particular by setting up specialised anti-corruption structures. It is important that Member States make further use of available funding and technical support instruments provided by the Commission in order to reinforce their structural and strategic approach, regulatory and operational tools and capacity in the area of the fight against corruption. Furthermore, given the crucial role of the media in uncovering corruption cases, it is of paramount importance to ensure the safety of investigative journalists across the Union, including against abusive litigation. As announced in the European Democracy Action Plan, in 2021 the Commission will issue a Recommendation on the safety of journalists, and put forward an initiative to fight abusive litigation against journalists and rights defenders.

The EU is party to **United Nations Convention against Corruption** since 2008 and it will be subject to the review of implementation foreseen under the Convention. The EU and the Member States are working in the framework of the Council of Europe's Group of States against Corruption (GRECO) and G20 to make further progress in the prevention and fight against corruption. The Special Session of the United Nations General Assembly, planned for June 2021, will be a major opportunity to advance the fight against corruption at global level.

Member States are also required to criminalise and prosecute the acts of corruption committed by EU citizens and companies in partner countries in line with the obligations under the **OECD Convention on Combating Bribery of Foreign Public Officials in International Business Transactions**. The consistent prosecution and adjudication of the acts of corruption committed abroad will play an important role in addressing corruption globally.

3.3. Addressing infiltration in the economy and society

Criminal groups invest part of their considerable earnings in legal businesses across sectors as varied as real estate and construction, transportation or hospitality[68]. By controlling companies in those sectors, criminal organisations are able to launder the illegal assets and maximise their profits. Organised crime infiltration hurts the licit economy and distorts market rules. Due to the economic situation generated by the Covid-19 pandemic, there is a heightened risk of organised crime taking over weakened companies and infiltrating entire business sectors. There is already proof of criminal attempts to defraud the various financial mechanisms established to support economic recovery[69]. In order to address this threat and to identify key points for intervention and awareness raising, Member States and Europol need to build up the intelligence picture about the scale and degree of criminal investments, the infiltration methods and the sectors at risk.

[68] Study on Mapping the risk of serious and organised crime infiltration in legitimate businesses, March 2021, DR0221244ENN, https://data.europa.eu/doi/10.2837/64101.

[69] Europol, 2021 EU Serious and Organised Threat Assessment Report (EU SOCTA), 12 April 2021 https://www.europol.europa.eu/activities-services/main-reports/european-union-serious-and-organised-crime-threat-assessment.

Lessons could be drawn from the exchange of best practices promoted through the European Network on the **Administrative Approach**[70], a method whereby local authorities, in collaboration with law enforcement authorities and civil society, use administrative tools such as procedures for obtaining permits, tenders and subsidies to prevent organised crime infiltration of legal businesses and administrative infrastructure. Local authorities should be empowered, in full respect of fundamental rights, to set up barriers that protect the economic fabric against organised crime.

The **local dimension** is also key to reduce the space for criminal groups to fill their ranks. Individuals raised in an organised crime environment and in socio-economically deprived areas are most vulnerable to recruitment for criminal activities. Starting from petty criminality or minor roles in the organisation, they will become the members and leaders of tomorrow's criminal organisations. Targeted actions in neighbourhoods and communities have proven successful in offering alternatives that prevent young people from joining a life of violence and crime. Moreover, crime prevention activities such as community policing or awareness campaigns in areas particularly affected by criminal activity are essential to raise the resilience of society against the activities of organised crime groups. The Commission will enhance the exchange of knowledge and best practices on crime prevention through the **European Crime Prevention Network**.

Key actions:

The Commission will:

- Propose the revision of the **Confiscation Directive** and the Council Decision on **Asset Recovery Offices** (2022);
- Assess existing **EU anti-corruption rules** (2022);
- Promote **cooperation** and the exchange of information on the **link between corruption and organised crime**, including through Europol.

Member States are urged to:

- **Systematically conduct financial investigations** in organised crime investigations and, as soon as the financial environment indicates the presence of criminal assets, systematically undertake asset recovery investigations;
- Swiftly transpose the **Directive on facilitating access to financial information** by the deadline of August 2021;
- **Exchange strategic information** with those **sectors at risk** of being infiltrated by organised criminality groups (public-private partnerships);
- Enhance the **specialisation** of law enforcement services, and strengthen the bodies responsible for investigations, prosecutions and judicial proceedings of high-level

[70] The administrative approach to serious and organised crime is complementary to traditional law enforcement activities. It offers additional tools to prevent and tackle the misuse of the legal infrastructure through multi-agency cooperation by sharing information and taking actions in order to set up barriers against infiltration.

corruption cases.

Member States and Europol are urged to:

- Improve the **intelligence picture** on the threat of **infiltration** in the legal economy, by assessing the risks and methods used by organised crime groups.

4. Making law enforcement and the judiciary fit for the digital age

4.1. Access to digital leads and evidence

The search for leads and evidence, including lawful access to communications data, is the cornerstone of law enforcement investigations and prosecutions, bringing criminals to justice. As our lives and activities have moved online more than ever, footprints of crime are also digital. Organised crime is planned, executed and concealed online, marketing illegal substances and products and finding ingenious ways to launder profits, unhindered by physical borders. The scale of the problem is amplified by fast developing technologies. The shift of some leads and evidence from a physical to an online space brings a variety of challenges, including the speed with which the data can be moved across jurisdictions, or the ability to hide behind encryption. In addition, some **evidence-gathering instruments and measures designed for physical evidence are not yet fully adapted to the digital world**[71]. This may hamper or slow down criminal investigations and prosecutions because data is not available or accessible in a timely manner.

Investigations of organised crime commonly require access to electronic communications data to make a link between the crime, the perpetrator and their victims, as well as to trace criminal networks. These communications, given the scale and structure of an organised crime network, are difficult for law enforcement to trace without retrospective access to communications metadata. Lack of such data makes it particularly challenging to identify the central actors pulling the strings in the background. Identification and arrest therefore often only touches the lowest ranks of these networks, those who were at the site of the crime, rather than the central actors[72]. In addition, organised crime groups use modern technology to arrange the next drug drop-off, to share promising targets for the next burglary, to agree the meeting point for an armed robbery, or, in the case of cybercriminal organised crime groups, to execute online banking malware attacks.

To ensure access to digital evidence and investigative leads, Member States have established **data retention frameworks**. Given the principle of confidentiality of electronic communications, communication service providers may have erased the metadata by the time law enforcement authorities request access to it. In such cases, important evidence may be lost, unless providers are required by law to store communications metadata for a reasonably

[71] https://ec.europa.eu/info/policies/justice-and-fundamental-rights/criminal-justice/e-evidence-cross-border-access-electronic-evidence_en#internaleurulesproposaloneevidence.
[72]https://www.bka.de/SharedDocs/Kurzmeldungen/DE/Kurzmeldungen/180611_MINDESTSPEICHERFRISTEN.html.

longer period under a data retention legislative framework. This risks resulting in crimes not being successfully investigated or victims not being identified. Communications metadata are, for example, of particular importance in the investigation and prosecution of cybercrime, and are often the primary means of detecting the crime and act as key pieces of evidence. They can also be an important means of corroborating (or disproving) other types of evidence relating to the facts of the case. Furthermore, the complexity of organised crime, such as illegal drugs trafficking or trafficking in human beings or money laundering, and the time it takes to investigate such crime, with new suspects only becoming apparent through the course of the investigation, underscores the relevance of data retention.

At the same time, data retention measures raise important questions in relation to their interference with fundamental rights, including the right to privacy and protection of personal data. In its recent judgements on data retention[73], the Court of Justice of the European Union confirmed its previous jurisprudence that electronic communications data are confidential and, in principle, traffic and location data cannot be retained in a general and indiscriminate manner. The scope of data retention measures can only be justified in relation to their interference with fundamental rights when they are necessary and proportionate to the objective pursued. The Court set out circumscribed exceptions to this rule concerning national security, public defence and security or crime prevention, investigation, detection and prosecution[74]. The Commission will analyse and outline possible approaches and solutions, in line with the Court's judgements, which respond to law enforcement and judiciary needs in a way that is operationally useful, technically possible and legally sound, including by fully respecting fundamental rights. It will consult Member States before the end of June 2021 with a view to devising the way forward.

An effective law enforcement response also requires timely access to digital evidence when held by providers in a different jurisdiction. In 2018, the Commission proposed **the e-evidence package** to facilitate access to electronic evidence across borders on the basis of European Production and Preservation Orders. The European Parliament and the Council are now engaging in inter-institutional discussions, supported by the Commission, to find the necessary common ground leading to the swift adoption of these proposals. Moreover, as part of the efforts to speed up the digitalisation of law enforcement and the judiciary[75], all Member States should participate in the e-Evidence Digital Exchange System (eEDES). In parallel, swift progress is needed in multilateral and bilateral international negotiations to facilitate

[73] Judgments in Case C-623/17, *Privacy International* and Joined Cases C-511/18, C-512/18 and C-520/18 *La Quadrature du Net a.o.* of 6 October 2020 and Case C-746/18 *H.K. v Prokuratuur* of 2 March 2021.
[74] The Court notably allowed general and indiscriminate retention of the civil identity of users for the purpose of fighting all crimes, and general and indiscriminate retention of IP addresses assigned to the source of an Internet connection for the purpose of fighting serious crimes. The reasoning of the Court of Justice is based on the Charter of Fundamental Rights and the analysis of the necessity and proportionality of the interference with those rights.
[75] Commission Communication on the Digitalisation of justice in the European Union: A toolbox of opportunities, COM(2020) 710 final, 2.12.2020.

cooperation with international partners and establish compatible rules at international level for cross-border access to e-evidence[76].

In view of increasingly large-scale attacks, gathering electronic evidence as soon as possible and before remediation remains essential for successful investigations, which facilitate deterrence. To this end, law enforcement and the cybersecurity community should cooperate closely to ensure a collective and comprehensive response. In addition, investigations require swift and reliable access to WHOIS data, *inter alia* to help identify organised criminal groups that regularly abuse the Domain Name System (DNS) and other internet protocols in their cyberattacks or for other crimes such as scams or dissemination of illegal products and services.

Encryption is essential to the digital world, securing digital systems and transactions and also protecting a series of fundamental rights, including freedom of expression, privacy and data protection[77]. However, if used for criminal purposes, it masks the identity of criminals and hides the content of their communications. The Commission proposed, in its 11th progress report towards an effective and genuine Security Union[78], a set of six practical measures to support law enforcement and the judiciary when they encounter encryption of data stored on devices (such as phones or hard drives) in criminal investigations without prohibiting, limiting or weakening encryption. As part of these measures, Europol's new decryption facility launched by the Commission in December 2020 will contribute to address those challenges. Training modules have been developed and pilot courses delivered by the European Cybercrime Training and Education Group (ECTEG), funded via the Internal Security Fund-Police. These courses will feature in the regular training offer of the European Police College (CEPOL).

Beyond mainstream devices, the niche market for encrypted communication devices, which are also acquired and used by organised crimes groups, is on the rise. As showcased by the recent Encrochat and Sky ECC operations, EU law enforcement authorities need to continuously develop their capacity to deal with encrypted information in the context of criminal investigations, in line with applicable laws.

In December 2020, the Council adopted a resolution[79] which calls for an active discussion with the technology industry and the development of an appropriate regulatory framework that would allow national authorities to carry out their operational tasks effectively while protecting privacy, fundamental rights and the security of communications. Furthermore, the Council asked for the improvement of the coordination of the efforts of Member States and European Union institutions and bodies. As already announced in the Counter-Terrorism

[76] In particular, the Second Additional Protocol to the Council of Europe 'Budapest' Convention on Cybercrime and an agreement between the EU and the United States on cross-border access to e-evidence.
[77] Commission Communication on the EU Security Union Strategy, COM(2020) 605 final, 24.7.2020; Commission Communication on the First Progress Report on the EU Security Union Strategy, COM(2020) 797 final, 9.12.2020.
[78] Eleventh progress report towards an effective and genuine Security Union, COM/2017/608 final, 18.10.2017.
[79] Council Resolution on Encryption - Security through encryption and security despite encryption, 13084/1/20 REV 1, 24.11.2020.

Agenda[80], the Commission is working to identify technical, operational, and legal solutions to ensure lawful access to encrypted information, while maintaining the effectiveness of encryption in protecting privacy and security of communications.

In 2020, the Commission, together with industry, cryptography experts, members of civil society organisations and competent authorities, conducted an expert process to identify technical solutions that may help companies to specifically detect child sexual abuse in end-to-end encrypted electronic communications. The Commission will support research to identify which technical solutions are the most feasible and could be scaled up and feasibly and lawfully implemented by companies.

More broadly, the Commission will steer the process to analyse with the relevant stakeholders the existing capabilities and approaches for lawful and targeted access to encrypted information in the context of criminal investigations and prosecutions. These approaches should not result in a general weakening of encryption or in indiscriminate surveillance. This analysis will not only focus on addressing the current obstacles but will also anticipate the likely evolution of encryption and decryption technologies, and the necessary cooperation with academia and the private sector to this end. In addition, the Commission is enhancing its efforts in the field of standardisation to maintain lawful interception capabilities in the context of 5G and beyond. As a result of this process the Commission will suggest **a way forward** in 2022 to address the issue of lawful and targeted access to encrypted information in the context of criminal investigations and prosecutions that shall be based on a thorough mapping of how Member States deal with encryption together with a multi-stakeholder process to explore and assess the concrete options (legal, ethical and technical).

4.2. Effective tools and technologies

Law enforcement authorities often do not have the means to acquire the right tools needed for conducting digital investigations. More than 80% of crimes today have a digital component; even when crimes are committed offline, almost every law enforcement officer and prosecutor needs to know the basics of how to investigate crime online[81]. To detect and prosecute organised crime, investigators need to detect suspicious online activity, to track virtual currencies criminal transactions, to understand what they found (data can be encrypted or must be put in context with other data), to preserve the data and to use them as electronic evidence in court.

[80] Commission Communication on A Counter-Terrorism Agenda for the EU: Anticipate, Prevent, Protect, Respond, COM(2020) 795 final, 9.12.2020.

[81] Commission Staff Working Document – Impact Assessment accompanying the document Proposal for a Regulation of the European Parliament and of the Council on European Production and Preservation Orders for electronic evidence in criminal matters and 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, SWD/2018/118 final, 17.4.2018.

There is a pressing need to increase the capacity and capabilities of non-specialised law enforcement and prosecution services[82]. In addition, digital investigations expertise in specific areas such as the Internet of Things forensics[83] is lacking. Law enforcement authorities and the judiciary need to keep pace with the fast developing technologies used by criminals and their cross-border activities. This requires coordination in developing tools and trainings, among Member States and across sectors in areas such as digital forensics, open source intelligence, cryptocurrencies, and darkweb investigations, e.g. to gain access to, and where possible take down, forums selling illegal goods and services. Moreover, national authorities are not always able to use open-source technical solutions due to a lack of awareness about what solutions have been developed and are available, differences in requirements and levels of expertise, and a lack of support for further development and maintenance. At the same time, a lack of coordination between the various authorities and Member States brings about risks of duplicating initiatives. Existing EU mechanisms (EMPACT, EU Agencies such as Europol, CEPOL and Eurojust, networks of practitioners, funding programmes such as the Internal Security Fund) can play a key role in fostering a more effective approach to online investigations, through coordinated and well-targeted actions to develop capabilities and competences.

The needs of online investigators have to be reliably identified. Europol, in accordance with its mandate, and the EU Innovation Hub for security[84] should coordinate a **comprehensive analysis of technological gaps and needs in the domain of digital investigation**, as well as foresight analysis, which is instrumental for steering research, innovation and development programmes and policy instruments contributing to capacity building. It is important that relevant entities and networks[85] support this work. On this basis, Europol and the EU Innovation Hub for security should establish priorities for research and development to be validated by Member States[86]. To provide a clear vision of practical mechanisms in place and available resources to support capacity of law enforcement authorities in the area of digital investigations, and to clarify roles and responsibilities of the entities involved, the Commission will consult Member States and other stakeholders by the end of 2021 and, will follow-up as necessary.

Research and innovation are necessary, both for technologies for investigations and to fight crime facilitated by technology. The EU Research and Innovation programme, Horizon 2020, has funded the development of innovative technology solutions to enhance the capacity of national authorities in combatting organised crime. This work will be further reinforced with the new programme Horizon Europe which will fund research projects to improve the

[82] See Commission Communication on Ensuring justice in the EU - a European judicial training strategy for 2021-2024, COM(2020) 713 final, 2.12.2020, highlighting need to enable professionals to address new challenges.
[83] Forensic analysis of connected devices and data pertaining to IoT systems.
[84] The EU Innovation Hub for Internal Security is a collaborative network to support the innovation labs of EU Agencies, Member States, the Joint Research Centre of the European Commission and other relevant entities in the delivery of innovative cutting-edge products.
[85] ENFSI, ENLETS, i-LEAD, ILEAnet.
[86] The Europol Clearing Board and the EUCTF (EU Cybercrime Task Force, the group gathering the chiefs of cybercrime units in EU LEAs) would be the formats of choice for Member States' consultation.

intelligence picture on organised crime, develop tools and training curricula, and reinforce inter-agency cooperation.

The Commission will facilitate **access to high quality datasets needed to develop investigative tools** including artificial intelligence systems that respond to law enforcement needs in criminal investigations, such as for the analysis of large quantities of data or for darknet investigations. For that purpose, the Commission will support, under the DIGITAL programme, the creation of a European security data space[87] that will be key to develop, train and evaluate tools for law enforcement and contribute to the European strategy for data in full respect of fundamental rights. In addition, the Commission will support Member States in relation to pilot projects on Artificial Intelligence[88] solutions that would help foster the take up of innovation by the law enforcement community. Law enforcement, industry and academia should cooperate in a network supported by EU funding **to develop tools and solutions at EU level that respond to EU law enforcement needs**[89], therefore supporting the work of Europol in providing services and technical solutions to EU law enforcement authorities. This network should ensure the sustainability of Horizon Europe and Internal Security Fund projects and support Europol in that endeavour.

The network should deliver its results through Europol to law enforcement authorities, free of charge, and continuously improve existing solutions. To that end, Europol should become the one-stop-shop for providing access to tools and services, such as malware analysis, to national law enforcement authorities.

4.3. Improving access to skills, knowledge and operational expertise

While research and analysis of digital evidence is at the heart of the majority of investigations, the level of necessary skills in the field of criminal procedure, tactics and techniques for digital investigation or digital forensics is still not available in some Member States and needs to be broadened and deepened in most. In addition, access to cutting-edge operational expertise in specific areas such as the Internet of Things forensics remains an issue for a number of Member States.

The development of training should be based on a definition of the competencies required to carry out digital investigations and the associated professional profiles (e.g. data analyst,

---

[87] In the 2021-2022 Work Program of DIGITAL, there is an action to lay down the framework of a federated data architecture for security innovation by funding the creation of the national components of a European Security Data Space for Innovation. This would allow innovation and development by setting up an EU-wide ecosystem for sharing, developing, testing, training and validating algorithms for AI tools for law enforcement and security purposes based on various different types of datasets, including pseudo operational and anonymized datasets, in line with the European strategy for data (Commission Communication on A European strategy for data, COM/2020/66 final, 19.2.2020). A call for proposal will be launched in Q1 2022 for the participation of at least 6 law enforcement agencies and two businesses in the value of €5-10 million in the form of a grant requiring 50 % co-financing.

[88] In line with the initiative on artificial intelligence put forward by the Commission in the White paper on Artificial Intelligence, COM (2020) 65 final, 19.2.2020.

[89] To this end, the European Commission is for instance funding the European Anti-Cybercrime Technology Development Association (https://www.eactda.eu/) under the Internal Security Fund (Police) Annual Work Programme 2020.

online investigator, or digital forensic expert). To this end, Europol and CEPOL should work with Member States[90] to define and periodically update a '**Training Competencies Framework**'. On this basis, the Commission should support the development of training materials, via the European Cybercrime Training and Education Group (ECTEG) and support the delivery of training at national level via available instruments[91].

CEPOL and the European Judicial Training Network (EJTN) should regularly assess training needs and prioritise training delivery accordingly, also with a view to further developing the general digital competence of law enforcement and judicial authorities. Based on the Training Competencies Framework, CEPOL should also work closely with practitioners[92] and Member States to create **certification/accreditation schemes for digital investigation experts**. Such schemes would (1) increase the number of experts able to deliver trainings in specific areas; (2) facilitate cross-border cooperation, as certification/accreditation would provide assurances regarding the gathering and handling of evidence, ensuring its admissibility in court also in other jurisdictions; and (3) facilitate identifying specialised investigators.

Digital investigations may require expertise that is scarce in the EU, such as on cryptocurrencies, on ransomware[93] or darkweb investigations. Member States should identify experts who have developed cutting-edge skills in these areas to support each other in operations where such expertise is needed. The Commission will support Europol in putting in place mechanisms to ensure that Member States' authorities and experts have proper incentives to be part of a pool of experts.

Key actions:

The Commission will:

- Analyse and outline possible approaches and solutions on **data retention** for law enforcement and judiciary and consult Member States on these by the end of June 2021;
- Propose a way forward to address lawful and targeted access by law enforcement authorities to **encrypted information** in the context of criminal investigations. This approach should be based on a thorough mapping of how member states deal with encryption and on a multi-stakeholder process to explore and assess the concrete lawful options;
- Encourage and facilitate full and swift **Member State participation in the e-Evidence Digital Exchange System** (e-EDES);
- Develop, through its Joint Research Centre, a monitoring tool to gather intelligence on

[90] In the framework of the European Union Cybercrime Task Force (EUCTF), which was established in 2010, comprising the Heads of the National Cybercrime Units from the various Member States as well as representatives from Europol, the European Commission and Eurojust. https://www.europol.europa.eu/about-europol/european-cybercrime-centre-ec3/euctf.

[91] Such as, for example, via the Internal Security Fund and the Technical Support Instrument.

[92] The European Cybercrime Training and Education Group (ECTEG) has already developed substantial work on the topic, in the framework of its Global Cybercrime Certification Project (https://www.ecteg.eu/running/gcc/).

[93] Europol has worked with industry to establish the No More Ransom Project (https://www.nomoreransom.org/), which provides prevention advice and decryption tools.

illegal activities developing in the **Darknet**;

- Support the **development of training modules and materials** and support training delivery by CEPOL, EJTN and national training institutions;

Europol is urged to:

- Coordinate **a comprehensive analysis** of technological gaps and needs in the domain of digital investigation;
- Create a **repository for tools**, allowing law enforcement to identify and access state of the art solutions;
- Create and maintain a database of **experts in investigations and forensics** in specialised areas such as Internet of Things or cryptocurrencies.

CEPOL is urged to:

- Create **certification/accreditation schemes** for digital investigation experts;
- Provide and regularly update **a Training Competencies Framework**, together with Europol.

The European Parliament and Council are urged to:

- Urgently adopt the e-evidence proposals to ensure speedy and reliable access to **e-evidence** for authorities.

Conclusion

This Strategy sets out the priorities, actions and targets to be achieved in the coming five years to put the EU on a stronger footing in the fight against organised crime. However, the criminal phenomenon is constantly evolving and it is essential to identify new trends and swiftly react to new developments. The Union and its Member States need to stay ahead of criminal organisations.

It is therefore time to intensify the Union's collective action against organised crime, by reinforcing existing instruments to support cross-border cooperation, including cooperation through justice and home affairs agencies, tackling high-priority crimes and disrupting the structures behind them, cracking down on criminal finances and their corrupt methods to infiltrate the economy and tackling criminals' use of new technologies. Any legislation is only as good as its implementation. Therefore, it is important that Member States fully and correctly implement existing EU instruments. The Commission will continue to play its role; it will support and give continuous guidance to Member States and it will be ready to take swift action if EU law is breached.

Authorities on the ground must be able to use existing tools to their full potential in order to disrupt criminal activities and the business model of criminal organisations. To achieve this

objective, the measures under this strategy need to be accompanied by a new culture where law enforcement and judicial authorities systematically check possible cross-border and international links during investigations on organised crime cases. The exchange of law enforcement officers, prosecutors and judges, including with third countries as well as further training opportunities can help bring this about.

The Commission is committed to doing its part in this renewed drive against organised crime and calls on the European Parliament and Council to engage in this common endeavour, which is essential to ensure security in the EU, to protect the European economy and to safeguard the rule of law and fundamental rights.