EUROPEAN
COMMISSION

Brussels, 9.12.2020
COM(2020) 797 final

COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT AND THE COUNCIL

First Progress Report on the EU Security Union Strategy

I INTRODUCTION

Security is one of the major concerns of citizens and the recent spate of terrorist attacks on European soil have underlined still further the need for EU action. On 24 July 2020, the Commission adopted an **EU Security Union Strategy 2020-2025**[1] to target action on priority areas where the EU can bring added value to national efforts. It builds upon progress achieved previously under the European Agenda on Security 2015-2020[2] and provides a new focus, to ensure that EU security policy reflects the changing threat landscape; that it builds long-term, sustainable resilience; that it engages the EU institutions and agencies, governments, the private sector and individuals in a whole-of-society approach; and that it brings together the many policy areas with a direct impact on security. Full respect of fundamental rights is at the heart of this work, as the security of the Union can only be ensured when everyone is confident that their fundamental rights are fully respected.

The threat of trans-national terrorist networks is a vivid reminder that coordinated EU action is indispensable to effective action to protect Europeans, upholding our common values and our European way of life. This is emblematic of how increasingly complex cross-border and cross-sectorial security threats have emerged, making closer cooperation on security at all levels ever more essential. This is true for organised crime or the drugs trade – it is also true for the digital world, with cyber-attacks and cybercrime continuing to rise. All these challenges also apply beyond our borders, with a clear inter-connection between internal and external security. The COVID-19 crisis has also put European security into sharp focus, testing the resilience of Europe's critical infrastructure, crisis preparedness, strategic value chains and crisis management systems, as well as the resilience of our societies vis-à-vis manipulative interference and disinformation.

The Security Union Strategy is composed of four strategic priorities for action at EU level: a future-proof security environment, tackling evolving threats, protecting Europe from terrorism and organised crime, and a strong European security ecosystem. Central to the strategy is implementation, and this is the core theme of this report: implementation which requires the full engagement of the national authorities in the front line of security in the EU. This report is the first implementation report under the Strategy, fulfilling the commitment made by the Commission to regularly report on progress[3]. It covers the period from 31 October 2019, when the last Security Union Progress Report was published under the previous Commission mandate[4].

II A FUTURE-PROOF SECURITY ENVIRONMENT

1. *Critical Infrastructure protection and resilience*

The daily lives of citizens rely on an ever more interconnected and interdependent physical and digital infrastructure. This infrastructure is vital for the functioning of the economy and of society. Without reliable supplies of energy, predictable transportation, comprehensive health systems or a digitally-driven financial network, our current way of life would not be possible. The COVID-19 pandemic has shown even more clearly the

1 COM (2020) 605.
2 COM(2016) 230.
3 During the Hearing of Vice-President Schinas in front of the European Parliament on 3.10.2019.
4 COM(2019) 552.

importance of **ensuring the resilience of critical sectors and operators**. The EU has recognised the common interest in protecting critical infrastructure from threats, whether natural or man-made disasters, or terrorist attacks. The current threat picture facing critical infrastructures is wide-ranging. It includes: terrorism, hybrid actions, cyber-attacks, insider incidents; threats associated with new and emerging technologies (such as drones, 5G, artificial intelligence); climate change related challenges; disruption of supply chains; and election interference. Our current rules need modernising and expanding[5]. They need to shift the focus from protection to resilience, bringing more coherence and consistency in sectoral coverage and focusing on critical entities delivering essential services.

This will be the goal of forthcoming proposals to promote the resilience of **physical and digital infrastructures**. The overall objective is to increase preparedness at national and EU level by building up robust capabilities to prevent, detect, respond to and mitigate threats, and to be prepared to act in crisis. Existing legislation has been able to increase and improve risk management in critical sectors; this needs to be stepped up. A key objective of the revised Critical Infrastructure Directive will be to promote a high common level of resilience in a sufficient range of key sectors. Similarly, updating the Network and Information Systems (NIS) Directive will target more consistency in Member States' identification of the 'operators of essential services'[6]. More generally, despite considerable progress, cybersecurity capabilities in the Member States are still uneven so the revision will seek to drive more cybersecurity in general[7]. The result will be greater and more coherent approaches to the resilience for physical and digital infrastructure.

As work is progressing toward this more coherent framework, **sectoral initiatives** complement this work and target specific vulnerabilities. The specific challenges of cybersecurity for the energy sector are now being taken forward on the basis of the 2019 Commission Recommendation,[8] taking into account the characteristics of the sector such as the real-time requirements, the risk of cascading effects, and the combination of legacy systems with new technologies. Work is ongoing on a dedicated network code on cybersecurity for cross-border flows of electricity, as well as on the resilience protection and cybersecurity of critical energy infrastructure. The Thematic Network for Critical Energy Infrastructure Protection was also re-launched, with a renewed focus and objectives, and met for the first time in June 2020, with over 100 online participants. This Network provides a platform to foster cross-border collaboration among critical energy infrastructure operators and owners in the energy sector.

To provide a common starting point for Member States' collaboration in **risk preparedness in the electricity sector**, in September 2020 the European Network of Transmission System Operators for electricity set out the most relevant regional electricity crisis scenario as provided in the risk preparedness regulation[9]. These include cyber-attacks as well as pandemic and extreme weather events. Member States will prepare national crisis scenarios and risk preparedness plans to prevent and mitigate electricity crises (first drafts are due in April 2021). To contribute to this process, a set of good practices were

---

5 Directive 2008/114/EC and Directive (EU) 2016/1148..

6 COM(2019) 546. The Commission also undertook a public consultation (7 July-2 October 2020) and country visits in all Member States aimed at verifying conformity in the implementation of the Directive through meetings with operators and national authorities.

7 COM(2019) 546.

8 C(2019) 2400.

9 OJ L 158, 14.6.2019, p. 1–21.

issued in June 2020[10], based on the close monitoring of the impact of COVID-19 on the energy sector through the Electricity, Gas and Oil Coordination Groups, as well as the European Nuclear Safety Regulators Group and the European Offshore Authorities Group.

The growing and sophisticated reliance on digital processes in the delivery of financial services also calls for increasing the level of cyber-security in the **financial sector**. While the security of ICT systems is recognised as an integral part of risk management for financial entities, this has not yet been fully reflected in the EU financial services regulatory landscape. On 24 September 2020 the Commission adopted its Digital Finance Strategy package[11], with the clear objective of addressing challenges and risks associated with the digital transformation, promoting resilience, data protection and appropriate prudential supervision. This included a legislative proposal on digital operational resilience[12], to ensure that safeguards are in place to mitigate cyber-attacks and other risks[13]. This initiative contributes to a strong and vibrant European digital finance sector and thus strengthens Europe's ability to reinforce its open strategic autonomy in financial services and, by extension, its capacity to regulate and supervise the financial system to protect Europe's financial stability.

During large-scale emergencies, the high degree of interdependence between sectors and countries require a coordinated action to ensure a rapid and effective response, as well as better prevention and preparedness for similar situations in the future. In the revision of the Union Civil Protection Mechanism Decision[14], the Commission has proposed[15] the development of **disaster resilience goals** and **resilience planning,** with a reinforced focus on building longer-term cross-sectoral resilience to transboundary disasters. The proposed new resilience building approach complements disaster risk management work at national level. On 26 November, the Council reached an agreement on a negotiating mandate to strengthen disaster prevention, preparedness and response, based on the Commission proposal of 2 June 2020[16].

The COVID-19 pandemic has demonstrated the impact of health crisis on security at the EU and global levels, and highlighted the need to step up preparedness and response planning for epidemics and other serious cross-border health threats. The Commission's package of 11 November 2020 on "**Building a European Health Union**: Reinforcing the EU's resilience" set out the next steps to tackle cross-border health threats. This would bring a reinforced framework for cross-border cooperation against all health threats and included three legislative proposals: to upgrade the legislation on serious cross-border health threats, and to strengthen the European Centre for Disease Prevention and Control (ECDC) and the European Medicines Agency (EMA). Together, these proposals will put in place a robust and cost-effective framework to put the EU and member States on a more secure footing when responding to future health crises.

---

10 Energy security: good practices to address pandemic risks (SWD(2020) 104).

11 https://ec.europa.eu/info/publications/200924-digital-finance-proposals_en.

12 COM(2020) 595.

13 The proposal sets out a coherent baseline for the ICT risk management requirements, the ICT incident reporting to financial supervisors, digital testing, and information sharing. In addition, the proposal submits critical ICT third-party service providers to an oversight framework at European scale.

14 Decision No 1313/2013/EU of 17 December 2013 on a Union Civil Protection Mechanism.

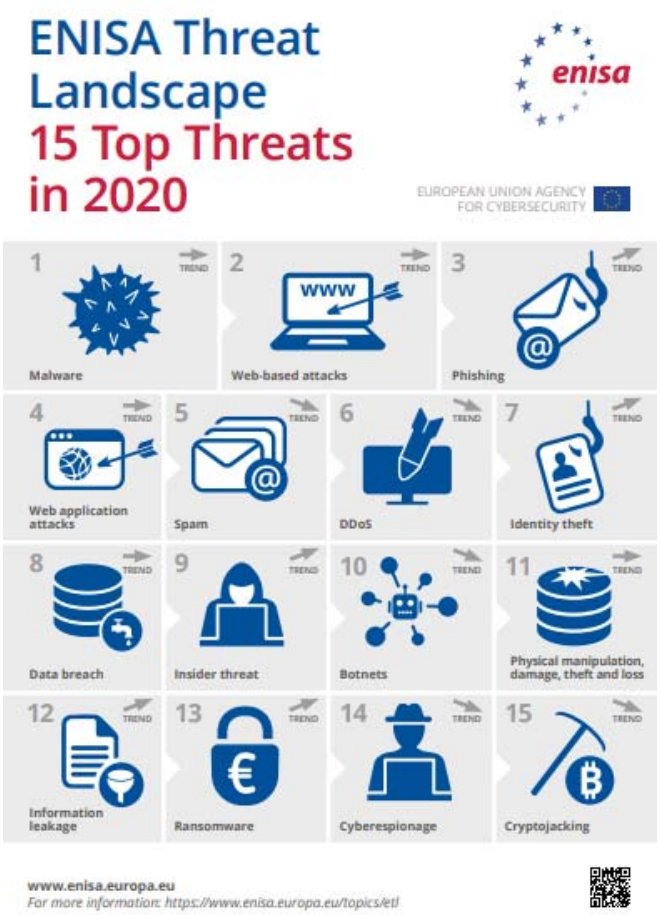
15 COM(2020) 220.

16 Proposal to amend Decision No 1313/2013/EU on a Union Civil Protection Mechanism - Mandate for negotiations with the European Parliament

A key element to protect key EU and national digital assets is to offer critical infrastructures a channel for **secure communications**. This is supported by the development of a network infrastructure for secure and resilient Governmental Satellite Communications as a component of the EU Space programme.

2. ***Cybersecurity***

The benefits of digital transformation are clear but so is the fact that it is inevitably accompanied by an increase in potential vulnerabilities[17]. Critical infrastructure is often the target of increasingly sophisticated cyber-attacks[18]. **Cybersecurity** must therefore be the concern not only of policymakers, but of everyone who works or communicates online.



To increase trust in and security of digital products, processes and services, the Cybersecurity Act of June 2019 created **an EU cybersecurity certification framework**. The Commission has requested the EU Agency for Cybersecurity, ENISA, to prepare two cybersecurity certification schemes, and their preparation is well underway. This work also involves national cybersecurity certification authorities, industry, consumers, accreditation, standardisation and certification bodies as well as the European Data Protection Board.

One of these schemes is a **cloud services** scheme in support of a secure and trusted cloud services market place. This is a key element in the **EU Data Strategy** adopted in February 2020[19]. It would create a common security baseline for cloud services across sectors, building on the highest common denominator of existing (European and international) standards, schemes and practices. This will be a key element in the free flow of data across the EU[20]. The scheme will also foster the adoption of cloud technologies by providing users, in particular small and medium-sized enterprises and public administration, with comprehensible reassurance on the level of security when they use the cloud.

As highlighted in the Security Union Strategy, given the ongoing roll-out of the 5G infrastructure across the EU and the potential dependence of many critical services on 5G networks, the consequences of systemic and widespread disruption can be particularly

[17] ENISA Threat Landscape 2020: Cyber Attacks Becoming More Sophisticated, Targeted, Widespread and Undetected.

[18] Since the outbreak of the pandemic, EU agencies and Member States have detected a significant rise in cyber-attacks, including against the healthcare sector.

[19] COM(2020) 66.

[20] Regulation (EU) 2018/1807.

serious. The result has been a common effort by Member States to develop and put in place adequate security measures. Following the Commission's Recommendation on the **Cybersecurity of 5G networks** of March 2019[21], Member State completed national risk assessments which translated into a coordinated EU risk assessment report[22] identifying the security challenges linked to 5G networks. On this basis, on 29 January 2020 the NIS Cooperation Group[23] published the **EU toolbox of risk mitigating measures**[24] setting out necessary strategic and technical measures. The toolbox includes measures to strengthen security requirements for mobile network operators (MNOs), ensure the diversity of suppliers for individual MNOs, assess the risk profile of suppliers, and apply restrictions for suppliers considered to be high risk. The Commission will support the implementation of the toolbox, making full use of its competences and means at its disposal[25], including telecoms and cybersecurity rules; coordination on standardisation as well as EU-wide certification; and the EU Foreign Direct Investment Framework[26].

The NIS Cooperation group published a progress report on the implementation of toolbox measures in July 2020[27]. This noted that a large majority of Member States have already adopted or are in the process of implementing the measures recommended in the toolbox. Measures where implementation was less advanced included mitigating the risk of dependency on high-risk suppliers and the development of multi-vendor strategies at both company and national level.

Over the course of the last few months, EU institutions and Member States responded to the increased level of cybersecurity risk triggered by the **COVID-19 crisis** by intensifying the exchange of information and enhancing the level of preparedness for a potential cyber crisis. EU cooperation was stepped up in key fora (NIS Cooperation Group and the Computer Security Incident Response Teams (CSIRTs) Network), as well as through new forms of coordination and information sharing tools[28]. In September 2020, there was a second table-top Blueprint Operational Level Exercise (Blue OLEx)[29], where the "Cyber Crisis Liaison Organisation Network" (CyCLONe) of Member States was also launched, which will implement further the Blueprint for rapid emergency responses for large-scale, cross-border cyber incidents or crises[30].

---

21 COM(2019)2335.

22 Report on EU coordinated risk assessment of the cybersecurity of 5G networks.

23 The NIS Cooperation Group was set up to ensure strategic cooperation and the exchange of information among EU Member States in cybersecurity.

24 https://ec.europa.eu/digital-single-market/en/news/cybersecurity-5g-networks-eu-toolbox-risk-mitigating-measures.

25 COM(2020) 50.

26 Regulation (EU) 2019/452. This also contains explicit references to "critical infrastructure" (as well as "critical technologies") more broadly as "factors that may be taken into consideration by Member States or the Commission" when assessing the potential impact of an investment.

27 Report on Member States' progress in implementing the EU Toolbox on 5G Cybersecurity.

28 EU Institutions and bodies gathered in a COVID-19 Cyber Task Force and launched a weekly Sectorial Situational Awareness and Analysis report. ENISA and Europol launched campaigns on how to remain cyber secure during COVID-19. CERT-EU has issued guidance on how to set up secure VPNs. In the summer of 2019, the Cooperation Group established a new workstream dedicated to cybersecurity in Health and the Commission and ENISA launched an EU Health Information Sharing and Analysis Centre.

29 https://www.enisa.europa.eu/news/enisa-news/blue-olex-2020-the-european-union-member-states-launch-the-cyber-crisis-liaison-organisation-network-cyclone.

30 C(2017) 6100.

In the global cyberspace, cyber-attacks and threats often originate from outside the EU. To effectively face these challenges, the EU and Member States cooperate to advance international security and stability in cyberspace, promote responsible state behaviour, increase global resilience and raise awareness on cyber threats and malicious cyber activities, including with international partners[31]. On 30 April 2020, the High Representative published a Declaration on behalf of the EU condemning malicious behaviour in cyberspace and expressing solidarity with the victims[32].

On 30 July 2020, the Council adopted the **first ever EU cyber sanctions** against six individuals and three entities responsible for or involved in cyber-attacks. These include the attempted cyber-attack against the OPCW (Organisation for the Prohibition of Chemical Weapons) and those publicly known as 'WannaCry', 'NotPetya', and 'Operation Cloud Hopper'. On 22 October 2020, the Council applied sanctions to another two individuals and one entity responsible for or involved in the cyber-attack against the German federal parliament. These decisions followed continuous signaling of the EU and Member States of the need to prevent, discourage, deter and respond to malicious cyber activities, including by using its cyber sanctions regime as part of its 2017 cyber diplomacy toolbox[33].

Negotiations between the co-legislators on new export rules that restrict the sale of cyber-surveillance goods to worldwide regimes engaging in the repression of human rights[34] have also progressed. Once adopted, these rules will lead to a more accountable, competitive and transparent trade of dual-use items[35]. The proposed amendments, made necessary by technological developments and growing security risks, include new criteria to grant or reject export licenses for certain items.

3. Protecting public spaces

As recognised in the EU Agenda on Counter Terrorism[36], the protection of public spaces, through building resilience against security threats remains a crucial component of the work towards an effective and genuine Security Union. The Commission is working with a wide range of public and private stakeholders to develop guidance and provide practical support and funding[37], in line with the **2017 Action Plan to support the protection of**

---

31 The EU promotes the strategic framework for conflict prevention, stability and cooperation in cyberspace, including through EU participation in the United Nations' discussions on cyber issues. Two important processes are the Open-ended Working Group on developments in the field of information and telecommunications in the context of international security; and the Group of Governmental Experts (GGE) to advance responsible State behaviour in cyberspace. Issues include the impact of international law, the implementation of agreed non-binding voluntary norms of responsible state behaviour and confidence building measures, as well as developing implementation through targeted capacity building.

32 https://www.consilium.europa.eu/en/press/press-releases/2020/04/30/declaration-by-the-high-representative-josep-borrell-on-behalf-of-the-european-union-on-malicious-cyber-activities-exploiting-the-coronavirus-pandemic/.

33 Council Decisions (CFSP) 2020/1127, 2020/1537, and 2020/651 as part of 9916/17.

34 COM(2016) 616. The Commission proposal aims at amending and recasting Regulation 428/2009, which set up a Community regime for the control of exports, transfer, brokering and transit of dual-use.

35 These are a vast group of goods, materials, software and technology which can be used for both civil and military purposes.

36 COM (2020) 795.

37 The 2019 ISF Protect call included 'Secu4All', developing a comprehensive training cycle for local authorities to provide citizens with a safe urban environment, and 'DroneWISE' to strengthen the preparedness of first responders to counter hostile unmanned aerial vehicles. In 2020, a new € 12m cal Will take place on the protection of public spaces.

public spaces[38] and the 2019 collection of good practices to support the protection of public spaces[39]. As set out in the EU Agenda on Counter-terrorism, the Commission will intensify its support to local and regional authorities, who play a key role in the protection of public spaces and the prevention of radicalisation. This will include drawing up an EU Protocol on Urban Security and Resilience for cities, setting out basic principles and objectives for local authorities in these areas.

As terrorist attacks have increasingly targeted **places of worship**, a particular emphasis is placed on cooperation between public authorities and faith-based leaders and congregations, in order to improve the level of security awareness and help implement good practices and training in places of worship. Simple measures can make the difference between life and death. In October 2019, a synagogue in Halle was the subject of a terrorist attack. A reinforced door, a panic button and security cameras all helped save lives.

To further support enhanced security in public spaces, particularly places of worship, in 2020 the Commission has made €20 million available to stakeholder-led projects.

The Commission is also working on responding to **emerging risks to public spaces**, including **unmanned aircraft systems** (UAS). While drones bring significant economic and employment opportunities, they also pose a significant risk to public spaces, critical infrastructures and other sensitive sites, such as prisons. Recent EU rules[40] in this area mitigate this risk, by enhancing the security of drone operations. From January 2021, drone operators will also be required to register with national authorities. This regime may be complemented by a **regulatory framework for the U-space**, Europe's unmanned traffic management system[41], to ensure safer and more secure drone operations. Combined, these steps will make it harder for individuals to fly drones in restricted areas and will help in identifying and prosecuting offenders.

The Commission is also working to support law enforcement, critical infrastructure operators, mass event organisers and other stakeholders to counter the non-cooperative use of drones, for instance, working with the European Union Aviation Safety Agency to develop **good practices to help airport stakeholders** respond to unauthorised drone incidents, facilitating more harmonised **countermeasure testing efforts** around the EU, and developing a practical handbook for stakeholders, focused on the urban context.

An **EU Digital Autumn School for the protection of public spaces**, organised by the Commission's Joint Research Centre in October 2020, gathered more than 200 urban planners and public and private operators of public spaces. Sessions examined a wide range of topics, such as how to protect against blasts and vehicle ramming, mitigating the threats posed by hostile drones in urban settings, and the use of surveillance and detection technologies.

The Commission has also continued to actively support the **Partnership for Security in Public Spaces,** launched in January 2019 under the Urban Agenda for the EU, which has published its new Action Plan[42] to tackle urban security at various levels of governance.

---

38 COM(2017) 612.
39 SWD(2019) 140.
40 Commission Implementing Regulation (EU) 2019/947.
41 The Commission may table na implementing regulation to this effect, which would be adopted under na examination procedure involving the aviation safety committee.
42 The Action Plan has been adopted and is available on Futurium: https://ec.europa.eu/futurium/en/security-public-spaces/security-public-spaces-partnership-final-action-plan-0.

The actions include the creation of a framework for a self-assessment tool, recommendations for policy-making, multi-level governance and funding, innovation through smart solutions and technologies, including the concept of security by design, prevention and social inclusion. The Partnership will now enter the implementation phase.

Support to improve security in public spaces at the local level was also provided through the 4th call of the Urban Innovative Actions. Three cities have been selected and are testing new solutions on urban security matters (Piraeus in Greece, Tampere in Finland and Turin in Italy), through funding from the European Regional Development Fund.

In terms of response, the Commission has also developed a European framework to enhance preparedness and response to mass burn casualty incidents, exploiting the overall European burn care capacity to treat patients through cooperation at EU level. The Union Civil Protection Mechanism can be used to support large numbers of patients with serious burn injuries by providing access to burn beds in specialised treatment centres, burn assessment experts, and medical evacuation capacities.

III TACKLING EVOLVING THREATS

1. Cybercrime

Shortcomings in cybersecurity are often exploited by criminals. This has been clearer than ever during the COVID-19 crisis. There has been an increase in 'classic' cybercrime using malware and ransomware (i.e. to steal personal and payment data or to blackmail victims) as well as a proliferation of new websites that lure users into installing malware. Cyber-attacks on healthcare and research infrastructure have occurred, locking up ICT systems that can only be unlocked against a ransom payment or with access to information on vaccine development[43]. A significant rise in child sexual abuse and child sexual abuse material has also been observed[44].

An effective response to cybercrime requires a strong framework for criminal investigations and prosecutions, and a key first step is full transposition and implementation of the Directive on **attacks against information systems**[45]. The Commission is monitoring the actions of Bulgaria, Italy, Portugal and Slovenia following the opening of infringement cases in 2019. Progress is also needed on implementation of

[43] Internet Organised Crime Threat Assessment (IOCTA) 2020, October 2020

[44] Report on Exploiting isolation: Offenders and victims of online child sexual abuse during the COVID-19 pandemic, Europol, 19.06.2020.

[45] Directive 2013/40/EU.

the 2011 **Directive on combating child sexual abuse**[46]. The areas in which efforts are still needed include prevention, substantive criminal law, assistance, support and protection measures for child victims. Since 2018, the Commission has opened infringement procedures against 25 Member States[47].

On 24 July 2020, the Commission adopted an **EU strategy for a more effective fight against child sexual abuse**[48], which aims to provide an effective EU response to the crime of child sexual abuse. A specific challenge has also emerged as, from 21 December 2020, certain online communication services, like webmail or messaging services, will fall under the scope of the e-Privacy Directive and they are covered by the revised definitions in the European Electronic Communications Code. As a result, there is a clear risk that providers of those services that undertake certain important voluntary activities for the purpose of detecting, tackling and reporting child sexual abuse online today would have to stop doing so. The Commission has therefore proposed a **Regulation**[49] to allow these voluntary activities to continue under certain conditions, until a long-term legislative solution. The Commission is working on a proposal for such a solution, scheduled for adoption in 2021.

A **COVID-19 Cyber Defence Alliance** has been established by the European network of Cybersecurity centres and competence Hub for innovation and Operations to develop innovative approaches to counter COVID-19 related crimes. In April 2020, a dedicated EIC COVID Platform[50] was set up to connect civil society, innovators, partners, and investors across Europe in order to develop innovative solutions.

In order to ensure a more effective prosecution of crimes and in view of the importance of electronic information and evidence in criminal investigations, law enforcement and judicial authorities should swiftly obtain access to such information and evidence for their criminal investigations. This was recognised in the Joint Statement by the EU Home Affairs Ministers of 13 November 2020[51]. Europol, Eurojust and the European Judicial Network publish on 1 December 2020 their second "SIRIUS EU Digital Evidence Situation Report". The report highlights the increased relevance of electronic evidence in criminal investigations[52]. On the Commission's proposals on **cross-border access to electronic evidence**[53] from April 2018, the European Parliament has not yet established its position, therefore the negotiations between the co-legislators are yet to start. Delays to adoption of these proposals are holding back the work of law enforcement and judicial

---

46 Directive 2011/93/EU.

47 Spain, Portugal, Italy, Netherlands, Sweden, Malta, Lithuania, Slovakia, Bulgaria, Romania, Germany, Austria, Belgium, Czechia, Estonia, Greece, Finland, France, Croatia, Hungary, Ireland, Luxembourg, Latvia, Poland, Slovenia.

48 COM(2020) 607.

49 COM(2020) 568.

50 The Commission, together with the European Innovation Council and Member States, hosted a Pan-European EUvsVirus Hackathon + Matchathon https://covid-eic.easme-web.eu/.

51 Joint Statement by the EU Home Affairs Ministers on the recent terrorist attacks in Europe, 13.11.2020, 12634/20.

52 According to the Report, the volume of cross-border requests submitted by EU authorities to online service providers increased significantly in 2019 with a large majority of them issued by Germany (37.7% of requests), France (17.9%) and the UK (16.4%). Requests to access electronic data doubled in Poland and nearly tripled in Finland. Furthermore, emergency disclosure requests increased by nearly half in one year.

53 COM/2018/226 and COM/2018/225

authorities, as well as complicating ongoing efforts to establish compatible rules for cross-border access to e-evidence through international negotiations[54].

At international level, the Commission participates, on behalf of the EU, in the ongoing negotiations of the Second Additional Protocol to the Council of Europe **Budapest Convention on cybercrime**. This Protocol would provide competent law enforcement authorities with enhanced, far-reaching tools for cross-border cooperation for the investigation and prosecution of cybercrime and other serious forms of crime, including direct cooperation with service providers. Since most of these enhanced, reinforced ways of cooperation will rely on the exchange of personal data, it is essential that the future Protocol will provide for appropriate data protection safeguards, not only from a fundamental rights perspective, but also to ensure legal certainty, mutual trust and the effectiveness of operational law enforcement cooperation.

The negotiations should be concluded in 2021. In parallel, further to the mandate received by the JHA Council last year, the Commission is negotiating an **EU-US agreement on cross-border access to electronic evidence**. This would complement the proposed internal EU rules for direct cross-border cooperation with service providers, by removing conflicts of law and providing for common rules and safeguards. Formal negotiations were launched on 25 September 2019 and several negotiation rounds already took place. However, the outcome of the negotiations depends largely on progress being achieved on the internal e-evidence rules.

With regard to the **retention and use of data for law enforcement purposes**, the previous *Tele2/Watson* judgment[55] from 2016 was followed up by the Commission through expert consultations with relevant service providers, police and judicial authorities, civil society, data protection authorities, academia and EU agencies. Reflections were also fed by a study on the data retention practices of electronic communication service providers and the needs and practices of law enforcement authorities to access data, the identification of relevant technological challenges, and an overview of the national legal frameworks.[56] This work has highlighted the need for law enforcement authorities to access data to carry out their tasks more effectively.

On 6 October 2020 the Court of Justice delivered judgments[57] concerning the national legislation of Belgium, France and the United Kingdom on the retention, transmission and access to non-content communication data for the purposes of law enforcement and national security. The Commission will assess available options to ensure that terrorists and other criminals can be identified and traced, while respecting EU law as interpreted by the Court of Justice, also having regard to other cases pending before the Court on this subject matter.

---

[54] For instance, the UN General Assembly (UNGA) adopted on 27 December 2019 Resolution 74/247 on 'Countering the use of information and communications technologies for criminal purposes', establishing an open-ended ad hoc intergovernmental committee of experts tasked to elaborate a comprehensive international convention on cybercrime. The EU does not support the creation of a new international legal instrument on cybercrime as the Budapest Convention on Cybercrime already provides a comprehensive multilateral legal framework. In July 2020, the UN Member States agreed to postpone first steps: the EU contributed to the process on the basis of a Common position (doc.7677/2/20).

[55] Judgment in Joined Cases C-203/15 and C-698/15, *Tele2 Sverige AB and Watson and Others,* 21 December 2016.

[56] https://data.europa.eu/doi10.2837/26288

[57] Judgments in Case C-623/17, Privacy International, and in Joined Cases C-511/18, La Quadrature du Net and Others, C-512/18, French Data Network and Others, and C-520/18, Ordre des barreaux francophones et germanophone and Others

Another important element in fighting cybercrime has been the work to ensure the availability and accuracy of internet domain name registration data (‘**WHOIS information’)**, in line with the efforts of the Internet Corporation for Assigned Names and Numbers (ICANN). Discussions seek to ensure that legitimate access seekers, including law enforcement and cybersecurity operators, obtain efficient access to generic Top-Level Domain registration data, in full respect of applicable data protection rules. The final recommendations for a new WHOIS policy were published on 10 August 2020 and are currently under review, before a decision will be taken by the ICANN Board. The Commission will examine the conclusions of the review and consider the extent to which they sufficiently reflect data protection and the public interest considerations of providing effective access for law enforcement authorities and cybersecurity operators.

2. Modern law enforcement

As technology continues to reshape nearly every sector of society, including security, law enforcement and judiciary needs to be able to keep up. Integrating artificial intelligence, Big Data and High Performance Computing into security policy whilst not weakening the effective protection of fundamental rights is essential to increase safety and security.

The Commission is working on a number of key workstrands[58]. On 25 November 2020 the Commission proposed[59] the Data Governance Act, a framework for facilitated sharing and re-use of personal and non-personal data for innovation and development purposes. This covers industry and public bodies via virtual or physical sectorial data spaces. It would allow access for national law enforcement authorities to data hosted in other data spaces for their own innovation purposes. At the same time, access to data held by national law enforcement and security authorities would not be allowed unless authorised by EU or national law. National law enforcement security authorities may also benefit if individual data subjects make their data available voluntarily for the common good, for the sole purpose of scientific research.

Work is also under way to prepare a new initiative on **artificial intelligence (AI),** following the publication of the White Paper on AI[60]. While recognising the opportunities AI technology offers to boost security and the well-being of citizens and society as a whole, the White Paper also identified a number of risks – such as cyber threats, personal security risks, or loss of connectivity. In the public consultation, participants’ main concerns related to the possibility of AI breaching fundamental rights and the risk that AI may lead to discriminatory outcomes[61]. In the Communication on Building Trust in Human Centric AI[62], the Commission emphasised the need to make AI systems resilient against both overt attacks and more subtle attempts to manipulate data or algorithms, and to take steps to mitigate this risk.

Encryption plays a fundamental role in ensuring strong cybersecurity and the effective protection of fundamental rights, such as privacy, including the confidentiality of communications, and protection of personal data and in ensuring trust in services and products based on encryption technologies, such as digital identity solutions. At the same time, it can also be used to conceal crime from law enforcement and judiciary, making it

58 Including the EU data strategy (see above).
59 COM(2020) 767.
60 COM(2020) 65.
61 Respectively 90% and 87% of respondents find these concerns important or very important.
62 COM(2019)168.

difficult to investigate, detect and prosecute. Member States in the Council have called for solutions that allow law enforcement and judicial authorities to gain lawful access to digital evidence, in full respect of privacy, data protection and fair trial guarantees[63]. The Commission will work with Member States to identify legal, operational, and technical solutions for lawful access to electronic information in encrypted environments which maintain the security of communications.

Practical steps under way include a **decryption platform** in Europol to help law enforcement to gain lawful access to encrypted information on devices seized during the course of criminal investigations[64]. The European Cybercrime Training and Education Group has developed pilot training modules which will feed into the work of the Agency for Law enforcement Training (CEPOL). A network of Member States' points of encryption expertise has been set up to share best practices and expertise, and to support the development of a toolbox of technical and practical instruments.

The **e-Evidence Digital Exchange System (eEDES)** will offer a tool for secure, swift and efficient cross-border exchange of European Investigation Orders, mutual assistance requests and evidence in digital format. It should be gradually enriched and extended to other judicial cooperation instruments in criminal matters and itsfuture scope will be laid down in a legislative proposal on the digitalisation of judicial cooperation procedures planned for 2021[65].

3. Countering illegal content online

Radicalisation leading to violent extremism and terrorism is a multidimensional and cross-border phenomenon that has been able to exploit the rapid growth of the internet. The internet continues to be used to radicalise and recruit the vulnerable. In July, Europol's Internet Referral Unit took down 2,000 links to terrorist content – including manuals and tutorials on how to carry out an attack. The evidence of the role of the internet in radicalising and advertising the crimes of those involved in attacks in France and in Austria further highlight the need for a clear legislative framework to prevent the dissemination of terrorist content online, while maintaining effective safeguards for the protection of fundamental rights. The negotiations between the European Parliament and the Council on the proposed **Terrorist Content Online Regulation**[66] have intensified in the recent weeks. Concluding these negotiations with the establishment of, in particular, the new and effective operational instrument of removal orders for the cross-border elimination of terrorist content within an hour or less from the reception of those orders is critical to addressing terrorist content, including content contributing to radicalisation.

In the meantime, the **EU Internet Forum** continues to act as a catalyst for action, providing an essential platform bringing together Member States and industry to prevent the spread of terrorist content online and counter radicalising messages. The Forum is working on developing a reference list of prohibited symbols and groups in Member States, that could inform the platform's content moderation policies.

The EU Internet Forum has expanded its scope of activities to also cover **child sexual abuse online**. The Forum will provide a common space to share best practices and identify

---

63 ST 13084 2020 - Council Resolution on Encryption - Security through encryption and security despite encryption.

64 This €6 million project is also supported by the Joint Research Centre of the Commission.

65 Communication on Digitalisation of Justice in the EU, COM(2020) 710, 2 December 2020.

66 COM(2018) 640.

obstacles faced by both private and public actors, to increase mutual understanding and find solutions together. It also enables high-level political coordination to maximise the efficiency and effectiveness of action. A technical expert process was created under the EU Internet Forum composed of academia, industry, public authorities and civil society organisations to map and preliminarily assess possible technical solutions to detect and report child sexual abuse in end-to-end encrypted electronic communications. Such technical solutions should not weaken encryption. This approach complements other elements of the fight against child sexual abuse, both online and offline, as described above.

The Commission has also continued to share EU expertise and experience as part of the Independent Advisory Committee of the newly established **Global Internet Forum to Counter Terrorism** and as Co-lead, together with Microsoft, of the Crisis Response Working Group. Together with Europol, the Commission continued to support Member States in the implementation of the **EU Crisis Protocol.** The EU Internet Referral Unit hosted a second tabletop exercise on 23 November 2020, to prepare guidelines to improve operational responses and real-time coordination between Member States and Online Service Providers.

In June 2020, the Commission published the results of the latest monitoring exercise on the implementation of the **Code of conduct on countering illegal hate speech online**[67]. This showed that on average, IT companies assess 90% of flagged content within 24 hours and remove 71% of the content deemed to be illegal hate speech. However, it also identified shortcomings in transparency and feedback to users. The implementation of the Code of Conduct over the past four years was also fed into reflections on how to address illegal content online while protecting freedom of expression in the forthcoming proposal for a Digital Services Act. In the 2020 State of the Union Address, President von der Leyen also announced that by the end of 2021, the Commission will propose to extend the list of EU-level crimes under Article 83(1) TFEU to hate crime and hate speech[68].

4. ***Hybrid threats***

In recognition of the evolving nature of hybrid threats, the Council established in July 2019 a **Horizontal Working Party on Enhancing Resilience and Countering Hybrid Threats**. Its main objective is to support strategic and horizontal coordination among Member States in the field of State and societal resilience, improving strategic communication and countering disinformation. Work has included follow-up to the hybrid risk surveys[69], as well as looking specifically at hybrid threats and disinformation in neighbourhood partner countries. The activities of the Horizontal Working Party have been presented in an Annual Report adopted on 14 September 2020.

In December 2019, the Council adopted 'Conclusions on Complementary Efforts to Enhance Resilience and Counter Hybrid Threats'[70], calling for a comprehensive approach to security and to counter hybrid threats, working across all relevant policy sectors in a more strategic, coordinated and coherent way. Two key follow-up steps took place in July 2020. First the Commission services and the EEAS prepared a **mapping of measures and**

[67] https://ec.europa.eu/info/policies/justice-and-fundamental-rights/combatting-discrimination/racism-and-xenophobia/eu-code-conduct-countering-illegal-hate-speech-online_en.
[68] Also set out in more detail in the LGBTIQ Equality strategy 2020-2025 (COM(2020) 698).
[69] Action 1 of the 2016 Joint Framework on countering hybrid threats, see JOIN/2016/018.
[70] Council Conclusions 14972/19.

documents relating to EU response to hybrid threats[71]. The mapping provides an overall inventory of countering hybrid threats-related measures at EU level and corresponding policy documents. It serves as a starting point to create a restricted online platform as one-stop-shop of all hybrid threats-related measures, policy and legislative documents, as well as relevant studies. Second, the latest annual **report on countering hybrid threats**[72] looked at the implementation covering situational awareness, building resilience, preparedness and crisis response, as well as international and in particular EU-NATO cooperation in countering hybrid threats. While the report notes some progress in terms of EU level coordination, the unprecedented scale and diversity of hybrid threats today needs further steps at EU approach level to integrate the external and internal dimension in a seamless flow and support Member States efforts to counter hybrid threats and strengthen their resilience.

In parallel, work is under way on the implementation of the measures laid down in the new Security Strategy to mainstream hybrid considerations into policy making, develop a restricted online platform, establish sectorial EU resilience baselines, as well as streamline information flows to further enhance situational awareness[73] This builds on the **EU Hybrid Fusion Cell** (HFC) established within the EU Intelligence and Situation Centre (EU INTCEN), which remains the main EU focal point for hybrid threat assessments. It has now produced more than 180 written reports on hybrid and cyber threats. One of the HFC projects is the **Hybrid Trends Analysis**[74] which provides data on topics such as: recurrent analysis of emerging actors' hybrid activities; foreign intelligence activities against the EU Member States, institutions, partners and interests; and hybrid state and non-state actors exploitation of the COVID-19 pandemic.

EU-NATO cooperation (under the comprehensive framework provided by the Warsaw and Brussels Joint Declarations of 2016 and 2018) has further intensified, as highlighted in the fifth Progress Report of June 2020, with staff-to-staff interaction and concrete deliverables in the areas of hybrid threats, cyber defence and capacity-building[75]. It is crucial to develop a single methodology across sectors for the work on hybrid resilience baselines, to address the risk of fragmented and duplicating policies, tools and actions. The European Centre of Excellence for Countering Hybrid Threats in Helsinki was also involved in this cooperation. Cooperation with NATO has been stepped up in the COVID-19 crisis, including on pandemic-related disinformation and addressing hostile information activities.

In general, the COVID-19 pandemic has highlighted the rapidly evolving risks of **disinformation** and the real risk to people's lives[76]. On 10 June 2020 the Commission and

---

71 SWD(2020) 152, Joint Staff Working Document, Mapping of measures related to enhancing resilience and countering hybrid threats.

72 SWD(2020) 153, Joint Staff working document, Report on the implementation of the 2016 Joint Framework on countering hybrid threats and the 2018 Joint Communication on increasing resilience and bolstering capabilities to address hybrid threats.

73 For example, in 26 November 2020, the Joint Research Centre proposed a new framework to raise awareness of threats: https://ec.europa.eu/jrc/en/news/jrc-framework-against-hybrid-threats

74 The Hybrid Trends Analysis is a tool to be used alongside national systems to monitor the scale and intensity of hybrid threats in the political/diplomatic, military, economic, information, intelligence, cyber, social, energy and infrastructure domains.

75 Cooperation between staffs in the field of cyber security and defence has further intensified through work on consistent concepts and doctrines, exercises, exchanges of information and cross-briefings.

76 Real-world consequences included the arson of telecommunications infrastructure and misleading health information with direct consequences.

the High Representative adopted a **Joint Communication on COVID-19 and disinformation**[77] to point out the specific risks of COVID-19 disinformation and what action should be taken. This involved action by major online platforms to develop policies to address the threat, and intensified monitoring of platforms' action as well as dedicated cooperation through the EEAS-managed Rapid Alert System. The pandemic sparked more efforts to tackle disinformation, and more public awareness. In the first half of 2020, the **EUvsDisinfo** public database of disinformation cases has added 1963 new pro-Kremlin related disinformation cases, of which close to one-third have been related to the COVID-19 infodemic. From mid-March to the end of April 2020, more than 10.000 people visited the website daily, and overall number of visitors grew by 400% compared to the same period in 2019. The EU response included targeted communication campaigns[78]and providing factual information about the pandemic.

The lessons learned have been fed into the development of the **European Democracy Action Plan** adopted on 2 December 2020[79]. This sets out key steps to reinforce the resilience of the EU's democratic fabric by promoting free and fair elections, addressing strains facing a free and independent media, and combating disinformation. This last aspect will build on the 2018 Action Plan against Disinformation[80] as the basis for increased EU action to tackle disinformation and for how to engage key stakeholders in civil society as well as private industry. It also looks forward to the next step with the **Code of Practice on Disinformation**, following the September 2020 assessment of the effectiveness of the Code[81]. The Code has been an important and necessary step towards creating a more transparent and accountable online platform ecosystem, but would be more effective with more uniform definitions, more consistent implementation, and more action to address specific areas such as micro-targeting. Another key tool that is now at the EU's disposal is the **European Digital Media Observatory,** which became operational as of June 2020. It brings together key stakeholders working on disinformation including fact-checkers and academic researchers.

IV PROTECTING EUROPEANS FROM TERRORISM AND ORGANISED CRIME

1. *Terrorism and radicalisation*

Recent attacks have shown once again that the terrorist threat in the EU remains high. The murder of a teacher in Conflans-Sainte-Honorine on 16 October 2020 was followed by the killing of three people in the church of Notre-Dame of Nice on 29 October. On 2 November, a terrorist attack in Vienna killed four people, and left 23 wounded. On 13 November, the Council adopted a Joint Declaration by EU Home Affairs Ministers on the recent terrorist attacks in France and Austria.[82] These recent jihadist-inspired attacks come on top of a rising threat from violent right-wing extremists and other forms of terrorism.

---

77 JOIN(2020) 8, Joint Communication, Tackling COVID-19 disinformation - Getting the facts right.

78 For example, the 'Think before you share' campaign was launched to provide advice how to limit the spread of disinformation to young audiences and multipliers in the EU's Eastern Partnership countries, reaching over 500.000 views on social media platforms.

79 COM (2020) 790.

80 JOIN(2018) 36 Joint Communication, Action Plan against Disinformation.

81 SWD(2020) 180.

82 Joint Statement by the EU Home Affairs Ministers on the recent terrorist attacks in Europe, 13.11.2020, 12634/20.

To further support Member States in the fight against terrorism and radicalisation, the Commission is adopting today a **Counter-Terrorism Agenda for the EU**[83]. This Agenda builds on existing policies and instruments and will strengthen the EU's framework to further improve on anticipating threats and risks, preventing radicalisation and violent extremism, protecting people and infrastructures, including through external border security, and effective follow-up after attacks. It also outlines the way forward to improve law enforcement and judicial cooperation, and the use of technologies and sharing of relevant information across the EU, including for those performing checks at the external borders. Implementation and enforcement of legislation remains key.

Prevention is key to fighting terrorism. EU efforts in the field of **prevention of radicalisation** build on the solid experience gained so far in the support to first line practitioners and policy makers. On 24 November, the Commission adopted a new **Action Plan on Integration and Inclusion**[84]. It is critical in the fight against radicalisation to work harder to bring communities together. A more cohesive and inclusive society can help prevent the spread of extremist ideologies that can lead to terrorism and violent extremism. Support to the **Radicalisation Awareness Network** includes a further €30m contract in January 2020 for the next four years of help to practitioners on the ground, as well as extra support to support policy makers and researchers. These and other instruments, such as the **EU Internet Forum**, will enable the Commission to address the priority actions highlighted in the 2021 Strategic Orientations on a coordinated EU approach to the prevention of radicalisation, developed with Member States. They are complemented by actions in the Counter-terrorism Agenda to counter extremist ideologies online, step up efforts in prisons and on rehabilitation and reintegration including for foreign terrorist fighters, and to strengthening support to local actors and building more resilient communities.

The **Directive on combating terrorism**[85] adopted in March 2017, is the main criminal justice instrument at EU level to counter terrorism. It sets minimum standards for defining terrorist and terrorism-related offences and for sanctions, while also giving victims of terrorism rights to protection, support and assistance. On 30 September 2020, the Commission adopted a report[86] assessing the measures that Member States have taken to comply with the Directive. It concludes that transposition into national law helped strengthen Member States' criminal justice approach to terrorism and the rights afforded to victims of terrorism, but that gaps remain. For example, not all Member States criminalise in their national law all the offences listed in the Directive as terrorist offences, as well as the provisions to criminalise travel for terrorism purposes and address the financing of terrorism, as well as to support victims. An evaluation report on the Directive will be adopted later in 2021.

The EU continues to work to support Member States to deny terrorists the means to attack and to support implementation of the rules. The Regulation on the marketing and use of **explosives precursors** adopted in June 2019[87] will start to apply as of 1 February 2021. To help national authorities and the private sector implement the Regulation, in June 2020 the

[83] COM (2020) 795.
[84] COM(2020) 758.
[85] Directive (EU) 2017/541.
[86] COM (2020) 619.
[87] Regulation (EU) 2019/1148.

Commission published a set of guidelines[88]. In addition, the Commission established a programme in June 2020[89] to monitor the outputs, results and impact of the Regulation.

In November 2019 the Commission invited Member States to assess the implementation of the 2017 Action Plan to enhance preparedness against **chemical, biological, radiological and nuclear (CBRN)** risks[90]. The overall conclusion was that a majority of actions have been implemented. In the beginning of 2020 the Commission, in cooperation with national experts, established a list of high risk chemicals of concern. This was the basis for engagement with equipment manufacturers with a view to improve detection capabilities. Recently, the Commission launched a study into the feasibility of restricting access to some of these chemicals. Work is also ongoing as part of the Union Civil Protection Mechanism, and additional CBRN response capacities are being discussed with Member States in the fields of Decontamination, Detection, Surveillance and Monitoring, as well as stockpiling.

On 12 October 2020, the Council decided to extend the sanctions regime against the proliferation and use of chemical weapons by one year[91], allowing the EU to impose restrictive measures on persons and entities involved in the development and use of chemical weapons.On 14 October 2020 the Council adopted restrictive measures against six individuals and one entity involved in the assassination attempt on Alexei Navalny, who was poisoned with a toxic nerve agent of the "Novichok" group on 20 August 2020 in Russia[92].

Financial information is also crucial to allow for the identification of terrorist networks, as terrorists rely on finance for travel, training and equipment, and **counter-terrorist financing** efforts are essential to counter-terrorism investigations. Key issues include exploiting existing tools and intelligence to their full potential, properly implementing internationally agreed standards, and addressing the evolving challenges posed by emerging technologies and social media platforms[93] (see below).

The **transport** network has been and continues to a target for terrorism. EU efforts include a risk-based assessment approach to protect the aviation sector[94]. Conflict zones pose a serious risk to civil aviation and information and risk assessment sharing is instrumental to risk mitigation[95]. The EU **Conflict Zone Risk Assessment** Information Alerting System is recognized as best practice and international standards on information sharing have been incorporated into EU legislation[96]. Based on the experience gained in the area of civil aviation, the Commission has extended the risk assessment based approach to other

---

88 Commission Notice - Guidelines for the implementation of Regulation (EU) 2019/1148 on the marketing and use of explosives precursors, OJ C 210/1, 24.6.2020.

89 SWD(2020) 114 final.

90 COM(2017) 610 final.

91 Council Decision (CFSP) 2020/1466 of 12 October 2020 amending Decision (CFSP) 2018/1544.

92 Council Decision (CFSP) 2020/1482 of 14 October 2020 and Council Implementing Regulation (EU) 2020/1480.

93 As set out by the EU in November 2019 at the *No Money For Terror* Ministerial Conference on Counter-Terrorism Financing hosted by Australia.

94 The integrated EU aviation security risk assessment process supports the decision making process in the area of air cargo security, aviation security standards and risks arising to civil aviation from conflict zones.

95 The tragic downing of the Ukraine International Airlines Flight 752 on 8 January 2020 further demonstrated the importance of information sharing and risks assessment for the security of civil aviation

96 https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32019R1583.

transport modes. The implementation of the EU **Rail Security Action Plan**[97] is well under way and benefits from the expertise of the EU Rail Passenger Platform, a dedicated expert group established by the Commission. In the maritime domain, the risk assessment based approach is well known and applied, and the Commission works with Member States and stakeholders to reinforce passenger security. This is incorporated into the **EU Maritime Security Strategy** and its **Action plan**, revised in 2018, including also a security and defence dimension. This is set out in last implementation report, adopted and published on 23 October 2020[98].

Europol provides support to Member States in investigations linked to terrorism through the **European Counter Terrorism Centre (ECTC)**. Member State requests for operational support to ECTC continued to increase, and ECTC is now part of nearly every major counter-terrorism investigation. During 2019, Europol supported a total of 632 different operations in the area of counter-terrorism. Member States investigators have also shown an increasing appreciation of this work, moving from a satisfaction level of 8/10 in 2018 to 9.1/10 in 2019. ECTC coordinated a total of 18 Action Days in 2019[99].

Eurojust also supported 116 terrorism investigations in 2019 and 2020. Current work will lead to a legislative proposal on exchanges on digital cross-border terrorism cases to develop the Counter Terrorism Register launched in 2019[100], as well as expanding work on right-wing and left-wing extremist groups.

On 30 July 2020, the Council last renewed the EU list of the persons, groups and entities subject to restrictive measures aimed at combating terrorism. The latest list contains 14 persons and 21 entities. On the same day, the Council imposed restrictive measures on one person under the ISIL (Da'esh)/Al-Qaida counter-terrorism sanctions regime. Currently there are five persons autonomously listed under this regime, which was renewed for one year on 19 October 2020.[101]

An important element of counterterrorism policy concerns the threats posed by **foreign terrorist fighters (FTFs)** currently in Syria and Iraq. While fully respecting the primary responsibility of Member States over these issues, support and cooperation at EU level helps Member States address common challenges: prosecution of those who have committed terrorist crimes, prevention of undetected entry into the Schengen Area and the reintegration and rehabilitation of returned foreign terrorist fighters. For instance, the Commission is working closely with Member States and key partner countries to ensure that battlefield evidence is shared and used effectively for identification, detection at EU's borders and prosecution. The 2020 Memorandum on Battlefield Evidence[102] published by Eurojust shows that while there are many challenges in obtaining such data and making sure it meets the criteria for admissible evidence, it can help to bring terrorist suspects to justice.

---

97 COM 2018 (470) final.

98 Report by Commission services, the European External Action Service and the European Defence Agency on the implementation of the revised EU Maritime Security Strategy Action Plan" SWD(2020) 252.

99 2019 Consolidated annual activity report, Europol, 9.06.2020.

100 The CTR is managed by Eurojust on a 24-hour basis and provides proactive support to national judicial authorities. This centralised information should help prosecutors to coordinate more actively and to identify suspects or networks being investigated in specific cases with potential cross-border implications.

101 Council Decisions (CFSP) 2020/1132, 2020/1126 and 2020/1516.

102 https://www.eurojust.europa.eu/eurojust-memorandum-battlefield-evidence-0.

The Commission is also facilitating a dialogue with Member States and humanitarian actors to provide a comprehensive and factual overview of the situation in the North East Syrian camps where European FTF family members are located. A particular focus is placed on the situation of children in the Syrian camps. The Commission also helps Member States to share experiences about national measures and mechanisms to better manage **the rehabilitation and reintegration** of returning FTFs, as well as children. The Radicalisation Awareness Network also runs study visits and provides tailor made advice to better deal with the challenges of convicted returnees in particular after release from prison, as well as the role of families and of local communities in reintegration efforts.

Counter-terrorism **partnerships and cooperation with third countries** and partners in the EU's neighbourhood is also essential to improve security inside the EU and to better link the internal and external dimensions of EU security policy. The Council has called for further strengthening of the EU's external counter-terrorism engagement[103] with a focus on the Western Balkans, North Africa and the Middle East, the Sahel region, the Horn of Africa and Asia. This work is taken forward making full use of external action tools, including high-level counter-terrorism dialogues and the network of 17 **counter-terrorism/Security experts**[104] deployed in EU Delegations which has continued to provide support, facilitating cooperation and promoting capacity building. A reflection on the possibility to strengthen and to expand this network is currently ongoing.

The 2018 Joint Action Plan on Counter-terrorism for the **Western Balkans** and the accompanying bilateral arrangements signed in 2019 with each partner[105] provide a focus on a region of key significance for common security objectives and for the protection of people living in the EU. At the EU-Western Balkans Ministerial Forum on Justice and Home Affairs on 22 October 2020, the EU and the Western Balkans partners reaffirmed their commitment to implementing the Joint Action Plan's objectives beyond 2020.[106] Cooperation with the Western Balkans includes managing the ongoing return of FTFs and their family members as well as a further integration into anti-radicalisation activities. The EU also maintains a regular engagement on counter-terrorism with the **Middle East, North Africa and Central Asia**[107]. Work with **Central Asia** has focused on addressing chemical, biological, radiological and nuclear threats. The **EU-Gulf Cooperation Council** Joint Cooperation Committee met on 25 June 2020 and covered issues including countering radicalisation and tackling financing of terrorism and anti-money laundering, as well as cybersecurity and cooperation with Europol. The EU worked with NATO on a first-ever audit on chemical, biological, radiological and nuclear threats in one of the Gulf countries in late 2019. Overall, at the end of 2019, some €465 million was devoted to on-going projects on counter-terrorism and the prevention of violent extremism outside the EU, a 15% increase from the previous year.

---

[103] Council Conclusions (8868/20)on EU External Action on Preventing and Countering Terrorism and Violent Extremism (16 June 2020).

[104] Algeria, Bosnia-Herzegovina (regional for Western Balkans), Chad (regional for the Sahel), Ethiopia (liaison to the African Union), Indonesia (regional for Southeast Asia and liaison to ASEAN-ARF), Iraq, Jordan, Kenya (regional for the Horn of Africa), Kyrgyzstan (regional for Central Asia), Lebanon, Libya, Morocco, Nigeria, Pakistan, Saudi Arabia, Tunisia and Turkey.

[105] Serbia, North Macedonia, Bosnia and Herzegovina, Kosovo*, Albania, and Montenegro.

[106] Joint Press Statement: https://www.consilium.europa.eu/en/press/press-releases/2020/10/23/joint-press-statement-eu-western-balkans-ministerial-forum-on-justice-and-home-affairs/pdf.

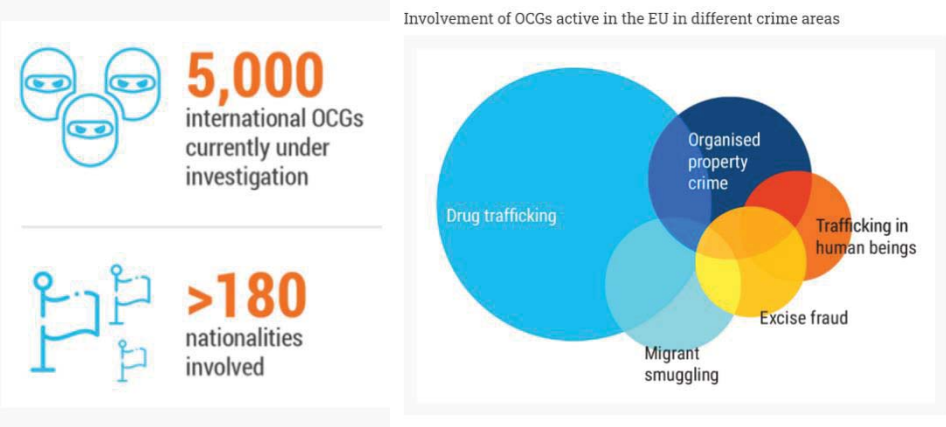
[107] Counter-terrorism action was for example highlighted in the new EU strategy on Central Asia.

*This designation is without prejudice to positions on status, and is in line with UNSCR 1244(1999) and the ICJ Opinion on the Kosovo declaration of independence.

The EU has also continued to deepen cooperation with the **United Nations** on counter-terrorism[108], notably with the UN Office of Counter-Terrorism and the Counter-Terrorism executive directorate, including though annual high-level dialogues and most recently through active participation in the virtual UN counter-terrorism week in summer 2020. The Commission has also closely followed the deliberations on a revision of the definition of terrorist offences in the **Council of Europe**'s Convention on the prevention of terrorism, encouraging close alignment with definitions in EU law. Good cooperation continued in the area of counter-terrorism and chemical, biological, radiological and nuclear materials between **NATO** and the EU, exchanging information on capacity-building to avoid duplication and ensure complementarity.

2. Fighting organised crime

Organised crime is rising, becoming ever-more cross-border, and moving online.



Europol, Serious and Organised Threat Assessment (SOCTA 2017)

Commission action has included the fight against drugs, illegal firearms, financial crime, illegal import of cultural goods, human trafficking or environmental crime, supporting Member States law enforcement and judicial authorities in Member States as well as partners in the neighbourhood. Cooperation with third countries, in particular in the neighbourhood such as the Western Balkans, and international organisations, including the United Nations' Office on drugs and crime[109], were also key.[110]

In 2019, **Europol Serious and Organised Crime Centre** received and processed almost 55,000 operational contributions, which represents an increase of 12% compared to 2018. With regards to the number of operations supported, the centre assisted countries in 726 cases[111]. It is also crucial that the EU's legislative framework on organised crime[112], which seeks to harmonise Member State's laws on the criminalisation of offences linked to participation in a criminal organisation, and lays down penalties for these offences, is fully transposed in all Member States. The Commission has launched a study to analyse ways to enhance this legislation. Further steps on stepping up the fight against organised crime in

[108] In 2019 a Framework for cooperation between de EU and the UN was signed on counter terrorism was signed https://eeas.europa.eu/sites/eeas/files/2019042019_un-eu_framework_on_counter-terrorism.pdf.
[109] A high-level EU-UNODC dialogue took place on 8 December 2020.
[110] At the end of 2019, some €830 million was devoted to ongoing actions on organised crime outside the EU.
[111] 2019 Consolidated Annual Report, Europol, June 2020.
[112] Framework Decision 2008/841.

the EU will be drawn together in the EU Agenda to tackle organised crime to be adopted in the first quarter of 2021.

The freezing and the confiscation of proceeds of crime are among the most effective means of combatting organised crime. The new **European Financial and Economic Crime Centre** (EFECC) established in June 2020 at Europol will enhance the operational support provided to Member States and EU bodies in the fields of financial and economic crime and promote the systematic use of financial investigations. Supporting EU efforts on more effective identification, freezing and confiscation of criminal assets, the Council adopted Conclusions in June 2020 on enhancing financial investigations to fight serious and organised crime.[113] In 2021, the Commission will review legislation on freezing and confiscation the proceeds of crime[114] and on Asset Recovery Offices.[115]

The fight against organised crime needs safeguards to ensure the work of law enforcement can operate effectively within essential boundaries, such as the protection of personal data. The 2016 Data Protection Law Enforcement Directive on the protection of natural persons regarding processing of personal data connected with criminal offences[116] protects fundamental right to data protection whenever personal data is used by criminal law enforcement authorities for law enforcement purposes. It ensures that the personal data of victims, witnesses, and suspects of crime are duly protected and facilitates cross-border cooperation in the fight against crime and terrorism. The deadline for the transposition of the Data Protection Law Enforcement Directive expired on 6 May 2018. To date, most Member States have adopted legislation transposing the Directive. However, some infringement procedures are still ongoing[117]. The Commission is currently assessing the conformity of national transposing laws with the Directive.

Fight against illegal drugs

The Commission adopted in July 2020 a new **EU Agenda and Action Plan on Drugs 2021-2025**[118], following on the current EU drugs strategies[119]**.** This sets out the political framework and priorities for action in the next five years. The main focus of the Agenda is on: (1) enhanced security measures against illicit trafficking of drugs from organised crime groups to external border management and illicit distribution and production; (2) increased prevention including awareness raising of the adverse effects of drugs, notably the intersection between drug use, violence and other criminality; and (3) addressing drug related harms through access to treatment, risk and harm reduction, and a balanced approach to the issue of drugs in prisons. On 30 November 2020 the Commission also adopted an evaluation of the EU drug precursor policy which concludes that additional action is needed to prevent access of organised crime groups in the EU to the chemicals they need to produce illegal synthetic drugs[120].

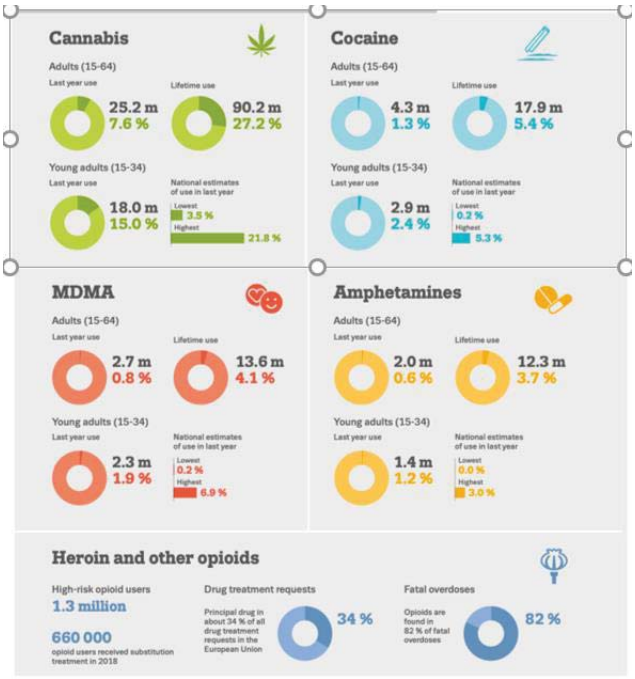
---

[113] Council conclusions 8927/20.
[114] Directive 2014/42/EU.
[115] Council Decision 2007/845/JHA.
[116] Directive (EU) 2016/680 on the protection of natural persons regarding processing of personal data connected with criminal offences.
[117] Three Member States (Germany, Slovenia, Spain) are yet to notify full transposition despite infringement procedures. The Commission brought one case for non-transposition to the Court of Justice, and in May 2020 addressed supplementary reasoned opinions to the other two Member States for failing to fully transpose the Directive.
[118] COM(2020) 606.
[119] The EU Drugs Strategy 2013-2020 and the EU Action Plan on Drugs 2017-2020.
[120] COM(2020) 768 of 30 November 2020.

The EU has also funded concrete projects to enhance the fight against drugs such as the Civil Society Forum on Drugs. The European Drug Report 2020 of the European Monitoring Centre for Drugs and Drug Addiction published on 22nd September 2020[121] shows recent drug use and market trends across the EU, Turkey and Norway. It shows an increase in cocaine availability with seizures at a record high amounting to 181 tonnes, an almost doubling of heroin seizures to 9.7 tonnes and high availability of high-purity drugs in the EU. It also explores the appearance of novel synthetic opioids, of particular health concerns and addresses the challenges caused by the COVID-19 pandemic.

Work against drugs is taken forward on several different levels. The **legislative package on new psychoactive substances** (NPS) was adopted in autumn 2017[122] and became fully applicable in November 2018. Five Member States are still under infringement procedure[123]. The first delegated act to define a new psychoactive substance (isotonitazene) as a drug has now been adopted.[124]

On the **international stage**, the EU has been active in the United Nations Commission on Narcotic Drugs[125], notably to update as regards the scheduling of new psychoactive substances[126] as well as for the re-scheduling of cannabis and cannabis-related substances[127]. Two new dialogues on drugs with China and Iran have been approved by the Council[128], and the European Monitoring Centre for Drugs and Drug Addiction has moved ahead with working arrangements with third countries[129].



Fight against financial crime

New legislation has been adopted to enhance the fight against financial crime as well as money laundering. The directive facilitating the use of financial and other information for the prevention, detection, investigation or prosecution of certain criminal offences was adopted in 2019 granting access to national centralised bank account registries to law enforcement authorities and Asset Recovery Offices for the purposes of fighting serious crime. The Directive also aims to improve cooperation between law enforcement authorities and Financial Intelligence Units (FIUs) and facilitate the exchange of information between FIUs. In June 2020, the Commission published a

[121] European Drug Report 2020: Trends and Developments, EMCDDA, 22.09.2020.
[122] Regulation (EU) 2017/2101, and Directive (EU) 2017/2103,
[123] Austria, Finland, Ireland, Portugal and Slovenia.
[124] C/2020/5897; OJ L 379, 13.11.2020, p. 55.
[125] A governing body of UN Office on Drugs and Crime (UNODC).
[126] COM(2019) 631.
[127] COM(2019) 624 and COM(2020) 659.
[128] The EU-China Summit of 16-17 July 2018 in Beijing resulted in an agreement to launch an annual EU-China Dialogue on Drugs. The modalities of the future dialogue were confirmed by COREPER on 30 October 2019. The Council approved the launch of a new EU-Iran dialogue on drugs on 5 March 2020.
[129] Commission opinion regarding the draft working arrangement with Kosovo adopted on 14 April 2020, and on the one with Serbia adopted on 16 December 2019.

report on "Asset recovery and confiscation: ensuring that crime does not pay"[130] This pointed to the potential for greater harmonisation in asset recovery regimes[131] to modernise EU legislation on asset recovery and strengthen national authorities' capacities in fighting organised crime. Further analysis of asset recovery through an external study has been launched. The regulation on the mutual recognition of freezing and confiscation orders[132] will apply from 19 December 2020 and will considerably enhance cooperation between Member States.

In May 2020, the Commission adopted **an action plan for a comprehensive Union policy on preventing money laundering and terrorism financing**[133] to enhance the EU framework. On 5 November, the Council adopted Conclusions on anti-money laundering and terrorism financing[134] notably asking the Commission to work on the adoption of a single rulebook, the establishment of an independent supervisor and coordination of Financial Intelligence Units. In line with the Council Conclusions on enhancing financial investigations[135], the Commission is also assessing the need to interconnect centralised bank account registries, which would significantly speed up access to information of bank accounts for Financial Intelligence Units and law enforcement. In parallel, efforts continue to ensure that the latest EU standards are effectively implemented by Member States. Rules under the 5th Anti- Money Laundering Directive aim to ensure the increased level of transparency of corporate ownership structures. The transposition deadline expired on 1 January 2020 and the Commission launched infringement proceedings against 16 Member States[136]. Another important measure is the new Cash Controls Regulation[137] adopted in October 2018 and applicable from 3 June 2021. It will improve the existing system of controls on cash entering or leaving the EU and implementing provisions are under preparation.

On the external front, efforts continue to support partner countries in addressing money laundering and terrorist financing. In this context, the EEAS and EU Delegations play a key role in promoting and supporting the political engagement with third countries and international organisations such as the Financial Action Task Force (FATF).

To complement this work, the Commission has launched a global facility to provide support to partner countries outside the EU to put in place effective anti-money laundering/countering terrorism financing frameworks in line with international standards. The €20m action also aims to encourage cooperation between financial, justice actors at national, regional and international levels.

Fight against corruption

Corruption is a crime in itself and a key enabler of organised crime. The prevention and fight against corruption will be subject to regular monitoring and assessment of Member States legal framework under the newly established **Rule of law mechanism**[138]. The first

[130] COM (2020) 2017.
[131] Including the assessment of Directive 2014/42/EU and Council Decision 2007/845/JHA.
[132] Regulation (EU) 2018/1805
[133] C(2020) 2800 final.
[134] Council conclusions 12608/20.
[135] Council conclusions 8927/20.
[136] Austria, Belgium, Cyprus, Czechia, Greece, Hungary, Estonia, Ireland, Luxembourg, Netherlands, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, as well as the United Kingdom
[137] Regulation (EU) 2018/1672.
[138] The European Rule of Law Mechanism provides a process for dialogue between the Commission and Member States, as well as the Council and the European Parliament, and national parliaments, civil

EU-wide report on the rule of law was adopted on 30 September 2020[139]. It showed that many Member States have high rule of law standards, but important challenges remain. The report covers all Member States with objective and factual annual assessments, with the goal of developing a stronger awareness and understanding of developments in the individual Member States as they occur, to be able to identify risks, develop possible solutions, and target support early on. The **European Public Prosecutor's Office** (EPPO) will tackle crime against the EU budget, at this stage in the participating 22 EU countries. It will have the power to investigate, prosecute and bring to judgment those responsible for criminal offences against the EU budget, such as fraud, corruption or serious cross-border VAT fraud. The EPPO should be operational in the first quarter of 2021. [140]

The Commission is currently assessing the transposition into national law of the rules laid down in the **Directive on the fight against fraud to the Union's financial interests** by means of criminal law[141] and has brought infringement procedures against those Member States that did not notify a full transposition[142]. In 2021, the Commission will adopt a report assessing the extent to which the Member States have taken the necessary measures in order to comply with the Directive.

Fight against trafficking in cultural goods

The main objective of the **Regulation on the introduction and import of cultural goods[143]** adopted in June 2019 is to stop imports in the Union of cultural goods illicitly exported from their country of origin. To ensure its proper implementation, the Commission is currently preparing the adoption of implementing provisions, including for a centralised electronic system for the Import of Cultural Goods, which will allow the storage and exchange of information between Member States and the necessary import formalities[144]. A general prohibition rule will enter into force by the end of 2020, providing Member States customs with the legal means to control and act on for shipments which may contain cultural goods illicitly exported from their country of origin.

Fight against illegal firearms trafficking

On 24 July 2020, the Commission published **a new 2020-2025 EU action plan on firearms trafficking.[145]** A High-level ministerial conference of EU and Western Balkan foreign affairs and home affairs ministries on 31 January 2020 had underlined the need for more action to fight illegal firearms trafficking. The Action Plan includes specific actions to improve the legal control of firearms, the knowledge of the firearm-related threat, law enforcement cooperation and international cooperation with a focus on south-east Europe. The Commission took steps to ensure that that Directive on control of the acquisition and

---

society and other stakeholders on the rule of law. The Rule of Law Reports are the core of this new process.

139 COM(2020) 580.

140 The Council Implementing Decision appointing the European Prosecutors entered into force on 29 July 2020. The European Prosecutors form the College held its first meeting on 28 September 2020. The EPPO will soon conclude working arrangements with Europol, Eurojust and OLAF.

141 Directive (EU) 2017/1371.

142 Infringement procedures currently remain open against Austria, Ireland, and Romania.

143 Regulation (EU) 2019/880

144 The ICG has to be established before 28 June 2025 at the latest. The Commission has adopted a first Progress Report on developing the ICG. [COM(2020) 342].

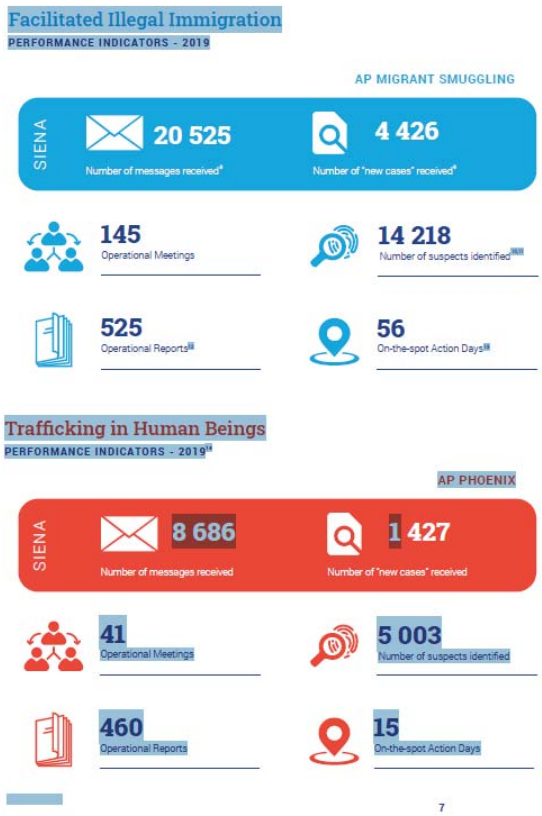
145 COM(2020)608: this new action plan integrates the franco-german initiative for the Western Balkan "Roadmap for a sustainable solution to the illegal possession, misuse and trafficking of SALW and their ammunition until 2024".

possession of weapons adopted in May 2017[146] is fully transposed by Member States. However, 10 Member States are yet to notify the full transposition of the Directive[147] and a large majority of Member States have not transposed the implementing legislation that followed. The Commission has launched infringement procedures as a result[148]. The Commission is also assessing in detail the notified transposition measures and will report on the implementation of the Directive in the first half of 2021. The Commission has also started to assess the possible modernization of the legal framework on imports, exports and transit measures of firearms.[149]

Fight against trafficking in human beings

The Security Union Strategy highlighted the need to develop a new strategic approach towards eradicating trafficking in human beings within the context of the Agenda on tackling organised crime. In addition, as laid down in Article 20 of the Anti-trafficking Directive[150] the Commission published in October 2020 its third report on the progress made in the fight against trafficking in human beings.[151].

This shows advances in transnational cooperation, cross-border law enforcement and judicial operational actions; the setting-up of national and transnational referral mechanisms for victims and developing the knowledge base about trafficking. Member States make increasing use of EU Agencies to exchange information, carry out joint action and Joint Investigation Teams to fight trafficking in human beings both inside the EU and beyond[152]. Operational cooperation



[146] Directive (EU) 2017/853. Also key were two implem technical specifications on marking and signal and alar

[147] These are Czechia, Denmark, Spain, Cyprus, Luxembourg, Hungary, Poland, Slovenia, Slovakia and Sweden

[148] There are 25 ongoing regarding this Directive(Austria, Belgium, Bulgaria, Cyprus, Czechia, Denmark, Germany, Estonia, Greece, Spain, Finland, France, Hungary, Ireland, Lithuania, Luxembourg, Latvia, Malta, Netherlands, Poland, Portugal, Romania, Sweden, Slovenia, and Slovakia, as well as the United Kingdom) and 34 related to the implementing Directives (Directive 2019/68 - Austria, Belgium, Bulgaria, Cyprus, Czechia, Germany, Greece, Spain, Finland, Croatia, Hungary, Ireland, Italy, Luxembourg, Poland, Romania, Sweden, Slovenia, plus the United Kingdom and Directive 2019/69 - Bulgaria, Cyprus, Czechia, Greece, Spain, Finland, Croatia, Hungary, Ireland, Italy, Luxembourg, Netherlands, Poland , Romania, Sweden, and Slovenia, as well as the United Kingdom)

[149] Regulated by Regulation (EU) No 258/2012.

[150] OJL -101, 15.04.2011, p1.

[151] COM(2020) 661 final, complemented by a study on the data collection of trafficking in human beings in the EU 2017-2018.

[152] For example, the European Labour Authority cooperated with Europol to combat trafficking in human beings in the EU for all forms of exploitation, including sexual and labour exploitation as well as all

has brought tangible results, notably in the framework of the European multidisciplinary platform against criminal threats: in 2019 this work has resulted in 825 arrests, 8,824 suspects identified and 1,307 potential victims, including 69 children identified. 94 organised crime groups involved in these crimes were identified or dismantled and €1.5 m of assets frozen in bank accounts, companies and web domains. On EU Anti-Trafficking Day on 18 October 2020, the Commission published a study on the costs of trafficking in human beings and another on the national and transnational referral mechanisms[153].

Smuggling of migrants

The European migrant smuggling centre has reported a continued increase of **migrant smuggling** activities, mostly in the Western Balkans and neighbouring countries, and in secondary movements across the EU. In 2019, Europol contributed to the identification of 14 218 suspects active in migrant trafficking[154]. In May 2020 Eurojust launched the Focus Group for Prosecutors on Migrant Smuggling as an important hub to regularly connect the key judicial actors at national level in the EU Member States and to support their joint operational response[155].

Fight against environmental crime

Environmental crime covers acts that breach environmental legislation and cause or can cause significant harm or risk to the environment and human health[156]. Among the most important areas of **environmental crime** are the illegal emission or discharge of substances into air, water or soil, the illegal trade in wildlife, illegal trade in ozone-depleting substances and the illegal shipment or dumping of waste. The recent evaluation of the Environmental Crime Directive[157] showed progress in developing a European framework was not matched by a significant effect on the ground, including in terms of better cross-border cooperation and a more level playing field with regard to sanctions across Member States. In particular, it had not led to more convictions and the imposition of more dissuasive sanctions in the Member States. It has therefore been decided to review the Directive by the end 2021.

On 29-30 October 2019, Eurojust held jointly with the European Network of Prosecutors for Environment (ENPE) the conference "International collaboration & co-operation in the fight against environmental crime", to raise awareness and to promote cross-border cooperation among prosecutors and other practitioners within and outside the EU on environmental crime.

The Action plan against wildlife trafficking adopted in 2016 is currently being evaluated. One specific action is a project running until January 2021 targeting wildlife trafficking in

---

forms of child trafficking. This is also in recognition of Forced Labour Protocol (P29) of the International Labour Organization. This Protocol is a core labour standard identifying forced labour as a crime, addressing prevention, protection of victims, compensation and international cooperation in present forms of forced labour, including related to trafficking.

153 Studies on the economic, social and human costs of trafficking in human beings and reviewing the functioning of Member States' National and Transnational Referral Mechanisms, available on https://ec.europa.eu/anti-trafficking.

154 European migrant smuggling centre, 4th annual report, 15.05.2020.

155 http://www.eurojust.europa.eu/press/PressReleases/Pages/2020/2020-05-29.aspx.

156 Directive on the protection of the environment through criminal law, 2008/99/EC.

157 SWD(2020) 259 final.

and via the EU using the internet and parcel delivery services, with the aim of disrupting and dismantling wildlife cybercrime networks[158].

V. A STRONG EUROPEAN SECURITY ECOSYSTEM

A genuine and effective Security Union must be the common endeavour of all parts of society. Governments, law enforcement, the private sector, education and citizens themselves need to be engaged, equipped, and properly connected to build preparedness and resilience for all, particularly the most vulnerable, victims and witnesses.

1. Cooperation and information exchange

One of the most critical contributions the EU can make to protecting citizens is through helping those responsible for security to work well together. Cooperation and information sharing are powerful tools to combat crime and terrorism, tackle threats like cybersecurity, and pursue justice. A number of tools have been put into place to support information exchange among law enforcement and judicial authorities.

Today, the Commission is adopting a revised mandate for **Europol**[159] to bring a number of targeted improvements to its work. This will enable Europol to deal better with the evolving nature of crimes carried out by means of the internet and with financial crimes. It will reinforce the cooperation with the private sector and align data protection provisions with existing EU rules.

Europol, and other EU Agencies such as Frontex, CEPOL and Eurojust, with the support of the Commission, has continued to develop the EU policy cycle for serious and international organised crime, the "**European Multidisciplinary Platform Against Criminal Threats**" (EMPACT).[160]. Cooperation under EMPACT has continued to prove an effective tool against organised crime across Europe, as for instance during "Joint Action Days" in September, October and November 2020.[161] This is a clear demonstration of the value of cooperation. It also supported less quantifiable goals: an improved intelligence picture, training and capacity building, prevention, cooperation with non-EU partners, and fighting online crime[162].The independent evaluation of the EU Policy Cycle 2018-2021/EMPACT in 2020[163], concluded that it was proving increasingly relevant and effective in tackling the most pressing threats posed by organised crime groups. Added value comes by providing a platform for cooperation that enables Member States to

---

158 https://wwf.be/fr/wildlife-cybercrime/.

159 COM (2020) 796.

160 EMPACT is the EU police cooperation tool to address the most important threats to EU security by strengthening co-operation between the relevant services of the Member States, EU institutions and EU agencies as well as third countries and organisations. EMPACT associates different stakeholders (multidisciplinary approach) to improve and strengthen the co-operation between Member States, EU institutions and EU agencies as well as third countries and organisations, including the private sector.

161 EMPACT Joint Action Days: "operation BOSPHORUS", 1,776 firearms seized (2-11 November)., "JADs Mobile 3": more than 350 stolen cars and more than 1000 stolen car parts were recovered. (12-13 October), "JADs against human trafficking for labour exploitation", officers identified 715 potential victims of labour exploitation (14-20 September). "JADs against crime in southeast Europe", 51 weapons of different types and 47 kilograms of a variety of drugs (September).

162 All detailed factsheets of results with figures, per EMPACT EU crime priorities, can be consulted here: https://data.consilium.europa.eu/doc/document/ST-7623-2020-INIT/en/pdf, Doc 7623/20 5 May 2020.

163 An independent evaluation was foreseen in Council conclusions of 27 March 2017 on the continuation of the EU Policy Cycle for organised and serious international crime for the period 2018-2021 (7704/17).

achieve better results against serious and organised crime than if they had tackled these issues alone. The evaluation also flagged opportunities and made recommendations to further develop this very useful cooperation tool for the next cycle 2022-2025.

The Commission will launch an initiative in 2021 for **an EU Police Cooperation Code**, to streamline, enhance, develop, modernise and facilitate law enforcement cooperation between relevant national agencies. This will be a major support to Member States in their fight against serious and organised crime and terrorism.

Cooperation is also needed between **police and other key law enforcement authorities**, as well as with agencies such as customs. EU **customs** holds a key role in ensuring external border and supply chain security and thus contributes to the internal security of the European Union. New and evolving threats touch upon the main interlinks between customs and law enforcement authorities, stressing in particular the "detection/prevention" value of customs controls and the lead role of customs regarding goods. The Commission has been supporting and encouraging cooperation between Customs and Europol[164], with a direct impact on action in areas including firearms, environmental crime, criminal financing, and cyber. Customs authorities currently participate in several Europol-led actions against serious and international organised crime[165], as well as in CEPOL trainings. These activities help to promote and develop further inter-agency cooperation and enhance the interaction between the key players.

Strong and efficient information systems are indispensable to better exchange information between judicial and law enforcement authorities across the EU. The **Schengen Information System (SIS)** has also been reinforced through updated rules which address potential gaps by establishing additional categories of alerts, by expanding the list of objects for which alerts can be entered as well as by permitting new types of data to be entered[166]. The new rules entered into force on 28 December 2018 and should be completely operational by December 2021[167].

Similarly, in 2019 the **European Criminal Records Information System (ECRIS)** was supplemented by an additional system allowing for an efficient exchange of the criminal records information on third country nationals convicted in the EU (ECRIS-TCN). The works on the technical development and implementation of this new centralized system are currently ongoing and its entry into force is expected in 2023.

On 24 July 2020, the Commission adopted the Passenger Name Record (PNR) Directive Review Report[168], reviewing the first two years of application of the PNR Directive.[169] This shows that the development of the EU-wide PNR system is well under way. The use of PNR data is essential in the fight against terrorism, serious crime and organised crimes, and has already delivered tangible results. Only one Member State has not yet notified the

[164] See for example the Customs Cooperation Working Party (CCWP) Action Plan. Key areas for 2020-2021 include: an increased presence of customs officials in the Liaison Bureaux in Europol, direct access for customs authorities to the Europol Secure Information Exchange Network Application (SIENA), a better representation of customs officials in the Europol National Units and participation of Police and Customs chiefs in the European Police Chief Convention.

[165] Excise/VAT fraud, firearms trafficking, environmental crime, criminal finances, fight against child sexual abuse.

[166] Regulation (EU) 2018/1860, Regulation (EU) 2018/1861, Regulation (EU) 2018/1862.

[167] The SIS will also be updated in line with the proposed amendments to the Europol Regulation (COM(2020) XXX).

[168] COM(2020) 305.

[169] Directive (EU) 2016/681.

Commission of full transposition[170]. On 3 December 2020 the Commission sent a Reasoned Opinion for failing to notify full transposition of the Directive.

On 9 September 2020 the Commission published the evaluation of the **Advanced Passenger Information Directive** of 2004[171]. The evaluation highlights a number of shortcomings and inconsistencies, which will be considered in the upcoming revision of the current legislative framework. Another key instrument under further examination is the **Prüm Decisions**[172], to be considered in the light of operational, technological, forensic and data protection developments.

Cooperation must also go beyond the EU to engage with **key third countries on tackling terrorism and organised crime**. On 13 May 2020 the Council authorised the opening of negotiations with New Zealand concerning the exchange of personal data between Europol and New Zealand. Negotiations with Turkey are ongoing, however, no progress has been made on negotiations with Algeria, Egypt, Israel, Jordan, Lebanon, Morocco, Tunisia on the exchange of personal data for fighting serious crime and terrorism. In addition, on 19 November 2020, the Commission adopted a Recommendation for a Council Decision authorising the opening of negotiations for an Agreement between the European Union and ten third countries on cooperation between Eurojust and those third countries regarding the exchange of personal data[173].

As regards **international cooperation on the exchange of PNR** for the purposes of fighting terrorism and serious crime, the Council authorised the opening of negotiations with Japan for the signature of a PNR agreement.[174] Meanwhile, the **joint evaluations of the existing EU-US and EU-Australia agreements** *are being finalised.* The Commission has also launched a process to review its current overall approach on PNR data transfers to third countries.[175]

The Commission is also working with the UN to increase the capacity of partner countries to prevent, detect, investigate and prosecute terrorist offences and other serious crimes, by collecting and analysing passenger data, both API and PNR.

The Commission engaged in the process of facilitating transfers of PNR data in compatibility with EU legal requirements in the framework of the new PNR standards[176] adopted by the International Civil Aviation Organisation (ICAO).[177]. On 23 June 2020, the ICAO Council adopted the new Standards and Recommended Practices (SARPs) on PNR [178] and its contracting parties have until 30 January 2021 to inform ICAO of any differences between their national regulation practices and the new PNR SARPs.

---

[170] Slovenia

[171] SWD(2020) 174.

[172] The Prüm Framework enables the automated exchange of DNA, fingerprint and vehicle registration data between law enforcement authorities. An inception impact assessment has been published.

[173] The proposed third countries are the following: Algeria, Armenia, Bosnia and Herzegovina, Egypt, Israel, Jordan, Lebanon, Morocco, Tunisia and Turkey, COM (2020) 743 final.

[174] 18 February 2020.

[175] Roadmap on the external dimension of the EU policy on Passenger Name Records available at: https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12531-External-dimension-of-the-EU-policy-on-Passenger-Name-Records-

[176] Council Decision (EU) 2019/2107, p. 117–122.

[177] Security Council resolution 2396 (2017).

[178] Referred to as Amendment 28 to Annex 9 (Facilitation) of the Convention on International Civil Aviation (the "Chicago Convention").

2. The contribution of strong external borders

Modern and efficient management of external borders is key to ensure the security of EU citizens. Engaging all relevant actors to make the most of security at the border and provide them with adequate tools can have a real impact on the prevention of cross-border crime and terrorism. The New Pact on Migration and Asylum[179] also highlighted the need for robust and fair management of external borders, including identity, health and security checks. This is part of the comprehensive approach, showing how policy on migration, asylum, integration and border management depends on progress on all fronts.

The New Pact underlined that an effective Schengen area was indispensable to migration policy, and it also has profound security implications. This was discussed at the first Schengen Forum held on 30 November 2020. Representatives from the Member States and European Parliament agreed of the importance of an effective Schengen delivering for citizens in terms of free movement, and also in terms of security. This process will feed into a new Schengen Strategy to be put forward in 2021. The Schengen Evaluation and Monitoring Mechanism is a key tool to ensure mutual trust and to guaranteeing a better and coherent implementation of the Schengen acquis, including its security implications. This was an important theme of the report adopted on 25 November[180], providing a state of play of the implementation of the Schengen acquis, and taking stock of the functioning of the Schengen Evaluation and Monitoring Mechanism.

The **Interoperability Regulations**[181] are designed to make existing and new or upgraded the EU information systems for security, border and migration management work together in a smarter and more efficient way. Interoperability between EU information systems will improve the effectiveness and efficiency of checks at the external borders, contribute to the prevention of irregular immigration and also to a high level of security. It will provide a valuable extra tool for law enforcement and border authorities[182]. Member States, Schengen associated countries and the relevant Union agencies (eu-LISA, the European Border and Coast Guard Agency and Europol) need to be ready and the Commission is monitoring preparation and readiness to ensure that full implementation is achieved by the end of 2023.

A provisional agreement has been found on 8 December 2020 between the co-legislators on the proposal to **update the Visa Information System**[183].

However, **some key legislation still need to be adopted**. The European Parliament needs to conclude its readiness to engage with the Council on the amendments[184] on the European Travel Information and Authorisation System (ETIAS)[185].

The links between relevant information systems for security risk analysis are crucial to enhance our security. Enhancing **cooperation between customs and border management** authorities and synergies between their **information systems** in compliance with relevant

---

[179] COM (2020) 609.
[180] SWD(2020)327final.
[181] Regulation 2019/817 and Regulation (EU) 2019/818.
[182] Existing systems: Schengen Information System, (SIS) Visa Information System (VIS), Eurodac and future systems: Entry/Exit system, European Travel Information and Authorization System (ETIAS), European Criminal Records Information System for third country nationals (ECRIS-TCN) ETIAS, ECRIS-TCN) .
[183] COM(2019)12
[184] COM(2019) 3 final and COM(2019) 4 final.
[185] Regulation (EU) 2018/1240 and Regulation (EU) 2018/1241.

checks and balances, including the protection of personal data and privacy legislations, is a priority of the Action Plan on Taking the Custom Union to the next level of 28 September 2020[186]. A preliminary assessment conducted by the Commission with police and customs experts from Member States recommends in particular a link-up of the Schengen Information System (SIS) and Europol data with the customs Import Control System (ICS2)[187], and a feasibility study will now be launched.

The **European Border and Coast Guard Regulation**[188] entered into force in December 2019 and represents a major overhaul of EU capabilities and tools to strengthen EU external borders. This will allow the contribution of borders to security to be significantly enhanced. The new mandate reinforces Frontex's ability to support the Member States in the management of external borders and returns and extends the possibilities for the cooperation with third countries. Work is under way to ensure the readiness of the European Border and Coast Guard standing corps for its first deployment as of 1 January 2021.

In June 2019, the EU introduced **tighter security standards for ID cards** in order to facilitate free movement of EU citizens and at the same time to reduce identity fraud [189]. Member States are required to start issuing identity cards and residence documents with new security standards as of August 2021. Most of them are currently in the process of aligning their document designs with the requirements of the Regulation.

3. Strengthening security research and innovation

Research on security and promoting innovation underpin a coordinated EU response to complex challenges, and allow for concrete steps to mitigate risks. The Security Union is one of four focus areas under the 2018-2020 work programme for **Horizon 2020**[190], which represents 50% of overall public funding for security research in the EU. The 2019 Horizon 2020 security research calls led to the selection of 42 projects to receive a total of €253 million in EU funding. Work will include protecting infrastructure, increasing disaster resilience, fighting crime and terrorism, and securing external borders, as well as improving digital security. The indicative budget available for projects in 2020 is €265 million. This includes a €20 million call for proposals on Artificial Intelligence which will support European law enforcement agencies scale up AI capacities, close their AI skills gap, and boost cooperation. Work under preparation under the new research framework programme Horizon Europe will support the implementation of the EU Security Union Strategy, as well as the border management and security dimension of the New Pact on Migration and Asylum, EU Disaster Risk Reduction policies and the EU Maritime Security Strategy[191].

---

[186] COM(2020) 581.

[187] System of advance cargo information used for early security risk assessment of all goods movements crossing the external border.

[188] Regulation 2019/1896.

[189] Regulation 2019/1157.

[190] The EU has allocated funding of around €91 million for projects enhancing the protection of infrastructures, including combined cyber and physical threats, improved and fast response to incidents, and better information sharing.

[191] Under Horizon Europe, Cluster 3 will support in particular the Commission policy priority 'Promoting our European way of life', as well as 'European Green Deal' and 'Europe fit for the digital age'.

EU-funded security research has also proven effective in fostering cooperation and supporting security practitioners during the COVID-19 pandemic.[192] Support includes tools for joint epidemiological and criminal risk and threat assessment and investigation.

In order to ensure the uptake of **innovative projects**, EU Agencies need to be integrated into the existing security research and innovation landscape. Following the October 2019 Justice and Home Affairs Council, EU agencies and the Commission's Joint Research Centre are currently setting up the **EU innovation hub for internal security**, based on their existing legal mandates, to serve as a collaborative network of their innovation labs. The hub will be a coordination mechanism to support the participating entities in the sharing of information and knowledge, the setting up of joint projects, and the dissemination of findings and technological solutions developed that are relevant for internal security[193].

The **European Cybersecurity Industrial, Technology and Research Competence Centre and the Network of National Coordination Centres** are Europe's response to support innovation and industrial policy in cybersecurity. They aim to strengthen European cybersecurity capacities, shield our economy and society from cyberattacks, maintain research excellence and reinforce EU competitiveness. Trilogues are currently ongoing.

4. Skills and awareness raising

Awareness of security issues and acquiring the skills to deal with potential threats are essential to build a more resilient society with better prepared enterprises, administrations and individuals. Also important is victims' access to their rights.

Law enforcement and justice professionals

The COVID-19-related restrictions heavily affected CEPOL, which was obliged to cancel all planned residential activities from March 2020. These special circumstances also caused a growing demand for online services; in the first four months of the year, the Agency recorded a 30% increase in virtual activities and 100% increase in online users. Among the priority trainings areas for 2019-2021[194] are the fight against illegal immigration, counter-terrorism, trafficking in human beings and cyber crime, and child sexual abuse. The Commission is currently preparing the evaluation of CEPOL to be completed by July 2021.

General public

The **#SaferInternet4EU campaign** was launched on Safer Internet Day 2018. The activities reached nearly 63 people in the EU in the last 2 years, and include awards, support to teachers and cyber-hygiene. The network of Safer Internet Centres provided more than 1,800 new resources covering topics such as fake news, cyberbullying, privacy concerns, grooming and cyber-hygiene.

October 2020 marked the EU's 8th European **Cybersecurity Month**, promoting online security in the EU. This year's campaign was designed to address security issues surrounding the digitalisation of everyday life, accelerated by the COVID-19 pandemic.

---

[192] Horizon 2020 actions supporting the pandemic response can be found at: https://www.researchgate.net/publication/341287556.

[193] On 21 February 2020, the Standing Committee on Operational Cooperation on Internal Security confirmed the mission statement, main features, tasks and governance of the EU innovation hub for internal Security.

[194] European Union Strategic Training Needs Assessment 2018-2021, EU-STNA report, CEPOL.

Encouraging people to 'Think Before U Click', the campaign highlighted different cybersecurity themes to help users identify and prepare for cyber threats. The 2021 European Cyber Security Challenge in Prague is under preparation.

A crucial tool to help victims of cybercrime is No More Ransom[195], a free decryption tool repository helping victims fight back without paying the hackers. Supported by Europol's Cybercrime Centre, it celebrated its fourth anniversary in July 2020 and since its launch has registered over 4.2 million visitors from 188 countries, stopping an estimated $632 million in ransom demands from ending up in criminals' pockets.

On 1 July 2020, the Commission presented the **European Skills Agenda**[196] for sustainable competitiveness, social fairness and resilience. It sets ambitious, quantitative objectives for improving existing skills training in new skills to be achieved within the next 5 years. It includes dedicated actions to increase the number of graduates in science, technology, engineering, arts and mathematics needed in cutting-edge areas such as cybersecurity. On 10 November 2020, the Commission launched the Pact for Skills during the fifth edition of the European Vocational Skills Week 2020. It promotes joint action to maximise the impact of investing in improving existing skills and training in new skills. Together with the Pact, the first European skills partnerships have been announced in three areas: automotive, microelectronics and aerospace and defence.

On 30 September 2020, the Commission adopted a set of policy strategies which will have an important impact on developing the EU's long term security skills capability. The **Digital Education Action Plan for 2021-2027**[197] will drive a high-performing digital education ecosystem with enhanced competences for the digital transformation[198]. A Communication on the **European Education Area** by 2025[199] was adopted on the same day, with basic and digital skills a key focus. A Communication on a new **European Research Area for Research and Innovation**[200] set out the path to improve Europe's research and innovation landscape and accelerate the EU's transition towards digital leadership as well as combatting gender-based violence, in all its forms, in Research and Innovation organisations.

The Erasmus+ programme also contribute to combatting radicalisation through projects combatting radicalisation, violent extremism, social inclusion, misinformation and fake news[201]. An example is the Radicalisation Prevention in Prisons Project aiming to enhancing the competences of frontline staff to identify, report and interpret signals of radicalisation and respond appropriately[202]. The No Hate BootCamp project helped youth workers to become "no hate speech ambassadors" in their local communities.

The Commission itself seeks to engage the public in reflections on EU security policy. Actions at EU level have been made more visible and accessible to citizens through the

[195] https://www.nomoreransom.org/.
[196] COM(2020)274.
[197] COM(2020)624.
[198] https://ec.europa.eu/education/sites/education/files/document-library-docs/deap-communication-sept2020_en.pdf.
[199] COM(2020) 625.
[200] COM(2020) 628.
[201] `So far, around 80 projects have been financed covering issues related to radicalisation; more than a hundred projects concerning how to prevent and combat cyber-bullying and more than a hundred around education for a critical and ethic use of Internet with a view to tacking online disinformation.
[202] http://www.r2pris.org/.

new **website on the EU Security Strategy**[203]. Several **public consultations** have been launched, giving citizens an opportunity to directly influence policy formation.

All victims of crime have rights to support and protection, but victims of the most severe crimes such as terrorism or sexual exploitation of children need specific attention. On 24 June 2020 the Commission adopted its first ever **EU Strategy on victims' rights (2020-2025)**[204]. This addresses victims of all crimes, but pays particular attention to the most vulnerable, including victims of terrorism, child victims of sexual exploitation, and victims of trafficking in human beings. On 22 September 2020, the Commission organised a high level Conference on victims' rights, during which it inaugurated the **Victims' Rights Platform**, to promote a more horizontal approach to victims' rights[205]. The Commission has also appointed its first ever **Coordinator for Victims' Rights**, to support consistency and effectiveness in victims' rights potlicy.

Regarding **victims of terrorism**, the EU Centre of expertise for victims of terrorism was set up in January 2020 to offer expertise, guidance and support to national authorities and victim support organisations. It promotes exchange of best practices and sharing of expertise among the practitioners and specialists across borders. It is not designed to offer direct help to particular victims of terrorism, but to support national structures in providing professional assistance and support, including guidelines to be published in 2020. The EU Centre is a pilot project that will last for two years. The Council Presidency is working on backing this up with a network of single national contact points on victims of terrorism.

VI CONCLUSION

The Security Union Strategy was put in place to provide a comprehensive and dynamic approach. The recent terrorist attacks have shown again how the EU needs to be able to react, strengthening our resilience and responsiveness by the modernisation and effective deployment of the key tools at our disposal. They have also shown the need for all actors to be fully engaged in a common approach, so that Member States, the EU institutions, the private sector, NGOs, and citizens themselves can all play a role in building a security base sufficiently strong and flexible to deliver. This coherent and consistent approach is also the best way to be sure that our fundamental rights are protected as part of promoting our European way of life.

This report shows the many workstreams under way, but also how the momentum must be maintained. The goal of the EU Counter-Terrorism Agenda presented today is to strengthen the European framework to counter terrorism by setting out the next steps needed: to anticipate and prevent terrorism, to protect citizens and infrastructure, and to be ready to respond, bearing in mind the internal-external security nexus. We already have more cooperation, more efforts to address radicalisation, more tools to deprive terrorists of means for an attack. Now this must be taken a step further. Emblematic of this is to ensure the adoption of new rules to address terrorist content online, where agreement this year is a

---

[203] https://ec.europa.eu/info/strategy/priorities-2019-2024/promoting-our-european-way-life/european-security-union-strategy_en.

[204] COM(2020) 258.

[205] The platform will bring together for the first time the main EU level actors including the European Network on Victims' Rights, the EU Network of national contact points for compensation, the EU Counterterrorism Coordinator, relevant agencies such as Eurojust, the Fundamental Rights Agency, the European Union Agency for Law Enforcement Training, the European Institute for Gender Equality, and civil society.

major priority. The Commission also urges Member States to accelerate the implementation of all agreed legislation. Ensuring the security of EU citizens is a common responsibility, and taking forward common action must be the collective ambition for a more secure Europe.

EUROPEAN
COMMISSION

Brussels, 9.12.2020
COM(2020) 797 final

ANNEX 1

ANNEX

to the

COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT AND THE COUNCIL

First Progress Report on the EU Security Union Strategy

Status of implementation of legislation on security

I. List of Directives and Framework Decisions where infringement procedures are ongoing

- **Prüm framework**[1]: ongoing infringement procedures against 2 Member States.
- **Framework Decision on accreditation of forensic services**[2]**:** ongoing infringement procedures against 2 Member States.
- **Directive on combating child sexual abuse**[3] (transposition deadline: 18.12.2013). Infringement procedures ongoing against 25 Member States.
- **Directive on attacks against information systems**[4] (transposition deadline: 4.09.2015). Infringement procedures ongoing against 4 Member States.
- **Freezing and confiscation Directive**[5] (transposition deadline: 04.10.2016). Infringements ongoing against 3 Member States.
- **Market Abuse Directive**[6] (transposition deadline: 03.07.16). Infringement procedures ongoing against 5 Member States.
- **4th Anti-Money laundering Directive**[7] (transposition deadline 16.06.2017), infringement procedures ongoing against 7 Member States.
- **Data Protection Law Enforcement Directive** (LED) [8] (transposition deadline 06.05.2018), infringements procedures ongoing against 3 Member States.
- **EU Passenger Name Record Directive**[9] (transposition deadline on 25.05.2018) Infringement procedure ongoing against 1 Member State.
- **Directive on the control of the acquisition and possession of weapons**[10] (Firearms Directive) (transposition deadline: 14.09.2018). Infringement procedures ongoing against 25 Member States and the UK.
- **Legislative package on new psychoactive substances (NPS)**[11] (transposition deadline 23.11.2018). Infringement procedure for Directive (EU) 2017/2103 ongoing

---

1 Council Decision 2008/615/JHA of 23 June 2008 on the stepping up of cross-border cooperation, particularly in combating terrorism and cross-border crime and Council Decision 2008/616/JHA of 23 June 2008 on the implementation of Decision 2008/615/JHA on the stepping up of cross-border cooperation, particularly in combating terrorism and cross-border crime.

2 Council Framework Decision 2009/905/JHA of 30 November 2009 on Accreditation of forensic service providers carrying out laboratory activities.

3 Directive 2011/93/EU of 13 December 2011 on combating the sexual abuse and sexual exploitation of children and child pornography, and replacing Council Framework Decision 2004/68/JHA.

4 Directive 2013/40/EU of 12 August 2013 on attacks against information systems and replacing Council Framework Decision 2005/222/JHA.

5 Directive 2014/42/EU of 3 April 2014 on the freezing and confiscation of instrumentalities and proceeds of crime in the European Union.

6 Directive 2014/57/EU of the European Parliament and of the Council of 16 April 2014 on criminal sanctions for market abuse (market abuse directive).

7 Directive (EU) 2015/849 of 20 May 2015 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, amending Regulation (EU) No 648/2012, and repealing Directive 2005/60/EC and Commission Directive 2006/70/EC.

8 Directive (EU) 2016/680 of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent 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.

9 Directive (EU) 2016/681 of 27 April 2016 on the use of passenger name record (PNR) data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime.

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

against 5 Member States and for Delegated Directive (EU) 2019/369 against 1 Member State.

- **Directive on the fight against fraud to the Union's financial interests** by means of criminal law[12] (transposition deadline: 06.07.2019). Infringement procedures ongoing against 3 Member States.
- **5th Anti-Money laundering Directive**[13] (transposition deadline 10.01.2020); infringement procedures ongoing against 16 Member States.
- **Implementing Directive establishing technical specifications for the marking of firearms**[14] (transposition deadline: 17.01.2020) infringement procedure ongoing against 18 Member States and the United Kingdom.
- **Implementing Directive on technical specifications for alarm and signal weapons**[15] (transposition deadline: 17.01.2020). Infringement procedures are ongoing for 16 Member States and the UK.
- Council framework Decision 2009/905/JHA of 30 November 2009 on **Accreditation of forensic service providers carrying out laboratory activities** (transposition deadline with regard to DNA data 30.11.2013, and dactyloscopic data 30.11.2015). Infringement procedures are ongoing for 2 Member States.
- **Directive concerning measures for a high common level of security of networks and information systems across the Union (NIS Directive)**[16] (transposition deadline: 09.05.2018). Infringement procedure ongoing against 3 Member States.
- **Victims' Rights Directive**[17] (transposition deadline: 16.11.2015). Infringement procedure ongoing against 12 Member States.
- **Framework Decision on European Arrest Warrant**[18] (transposition deadline: 31.12.2003). Infringement procedure ongoing against 7 Member States.
- **Framework Decision on custodial sentences**[19] (transposition deadline: 5.12.2011). Infringement procedure ongoing against 1 Member State.

---

[11] Directive (EU) 2017/2103 of 15 November 2017 amending Council Framework Decision 2004/757/JHA in order to include new psychoactive substances in the definition of 'drug' and repealing Council Decision 2005/387/JHA; Commission Delegated Directive (EU) 2019/369 of 13 December 2018 amending the Annex to Council Framework Decision 2004/757/JHA as regards the inclusion of new psychoactive substances in the definition of 'drug'.

[12] Directive (EU) 2017/1371 of 5 July 2017 on the fight against fraud to the Union's financial interests by means of criminal law.

[13] Directive (EU) 2018/843 of 30 May 2018 amending Directive (EU) 2015/849 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, and amending Directives 2009/138/EC and 2013/36/EU.

[14] Commission Implementing Directive (EU) 2019/68 of 16 January 2019 establishing technical specifications for the marking of firearms and their essential components under Council Directive 91/477/EEC on control of the acquisition and possession of weapons.

[15] Commission Implementing Directive (EU) 2019/69 of 16 January 2019 laying down technical specifications for alarm and signal weapons under Council Directive 91/477/EEC on control of the acquisition and possession of weapons.

[16] Directive (EU) 2016/1148 of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union.

[17] Directive 2012/29/EU of 25 October 2012 establishing minimum standards for the rights, support and protection of victims of crime.

[18] Council Framework Decision of 13 June 2002 on the European arrest warrant and the surrender procedures between Member States.

[19] Council Framework Decision 2008/909/JHA of 27 November 2008 on the application of the principle of mutual recognition to judgments in criminal matters imposing custodial sentences or measures involving deprivation of liberty for the purpose of their enforcement in the European Union.

- **Framework Decision on financial penalties**[20] (transposition deadline: 22.3.2007). Infringement procedure ongoing against 1 Member State.
- **Framework Decision on supervision measures**[21] (transposition deadline: 1.12.2012). Infringement procedure ongoing against 1 Member State.
- **Revised Audiovisual Media Services Directive** (transposition deadline: 19.09.2020). Infringement procedures launched against 23 Member States.

II. List of Directives to be transposed before end 2020 and in 2021

- Directive on **combating money laundering**[22] (transposition deadline: December 2020).
- Directive facilitating the **use of financial and other information for the prevention, detection, investigation or prosecution of certain criminal offences**[23] (transposition deadline: 01.08.2021).
- Directive on **combating fraud and counterfeiting of non-cash means of payment** [24] (transposition deadline: May 2021).

III. List of legislations that still need to be approved by the co-legislators

- **Regulation on terrorist content on line**[25]: trilogues ongoing
- **European Cybersecurity Industrial, Technology and Research Competence Centre and the Network of National Coordination Centres**[26]: trilogues ongoing
- **Visa Information System (VIS)**[27] **:** provisional agreement found on 8 December 2020**.**
- **Consequential amendments on the European Travel Information and Authorisation System (ETIAS) regulation**[28] : Council adopted its position in May 2019, waiting for the European Parliament to adopt its position.

---

[20] Council Framework Decision 2005/214/JHA of 24 February 2005 on the application of the principle of mutual recognition to financial penalties.

[21] Council Framework Decision 2009/829/JHA of 23 October 2009 on the application, between Member States of the European Union, of the principle of mutual recognition to decisions on supervision measures as an alternative to provisional detention.

[22] Directive (EU) 2018/1673 of 23 October 2018 on combating money laundering by criminal law.

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

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

[25] Proposal for a Regulation on preventing the dissemination of terrorist content online, COM(2018) 640 final, 12 September 2018.

[26] Proposal for a Regulation establishing the European Cybersecurity Industrial, Technology and Research Competence Centre and the Network of National Coordination Centres, COM(2018) 630 final, 12 September 2018.

[27] Proposal for a Regulation amending Regulation (EC) No 767/2008, Regulation (EC) No 810/2009, Regulation (EU) 2017/2226, Regulation (EU) 2016/399, Regulation XX/2018 [Interoperability Regulation], and Decision 2004/512/EC and repealing Council Decision 2008/633/JHA, COM (2018), 302 final, 16 May 2018.

[28] Regulation (EU) 2018/1240 of 12 September 2018 establishing a European Travel Information and Authorisation System (ETIAS) and amending Regulations (EU) No 1077/2011, (EU) No 515/2014, (EU) 2016/399, (EU) 2016/1624 and (EU) 2017/2226; and Regulation (EU) 2018/1241 of 12 September 2018

- **Regulation on cross-border access to e-evidence**[29] and **Directive on harmonised rules on the appointment of legal representatives for the purpose of gathering evidence in criminal proceedings**[30]: Council adopted its positions, waiting for the European Parliament to adopt its position.
- **Interim regulation on child sexual abuse on line**[31]: Council adopted its position, waiting for the European Parliament to adopt its position.
- **Regulation on the Space Programme of the Union**[32]**:** trilogues ongoing.
- **European Defence Fund**[33]**:** trilogues ongoing.

amending Regulation (EU) 2016/794 for the purpose of establishing a European Travel Information and Authorisation System (ETIAS).

29 Proposal for a Regulation on European Production and Preservation Orders for electronic evidence in criminal matters, COM/2018/225 final, 17 April 2018.

30 Proposal for a Directive laying down harmonised rules on the appointment of legal representatives for the purpose of gathering evidence in criminal proceedings, COM/2018/226, 17 April 2018

31 Proposal for a Regulation on a temporary derogation from certain provisions of Directive 2002/58/EC 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 September 2020.

32 Proposal for a Regulation establishing the space programme of the Union and the European Union Agency for the Space Programme COM(2018) 447 final, 6 June 2018.

33 Proposal for a Regulation establishing the European Defence Fund, COM(2018) 476 final, 13 June 2018.

EUROPEAN
COMMISSION

Brussels, 9.12.2020
COM(2020) 797 final

ANNEX 2

ANNEX

to the

COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT AND THE COUNCIL

First Progress Report on the EU Security Union Strategy

Implementation Roadmap

Actions	State of Play
I. A future-proof security environment (critical infrastructure, cybersecurity, public spaces)	
• Proposal for a Directive on the resilience of critical entities	• To be adopted by Commission in December 2020
• Review of NIS Directive	• To be adopted by Commission in December 2020
• Cross-sectoral financial services act on operational and cyber resilience	• Adopted by Commission on 23.09.2020
• Resilience of critical energy infrastructure	• Ongoing consultation of relevant energy operators and Member States
• Network code on cybersecurity for cross-border electricity flows	• COM adoption planned 2022
• A European Cybersecurity Strategy	• To be adopted by Commission in December 2020
• Amendment to EU judicial cooperation instruments in view of their digitalisation	• COM adoption plan Q4 2021
• Creation of a Joint Cyber Unit	• Cybersecurity Strategy to be adopted December 2020
• Common rules on information security and cybersecurity for EU institutions, bodies and agencies	• COM adoption planned Q4 2021
• Step up cooperation for the protection of public spaces, including spaces of worship	• Counter-Terrorism Agenda for the EU, to be adopted on 9 December 2020
• Sharing of best practices on addressing misuse of drones	• Ongoing
II. Tackling evolving threats (Cybercrime, modern law enforcement, illegal content online, hybrid threats)	
• Ensure full and fit-for purpose implementation of legislation on cybercrime (Directive 2013/40/EU)	• Infringement proceedings and preparations for additional proceedings are ongoing

• Enhance law enforcement / judiciary capacity in digital investigations	• Digital Capacity Building action plan for law enforcement in preparation, to be adopted in 2021
• EU Strategy for fight against child sexual abuse	• Adopted by Commission on 24.07.2020
• Proposals on detection and removal of child sexual abuse	• Short term proposal: Adopted by Commission on 10.09.2020 • Long term proposal: Work ongoing – adoption planned for Q2 2020
• Set out an EU approach to countering hybrid threats: mainstream considerations on hybrid into policy making	
• Review of EU operational protocol for countering hybrid threats (EU Playbook) SWD(2016)227	
• Legislative proposal on the digitalisation of crossborder judicial cooperation (see Commission work programme for 2021)	To be adopted by the Commission in Q4 2021
III. Protecting Europeans from terrorism and organised crime	
• A Counter-Terrorism Agenda for the EU	• Adopted by Commission on 9.12.2020
• Negotiations with third countries for cooperation with Europol	• Negotiations with Turkey are ongoing. On 13 May 2020, the Council authorised the opening of negotiations with New Zealand.
• Opening of negotiations with 10 third countries for cooperation between the latter and Eurojust	• Recommendation for the adoption of a Council Decision on authorising the negotiations with 10 third countries was sent to the Council on 19 November 2020, awaiting authorisation.
• European Public Prosecutor's Office (EPPO): Recommendation on cooperation agreements with selected third countries	• Recommendation for the adoption of a Council Decision authorising the negotiations for the conclusion of cooperation agreements between the EPPO and selected third countries. • Adoption planned for Q2 2021

• An Agenda on tackling organised crime, including trafficking in human beings	• Targeted consultations took place • Adoption planned for Q1 2021
• EU Agenda on Drugs and Action Plan 2021-2025	• Adopted by Commission on 24.07.2020
• Revision of the mandate of the European Monitoring Centre for Drugs and Drug Addiction	• Inception impact assessment published and feed-back period closed on 31. 07. 2020 • Adoption planned for Q1 2021
• 2020-2025 EU Action Plan on Firearms trafficking	• Adopted by Commission on 24.07.2020
• Commission report on the application of the Firearms Directive	• Adoption planned for Q1 2021
• Review of the Regulation on export authorisation, and import and transit measures for firearms	• Adoption planned for Q4 2021
• Review of Directive on freezing and confiscation of proceeds of crime	• Adoption planned for Q4 2021
• Proposal for a Directive on Asset Recovery Offices	• Adoption planned for Q3 2021
• Review of the Environmental Crime Directive 99/2008/EC	• Adoption of a proposal planned for Q4 2021
• An EU Action Plan against Migrant Smuggling, 2021-2025	• Consultations ongoing • Adoption planned for Q2 2021
IV. A strong European security ecosystem	
• Strengthening the Europol mandate	• Adopted by Commission on 09.12.2020
• Revision of the Prüm decisions	• Adoption planned for Q2 2021
• An EU 'Police Cooperation Code' and police coordination in times of crisis	• Adoption planned for Q4 2021
• Revision of the Advance Passenger Information Directive	• Adoption planned for Q2 2021
• Digital information exchange on cross-border terrorism cases	• Adoption planned for Q4 2021
• IT collaboration platform for Joint Investigation Teams	• Adoption planned for Q4 2021
• Communication on the external dimension of Passenger Name Records	• Roadmap published on 24.07.2020 • Adoption planned for Q1 2021
• Strengthening cooperation between the EU and Interpol	• Adoption planned for Q1 2021
• A framework to negotiate with key third countries on sharing of information	• Adoption planned for Q2 2022

• Better security standards for identity cards and residence documents (implementation of regulation 2019/1157)	• Ongoing (Member States will start issuing identity cards and residence documents according to tighter security standards as of August 2021)
• European Innovation hub for internal security	• Report planned for Q4 2020
• Strengthening and improving of the exchange of criminal records information (ECRIS and ECRIS-TCN)	• Adoption of the Report on the functioning of ECRIS planned for Q4 2020/ Q1 2021 • Adoption of the implementing acts for ECRIS-TCN planned for 2021.
• European Cybersecurity Industrial, Technology and Research Competence Centre and Network of National Coordination Centres proposal Regulation	• Ongoing negotiations (subject to conclusion of negotiations and adoption of Regulation)