Council of the European Union

Brussels, 16 December 2022
(OR. en)

16124/22

JAI 1695	**DROIPEN 165**
COSI 328	**COPEN 450**
ENFOPOL 648	**FREMP 275**
ENFOCUSTOM 179	**JAIEX 106**
IXIM 298	**CFSP/PESC 1733**
CT 227	**COPS 616**
CRIMORG 184	**HYBRID 120**
FRONT 464	**DISINFO 112**
ASIM 108	**TELECOM 528**
VISA 203	**DIGIT 248**
CYBER 409	**COMPET 1045**
DATAPROTECT 369	**RECH 665**
CATS 74	**CULT 133**

COVER NOTE

From:	Secretary-General of the European Commission, signed by Ms Martine DEPREZ, Director
date of receipt:	13 December 2022
To:	Ms Thérèse BLANCHET, Secretary-General of the Council of the European Union
No. Cion doc.:	COM(2022) 745 final
Subject:	COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT AND THE COUNCIL on the Fifth Progress Report on the implementation of the EU Security Union Strategy

Delegations will find attached document COM(2022) 745 final.

Encl.: COM(2022) 745 final

EUROPEAN
COMMISSION

Brussels, 13.12.2022
COM(2022) 745 final

COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT AND THE COUNCIL

on the Fifth Progress Report on the implementation of the EU Security Union Strategy

1. INTRODUCTION

In July 2020, the Commission adopted the comprehensive Security Union Strategy[1]. Since then, the threat environment has evolved in very significant ways. The COVID-19 crisis accentuated some vulnerabilities, particularly with activity pushed online. Cybersecurity attacks have continued to increase in scale and spread to new forms of attack[2]. The impact of the war of aggression of Russia against Ukraine has been felt on EU internal security, with an increased risk of trafficking in human beings, the threat of chemical and nuclear incidents, and of illicit circulation of firearms. It has also spurred the use of foreign information manipulation and interference. The recent sabotage of the Nord Stream pipelines has underlined how essential sectors such as energy, digital infrastructure, transport and space depend on resilient critical infrastructure. It has shown again how both physical and digital security are closely intertwined and must be protected in tandem.

This Security Union Progress Report aims to give a "mid-term" overview of the implementation of the Strategy, highlighting what has been achieved, and what still needs to be done, by the end of this Commission's mandate. Since July 2020, the EU has taken great strides towards completing the actions in the key areas covered by the four pillars of the Strategy[3]. This report shows that the overwhelming majority of the actions itemised in the Strategy have been addressed[4]. However, work remains to be done to achieve the full impact of the Security Union Strategy for citizens – in particular, the adoption of outstanding legislative proposals by the European Parliament and the Council and the implementation by Member States of agreed legislation. The goals of the Security Union can also be best secured through close collaboration with linked EU initiatives in areas like energy security, the European Health Union, and the European Democracy Action Plan. The Commission's continuing contribution includes three proposals adopted alongside this report, the trafficking of cultural goods, the essential intelligence offered by Advance Passenger Information[5] as well as a proposal to tackle human trafficking[6].

2. PROTECTING PHYSICAL AND DIGITAL INFRASTRUCTURE FROM PHYSICAL, CYBER AND HYBRID ATTACK

Protecting critical infrastructure in the EU against physical and digital attacks

Even before the recent attacks on critical infrastructure, the EU was building its resilience through two linked initiatives: the revised Directive[7] on measures for high common level of cybersecurity across the Union **(Network Infrastructure Security – 'NIS2 Directive')[8],** and a new Directive on the resilience of critical entities **(Resilience of Critical Entities – 'CER**

1 COM(2020) 605.
2 ENISA Threat landscape 2022.
3 1) a future proof security environment, (2) tackling evolving threats (3), protecting Europeans from terrorism and organised crime, (4) A strong European Security Ecosystem.
4 A table in annex provides an overview of legislative and non-legislative actions since the launch of the Security Union Strategy.
5 An Action Plan on trafficking of cultural goods (COM(2022) 800 and two proposals on the revision of the Advance Passenger Information Directive (COM(2022) 729 and 731).
6 A proposal for a revised Anti-trafficking Directive (COM(2022) 732) and the 4th progress report on trafficking in human beings are foreseen for adoption on 19 December 2022.
7 Proposal to revise Directive (EU) 2016/1148.
8 COM(2020) 823.

Directive')[9]. Together, this framework addresses current and future online and offline risks, from cyberattacks to natural disasters. These Directives have been agreed by the co-legislators and will enter into force in the coming weeks. The **NIS2 Directive** will increase the coverage for medium and large entities in a range of key sectors[10]. It strengthens security requirements including for incident response and crisis management, supply chain security, vulnerability handling and disclosure, cybersecurity testing, and the effective use of encryption. It also streamlines incident-reporting obligations, introduces more stringent supervisory measures and aims to harmonise sanctions regimes across Member States[11]. The **CER Directive** covers the physical resilience of critical entities against both man-made and natural hazards. Covering 11 sectors, the Directive is a major step to improving the ability of critical entities providing essential services to prevent, protect against, respond to, resist, mitigate, absorb, accommodate and recover from an incident.

In the **financial** sector, the Digital Operational Resilience Act (DORA) has also been adopted[12], as part of the Digital Finance package. Once implemented, DORA will strengthen the digital operational resilience of EU financial sector entities by streamlining and upgrading existing rules, introducing new requirements where necessary.

To further increase the protection of **critical infrastructure against large scale cyberattacks**, the Commission, the High Representative and the NIS Cooperation Group[13] are developing **risk scenarios,** focusing on cybersecurity in the energy, telecoms, transport sectors and space. Work is also ongoing regarding measures to improve the collective level of protection and cyber resilience of space systems and services[14]. Targeted cybersecurity risk assessments for communications infrastructure and networks in the EU (including fixed and mobile infrastructure, satellite, undersea cables, and internet routing) are also under way[15]. The Commission has also initiated a scenario-building initiative covering **natural disasters linked to security-related threats** like cyberattacks or terrorism, to improve disaster prevention, preparedness and response.

The sabotage of the Nord Stream gas pipelines and other recent incidents underlined the threat to **EU critical infrastructure** and the urgency for action. The framework of the CER Directive and the NIS2 Directive is therefore being foreshadowed, to accelerate action to strengthen the resilience of critical infrastructure and enhance preparedness and response in key sectors. This is being brought together in a **Council Recommendation**[16] which will allow the effective implementation of the Directives to be accelerated. It offers a common approach to conducting **stress tests** on entities operating critical infrastructure, starting in the energy

---

9 COM(2020) 829.

10 The following sectors are covered by the NIS2 and CER Directive: energy, transport, banking, financial market infrastructure, digital infrastructure, health, drinking water, wastewater, public administration, space and food production, processing and distribution.

11 Discussions are under way amongst national experts in the NIS Cooperation Group to support Member States in transposition and implementation of the NIS2 Directive.

12 COM (2020) 595. Political agreement reached in May 2022.

13 The group is made up of representatives of the Member States, the Commission and the European Union Agency for Cybersecurity (ENISA), to support and facilitate strategic cooperation between the Member States on security of network and information systems.

14 Council conclusions on the development of the European Union's cyber posture, 23 May 2022.

15 In line with the Nevers Call to Reinforce the EU's Cybersecurity Capabilities agreed during the Informal Meeting of the Telecommunications Ministers on 9 March 2022.

16 The Commission proposal COM(2022) 551 was followed by adoption of a Council recommendation on 8 December 2022.

sector, drawing on agreed common principles. Work on stress tests will start immediately so that these can be completed before the end of 2023, with progress to be looked at in April 2023. A Blueprint, to be prepared by the Commission in cooperation with the Council, building on the support and contributions of relevant Union agencies, will help ensure a coordinated response at EU level to significant disruptions of critical infrastructure.

In the **energy sector**, the Commission is working on a network code on cybersecurity for cross-border electricity flows[17], including rules on risk assessments, common minimum requirements, planning, monitoring, reporting and crisis management which will be fully coherent with the NIS2 framework. In a separate action responding to Russia's aggression against Ukraine, the electricity grids of Ukraine and the Republic of Moldova were synchronized with the Continental Europe Grid in March 2022, complementing risk mitigating measures, including for cybersecurity.

In the **transport sector**, the Commission works with Member States, the European Union Aviation Safety Agency (EASA) and EU Intelligence and Situation Centre (EU INTCEN) to regularly assess the level of threat and risk to EU civil aviation from conflict zones. The EU Conflict Zone Alerting System is referenced as a best practice at the international level[18]. Actions include relaunching an air cargo risk assessment workstream, a first risk assessment at EU level to assess threats to passenger ships, and a comprehensive aviation security risk-mapping exercise to update the assessment of threats to civil aviation.

Maritime critical infrastructure is also the subject of dedicated attention[19]. The Common Information Sharing Environment for the maritime domain is currently being developed and will be fully operational by the end of 2023, interconnecting maritime surveillance authorities on a voluntary basis, to exchange near-real time information. The European Coast Guard Functions Forum has also strengthened its capacity to guard against cyberattacks.

Several research projects under **Horizon Europe** also seek to make our digital infrastructure safer and build capacity to prevent and mitigate cyberattacks[20].

Enhancing the EU's cybersecurity

On 16 December 2020, the Commission and the High Representative presented a new **EU Cybersecurity Strategy for the Digital Decade[21],** to bolster Europe's collective resilience against cyber threats and ensure that citizens and businesses benefit from reliable, trustworthy services and digital tools. The Strategy has been almost fully implemented.

The NIS2 Directive foresees the establishment of the **European Cyber Crises Liaison Organisation Network (EU-CyCLONe)**[22] to support the coordinated management of large-scale cybersecurity incidents and crises at operational level. This will ensure a regular

---

17 This is required by the Electricity Regulation (EU) 2019/943.

18 International Civil Aviation Organisation (Doc 10084 entitled "Risk Assessment Manual for Civil aircraft Operations Over or Near Conflict Zones" 2018).

19 Including through the implementation of PESCO capability projects and Horizon 2020 projects.

20 EU-CIP, for a European Knowledge Hub and Policy Testbed for Critical Infrastructure Protection and ATLANTIS - The Atlantic Testing Platform for Maritime Robotics: New Frontiers for Inspection and Maintenance of Offshore Energy Infrastructures.

21 JOIN(2020) 18.

22 EU-CyCLONe is composed of the representatives of Member States' cyber crisis management authorities with the participation of the Commission in cases where a potential or ongoing large-scale cybersecurity incident has or is likely to have significant impacts on services and activities foreseen in the directive.

exchange of relevant information among Member States and EU institutions, bodies, offices and agencies. The Commission is developing a **cybersecurity situation and analysis centre** to boost its internal capacity. The Commission is working with Member States including through follow up to its Recommendation on a **Joint Cyber Unit**[23] to ensure an EU coordinated response to large scale cyber incidents. The Commission and the High Representative are also actively involved in cyber exercises in 2022 organised with Member States[24].

Networks and computer systems require constant monitoring and analysis to detect intrusions and anomalies in real time. The Commission has proposed to build a network of **Security Operations Centres** (SOCs) across the EU, to monitor communications networks and identify suspicious events. By scaling up existing SOCs, establishing new centres, and by linking SOCs across several Member States, collective detection capabilities will be stepped up. These could also draw on the latest artificial intelligence (AI) and data analytics, protecting civilian communication networks and speeding up detection of cyberattacks.[25]

To reinforce preparedness and response to major cyber incidents, the Commission has also set up a short-term programme to support Member States, through additional funding allocated to ENISA, including penetration testing of critical entities to identify vulnerabilities. This can also assist Member States with incident response, provided by ENISA with the support of trusted private cybersecurity service providers, after a major incident affecting critical entities. The next step will be to ensure that Member States make full use of these opportunities.

Both hardware and software products are increasingly subject to **cyberattacks**. Cyberattacks are growing in numbers and sophistication with the exploitation of software vulnerabilities being the key vector. Two-thirds of all incidents reported under NIS involve the exploitation of software vulnerabilities. The impact on citizens, infrastructure, or companies is also growing[26]. Two-thirds of all incidents reported under NIS involve the exploitation of software vulnerabilities. In September 2022, the Commission proposed the **Cyber Resilience Act**[27]**,** to reduce vulnerabilities in products with digital elements, and ensure that patches and mitigating measures are made swiftly available. It proposes that products with digital elements (hardware and software) should only enter the market if they meet specific essential cybersecurity requirements[28]. Manufacturers and developers would be required to ensure the cybersecurity of their products for five years and to be transparent with consumers about cybersecurity. This will make a significant contribution to the security of the supply chain[29].

Certification plays a crucial role in increasing trust and security in important products and services for the digital world. The Cybersecurity Act[30] sets up the European Cybersecurity

---

23 COM (2021) 4520.

24 Examples include the Blueprint Operational Level Exercise (Blue OLEx) organied by Lithuania and ENISA, and the EU Cyber Crisis Linking Exercise on Solidarity (EU CyCLES) organised by French Presidency.

25 A first phase was launched with a call for proposals on "Capacity Building of Security Operation Centres", and a Call for Expression of Interest to engage in a joint procurement of tools and infrastructures", with the ECCC, with €110 million EU funding in total from the DIGITAL program, published in November 2022.

26 ENISA Threat landscape 2022.

27 COM(2022) 454.

28 In the meantime, the Commission adopted in October 2021 a delegated regulation under the Radio Equipment Directive which imposes obligations on the manufacturers of wireless devices to improve their level of cybersecurity, privacy and protection from fraud.

29 In line with Council conclusions on ICT supply chain security, 17 October 2022.

30 Regulation 2018/881, introducing an EU-wide cybersecurity certification framework for ICT products,

Certification Framework under which the Commission can ask ENISA to develop certification schemes. A European Common Criteria-based cybersecurity certification scheme has been developed and schemes for cloud services and 5G security are under preparation.

The Commission continues to work with Member States to ensure that **5G networks** are secure and resilient, and to monitor implementation of the EU 5G Toolbox at national and EU level. While a vast majority of Member States have already reinforced or are in the process of reinforcing security requirements for 5G networks, it is now urgent that all Member States complete implementation of the Toolbox measures[31] in particular that the Member States enact restrictions on high-risk suppliers, considering that a loss of time can increase vulnerability of networks in the Union, and also reinforce physical and non-physical protection of critical and sensitive parts of 5G networks, including through strict access controls.

To help the EU and Member States take a proactive, strategic approach to cybersecurity industrial policy, the **European Cybersecurity Competence Centre** will work with National Coordination Centres to support innovation in cybersecurity and strengthen the capacities of the cybersecurity technology community.[32]

In September 2022, ENISA formally launched a **European framework for cybersecurity skills** that identifies the most necessary job profiles in the field and provides a common European basis for facilitating skills recognition and developing cybersecurity-related training. This framework will be a building block for the **Cybersecurity Skills Academy** proposed under the Commission Work Programme 2023, which will offer a comprehensive approach to address the growing need for cybersecurity professionals in Europe.

Given the sensitive non-classified and EU classified information handled by **EU institutions, bodies, offices and agencies (EUIBA)**, it is important that these are well protected against cyberattacks. The Commission proposed in March 2022 a Regulation for a high common level of cybersecurity across these bodies[33], applying the principles underlying the NIS2 Directive to the EU institutional environment. It includes a new Inter-institutional Cybersecurity Board and a reinforced cybersecurity centre (CERT-EU)[34] to ensure appropriate information exchange and cooperation with Member State authorities, for example through the network of Cyber Security Incident Response Teams (CSIRTs). In parallel, the Commission has adopted a proposal for a Regulation on information security in the EUIBA,[35] to enhance resilience against cyber and hybrid threats by creating a common set of high-level information security standards for all institutions, bodies, offices and agencies of the Union. It is essential that the Council accelerates its work on this proposal, considering the multiple calls from Member States requesting the Commission to work on measures to better protect the EU decision-making process from malicious activities of all kinds. CERT-EU and

---

services and processes.

31 Member States, with the support of the Commission and ENISA, published earlier this year a report on the cybersecurity of Open Radio Access Networks, which, when more mature, will provide an alternative way of deploying the radio access part of 5G networks based on open interfaces.

32 The Governing Board of the ECCC is in place and hold its 4th meeting on 20 October 2022.

33 COM(2022) 122.

34 CERT-EU has also significantly invested in further improving its existing services to EUIBAs and in adding new ones, to better prevent, detect and respond to cyberattacks.

35 COM(2022) 119.

ENISA have also designed and tested a new type of cyber exercise that is tailored to EU agencies, as recommended by the European Court of Auditors.

Key delivery examples

The European Cybersecurity Month (ECSM): Including workshops, social media campaigns, and lectures, the ECSM initiative has grown from 184 activities in 2014, to 500 activities in October 2022. These help improve users' response online, when faced with a cybersecurity threat (as reported by 73% of the Members States surveyed in 2021).

The Cybersecurity Higher Education Database (CyberHEAD): CyberHEAD has been the most highly visited webpage of ENISA for the past 2 years, with around 70 000 visits a year. It allows young talents to make informed decisions on the variety of possibilities offered by higher education in cybersecurity and helps universities attract high-quality students motivated in keeping Europe cyber-secure.

Countering hybrid threats, fighting foreign interference and enhancing EU cyber defence

The **EU Strategic Compass** for Security and Defence outlines an ambitious plan of action to increase the EU's capacity to act, strengthen resilience and invest better in the EU's defence capabilities.

Whilst countering **hybrid threats** is predominantly a Member States' responsibility, the EU complements national action by supporting coordination, enhancing situational awareness, promoting cooperation with like-minded countries and international organisations, and providing joint response options. Over the past decade, more than 200 measures have been put in place to enhance resilience and counter hybrid threats at EU level. The EU INTCEN Hybrid Fusion Cell contributes to EU decision-making and is the central body for providing comprehensive situational awareness and strategic foresight, aggregating all-source information and conducting intelligence assessments on hybrid threats. Work has started to create EU Hybrid Rapid Response Teams, announced by the Strategic Compass, to support Member States, and Common Security and Defence Policy missions and operations, as well as partner countries, in countering hybrid threats by drawing upon relevant national and EU expertise at short notice, including military expertise as necessary. An EU hybrid toolbox is in preparation and will provide a framework for a coordinated response to hybrid campaigns affecting the EU and Member States integrating the external and internal dimension in a seamless flow and bringing the national and EU-wide considerations together. Significant progress has also been made on enhancing resilience and countering hybrid threats through the identification of existing sectoral resilience baselines.[36] The Commission has also continued analytical research on building resilience against hybrid threats[37] and completed the mainstreaming of hybrid considerations into policy making.

The COVID-19 pandemic and Russia's war against Ukraine have shown how the manipulation of the information environment can impact on the EU and partners around the globe. Aimed at corroding trust in the EU and in the international rules-based order, **foreign information manipulation and interference (FIMI)** is also an increasingly important component in hybrid attacks. Building on the European Democracy Action Plan, the Commission has put in place a set of tangible measures and structures, including the revised Code of Practice on Disinformation, the Digital Services Act, and the proposal on

[36] SWD(2022) 21.

[37] Hybrid threats: a comprehensive resilience ecosystem, JRC130097.

transparency of political advertising currently in inter-institutional negotiations, to tackle information manipulation and disinformation. The result would be new obligations on platforms and for the first time a legally binding oversight framework. In addition, as announced by the Strategic Compass, in close cooperation with the Commission and the Member States, the EEAS is further developing the **EU's Toolbox to tackle Foreign Information Manipulation and Interference** (FIMI Toolbox), to boost a coordinated response to manipulative behaviour by foreign actors.[38] The EEAS has also continued to strengthen cooperation with international partners like the G7 Rapid Response Mechanism (RRM) and NATO.

The Commission condemns any foreign interference on the sovereign territory of EU Member States and is concerned at reports of Chinese Overseas Police Service Stations in the EU, which, if true, would be completely unacceptable. Although it is for Member States authorities to investigate these allegations, the Commission, with the support of Europol, stands ready to facilitate exchange between Member States. The Commission raised this issue at the Justice and Home Affairs Council in December 2022.

In November 2022, the Commission and the High Representative presented a new EU Policy on **Cyber Defence,**[39] setting out means to enhance cooperation and investments in cyber defence to better protect, against cyberattacks. The objective is to defend EU interests in cyberspace by increased cooperation among EU's cyber defence actors, developing mechanisms for leveraging capabilities at the EU level, including in the context of CSDP missions and operations. It will boost development of full spectrum cyber defence capabilities and strengthen cooperation between the EU military and civilian cyber communities, enhancing situational awareness, crisis coordination and training, including with the private sector. It will also help reduce strategic dependencies in critical cyber technologies, through the development of a strategic roadmap for critical cybersecurity and cyber defence technologies, and strengthen the European Defence Technological Industrial Base.

The Strategic Compass identifies **space** as a fifth operational domain of warfare (alongside land, sea, air and cyber) and requests the Commission and the High Representative to develop the first Space Strategy for Security and Defence. The Strategy will propose measures to improve the collective level of protection and resilience of space systems and services and to deter and respond to any threats, including cyber, to sensitive space systems and services in the EU.

3 FIGHTING TERRORISM AND RADICALISATION

Nearly all the key initiatives presented in the EU Security Strategy to support Member States in the fight against terrorism and radicalisation have been adopted. Protecting against online threats has been a particular theme. The next step is to ensure that these initiatives achieve their full impact.

---

[38] Work is ongoing on the Strategic Compass' tasks to build a FIMI Data Space and equip the CSDP missions and operations with capabilities and resources to deploy relevant instruments of this toolbox. The EEAS continues to provide open-source situational awareness to EU Member States via the EU Rapid Alert System, raises public awareness in particular through the EUvsDisinfo campaign and has further enhanced its cooperation with stakeholders like NATO and the G7 Rapid Response Mechanism.

[39] JOIN(2022) 49.

The fight against terrorism

Since its adoption in December 2020**, the EU Agenda on Counter-Terrorism**[40] has equipped the EU to better anticipate, prevent, protect and respond to terrorist threats. Specific geographic initiatives have also helped respond to the evolving threat situation. In the light of developments in Afghanistan, the EU Counter Terrorism Coordinator in coordination with the Commission, the High Representative, the Presidency and key EU Agencies, drew up a **Counter-Terrorism Action Plan on Afghanistan**[41], endorsed by Member States in October 2021. A clear achievement has been a voluntary procedure for enhanced security checks on people coming from Afghanistan.

Addressing the threat posed by **returning Foreign Terrorist Fighters** in Syria and Iraq is a priority. While primary responsibility lies with Member States, cooperation at EU level helps Member States address common challenges such as 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. The Commission continues to work closely with Member States and key partner countries to ensure that battlefield evidence is entered into EU databases and information systems. In agreement with the Member States the EU Counter-Terrorism Coordinator is, in close cooperation with the High Representative and the Commission, exploring new ways to use improved living conditions in prisons and camps in North East Syria to help combat radicalisation.

EU legislation related to the fight against terrorism has been updated. **The Directive on combating terrorism** adopted in 2017 is now implemented by all Member States[42], to criminalise conduct such as training and travelling for terrorism, as well as terrorist financing. Incorrect transposition of the Directive in a number of Member States still needs to be addressed.

Depriving terrorists of the means to perform an attack is key in the fight against terrorism. Nearly all Member States have now adopted the updated legislation on firearms[43] in their national law. New legislation designed to limit the accessibility of explosive precursors that terrorists could use to produce bombs, came into force in February 2021. Building on the approach used to regulate access to explosive precursors, the Commission is exploring how to restrict access to certain dangerous chemicals that could be used to carry out attacks.

Public spaces have repeatedly been the focus of terrorist attacks. The Commission has issued a handbook to promote the security by design of public spaces[44]. This follows detailed technical guidance,[45] tools for vulnerability assessment of public spaces[46] and comprehensive support to key stakeholders,[47] as well as a Recommendation on voluntary performance

---

40 COM (2020) 795.
41 Afghanistan: Counter-Terrorism Action Plan, 29 September 2021.
42 COM (2021) 701. Member States were required to transpose the Directive into their national framework by 8 September 2018.
43 COM(2015) 750.
44 SWD(2022) 398.
45 Guideline - Building Perimeter Protection, EUR 30346 EN.
46 http://counterterrorism.jrc.ec.europa.eu
47 See in particular: EU Digital Autumn School, JRC127168 and Terrorism and Extremism Database - User Guide, JRC130461.

requirements for X-ray equipment used in public spaces (outside aviation).[48] In 2022, the Internal Security Fund has also funded €14.5 million of projects to improve the protection of public spaces including places of worship. **Drones** are a highly innovative tool that can be used for legitimate but also malicious purposes, including attacks on public spaces, individuals and critical infrastructure. In November 2022, the Commission adopted a **Drone Strategy 2.0,**[49] to be followed in 2023 by a more detailed EU approach on countering the malicious use of drones.

Combatting radicalisation leading to violent extremism and terrorism online and offline

Preventing and fighting **radicalisation** is key to effective counter-terrorist policies. The Commission supports Member States, with the Radicalisation Awareness Network (RAN) bringing together 6 000 experts active on prevention work. The main areas of support to Member States include countering violent extremist ideologies and polarisation leading to radicalisation; radicalisation online and misuse of new technologies; and managing and preparing reintegration of offenders released from prison. Links between violent extremist groups and ideologies and the manifestations of hate speech are addressed through the EU Code of Conduct on countering illegal hate speech online.[50]

The EU is also working to prevent foreign influences and funding supporting radical/extremists views in the Member States. For its part, the Commission remains vigilant to prevent EU funds supporting any project incompatible with European values or pursuing an illegal agenda. In this regard, since the end of 2021, projects managed by the Commission are published as soon as the grant agreement is signed, in a unique platform called the Funding and Tenders opportunities platform. It is essential that Member States use this window to themselves screen the beneficiaries and provide the Commission with any supplementary information available to them. In this context, the Commission's proposed revision of the Financial Regulation includes adding the issue of a conviction for "incitement to hatred" as grounds for exclusion from EU funding. The Commission calls on the European Parliament and the Council to effectively address this issue in the final text. In addition, the Commission is undertaking internal awareness raising measures and developing internal working methods to ensure increased scrutiny in the selection of projects.

Preventing radicalisation online is another key focus. The **Regulation to address the dissemination of terrorist content online**[51] became applicable in June 2022. Since then, national competent authorities can require terrorist content to be removed within one hour of an official removal order. Online service providers exposed to terrorist content have to take specific measures to protect their platforms against misuse. This complements the work of the **EU Internet Forum** (EUIF), launched by the Commission to bring together Member States, internet companies and civil society to prevent the dissemination of violent extremist and terrorist content online. Recent EUIF support to tech companies and internet infrastructure providers in their content moderation efforts include a directory on Terrorist Operated Websites, and a yearly updated knowledge package of violent right wing extremist

[48] This act recommends Member States to comply with the EU performance requirements when procuring X-ray equipment to be used for threat detection in public spaces (C(2022) 4179).

[49] COM(2022) 652.

[50] https://ec.europa.eu/commission/presscorner/detail/en/IP_16_1937

[51] Regulation (EU) 2021/784 of the European Parliament and of the Council of 29 April 2021 on addressing the dissemination of terrorist content online, OJ L 172, 17.5.2021, p. 79–109.

groups, symbols and manifestoes[52]. Since 2019, preventing Child Sexual Abuse online has also been addressed in this Forum.

Key delivery examples

How cooperation with Eurojust led to the conviction of a foreign fighter for terrorism: The main target of a terrorist-related investigation was sentenced in 2021 to four years' imprisonment for participation in a terrorist organisation after the Italian authorities used the Counter Terrorism Registry to identify links between a suspected foreign fighter and other terrorism cases. National authorities were brought together by Eurojust, leading to the execution of European Investigation Orders and Mutual Legal Assistance requests.

Europol coordination against bomb manuals available online: In one of a series of regular joint initiatives, an action day in February 2022, supported by Europol with participation of 8 Member States and the United Kingdom, found hundreds of items online including instructions on how to make bombs with precursors and how to use them in terrorist attacks. The information was referred to the online service providers.

4. FIGHTING ORGANISED CRIME

In the organised crime landscape in Europe cooperation between criminals is ever-changing. Criminal networks may be involved in a variety of criminal activities, combining drugs trafficking, organised property crime, fraud, migrant smuggling and trafficking in human beings[53]. Cybercrime and gender-based cyber violence has been further stimulated by the increased use of internet and online services. The increasing use of encrypted communication channels, while protecting privacy and fundamental rights, poses additional challenges for law enforcement[54]. Meanwhile, the disruption caused by the Russian war of aggression against Ukraine has created new openings, swiftly exploited by organised crime groups.

In April 2021, the Commission adopted the **EU Strategy to tackle Organised Crime 2021-2025**[55]. The Strategy highlights the importance of dismantling organised crime structures, targeting those groups that are a higher risk to Europe's security and the individuals in the higher echelons of criminal organisations. Its implementation is now well underway, with several key actions already adopted or implemented. The Commission has also been providing financial support to Member States to combat the criminal threats facing the EU[56].

Cybercrime

The accelerated digitalisation during the COVID-19 pandemic stimulated the spread of cyber threats such as ransomware[57]. **Ransomware** creates substantial cybersecurity risks for critical

[52] Other deliverables include: an update of the EU Crisis Protocol; handbooks with guidelines on malicious use of borderline content and video gaming leading to radicalisation; and a study on the effects of algorithmic amplification on the user path to radicalisation.

[53] Europol (2021), European Union serious and organised crime threat assessment, a corrupting influence: the infiltration and undermining of Europe's economy and society by organised crime, Publications Office of the European Union, Luxembourg.

[54] Internet Organised Crime Threat Assessment (IOCTA), 2021.

[55] COM(2021) 170.

[56] In July 2022, through the Internal Security Fund (ISF), the Commission allocated €15.7 million to Member States to support long-term projects and activities within the European Multidisciplinary Platform Against Criminal Threats (EMPACT), tackling the ten EU crime priorities adopted by the Council for 2022-2025.

[57] Internet Organised Crime Threat Assessment Report (IOCTA).

infrastructure and public safety. Europol's Cybercrime Centre (EC3), together with the Joint Cybercrime Action Taskforce (J-CAT) recently developed the International Ransomware Response Model to operationalise a comprehensive law enforcement response. The EU participated in the 2022 Summit of the Counter Ransomware Initiative to strengthen international cooperation on ransomware. 36 countries and the EU agreed to take forward work on International Counter Ransomware Task Force to coordinate work on resilience and disruption and counter illicit financing activities[58]. The Commission and Europol have jointly set up a Decryption platform[59], reducing the time taken for forensic access to digital evidence and helping to tackle encrypted criminal communication networks leading to major blows to organised crime activities.

The EU was instrumental in the successful negotiation of the Second Additional Protocol to the **Budapest Cybercrime Convention** in May 2022. This includes much needed tools for cross-border cooperation in investigating and prosecuting cybercrime, as well as detailed data protection conditions and safeguards. All Member States should swiftly sign the Second Additional Protocol and the European Parliament is invited to give its consent, to allow for swift ratification. The Commission is also negotiating on behalf of the EU a new United Nations cybercrime convention.

With 85 million pictures and videos depicting **child sexual abuse** reported worldwide in 2021 alone, and many more unreported, child sexual abuse is alarmingly pervasive. Children spending more time online has made them more susceptible to grooming, leading to an increase of self-produced exploitation material. In line with the EU Strategy for a more effective fight against child sexual abuse adopted in July 2020[60] and the EU Comprehensive Strategy on the Rights of the Child of March 2021[61], the Commission adopted a proposal laying down rules to prevent and combat child sexual abuse online in May 2022[62], with new obligations on online service providers. Where prevention fails to reduce a significant risk, service providers could be ordered to detect, report, remove and block child sexual abuse online. The proposal would also create a dedicated EU Centre, to facilitate implementation. Temporary legislation adopted in August 2021 to allow online service providers to continue voluntary detection and reporting of child sexual abuse online[63] will expire in the summer of 2024. It is therefore essential that the European Parliament and the Council find a swift agreement on the proposed Regulation. Early next year, this initiative will be complemented by a proposal to update the 2011 Directive on combating sexual abuse and sexual exploitation of children and child pornography[64].

Cyber violence against women and girls is an emerging new dimension of **gender-based cyber violence**. In 2020, it was estimated that 1 in 2 young women experienced this form of violence.[65] In its proposal for a directive on combating violence against women and domestic

---

58 International Counter Ransomware Initiative 2022, Washington DC, 1 November 2022.
59 The Europol Decryption Platform is hosted at the EC Joint Research Centre, Ispra site.
60 COM(2020) 607.
61 COM(2021) 142.
62 COM(2022) 209.
63 COM(2020) 568.
64 Directive 2011/93/EU of 13 December 2011 on combating the sexual abuse and sexual exploitation of children and child pornography, OJ L335, 17.12.2011.
65 European Parliamentary Research Service (EPRS), Combating gender-based violence: Cyberviolence, European added value assessment, 2021.

violence,[66] adopted in March 2022, the Commission proposed targeted rules on gender-based violence against women online or offline[67].

Organised Crime

Trafficking in human beings is a core activity of organised crime in the EU[68]. Tough already identified as a priority in the Security Union Strategy, criminals found new opportunities to generate significant profits and intensify criminal activities during the COVID-19 pandemic. Rapid EU level coordination is helping prevent the intensified threat of trafficking in human beings following Russia's war of aggression against Ukraine. The EU Anti-trafficking Coordinator developed a **Common Anti-Trafficking Plan**[69] to bring together the work of the Commission with Member States, EU Agencies and the European External Action Service to address the risks of trafficking in human beings and to support potential victims. These efforts have helped to ensure that the number of confirmed trafficking cases has remained limited, even if the threat remains high.

In April 2021, the EU Strategy on Combatting Trafficking in Human Beings 2021-2025 provided a comprehensive internal and external frame for action[70]. The Commission is following up with an upcoming proposal amending the **Anti-trafficking Directive**[71] to address shortcomings in the current legal framework and update it to reflect the online dimension, as well as seeking the reduction of demand. In September 2022, an EMPACT joint action day targeted criminal networks using websites and social media platforms to recruit victims for sexual exploitation in a first EU-wide hackathon against trafficking in human beings, supported by Europol and Eurojust, with law enforcement authorities from 20 countries. 11 suspected human traffickers and 45 possible victims were identified[72].

Unlike in the case of trafficking, those who pay smugglers to enter the EU irregularly do so voluntarily. However, the activity of smugglers is criminal, often puts lives at risk, and may lead to additional security risks for the EU. Preventing and fighting **migrant smuggling** is a key objective of the EU Security Union Strategy, the EU Strategy to tackle Organised Crime and the New Pact on Migration and Asylum[73]. It requires continuous international cooperation and coordination at all levels. The implementation of the EU Action Plan against Migrant Smuggling 2021-2025[74] is progressing, with Anti-Smuggling Operational Partnerships are being developed with Morocco, Niger, and the Western Balkans supported by EU institutions, bodies and agencies, and EU funding.

The **illegal drugs** market, estimated at a minimum retail value of €30 billion per year, remains the largest criminal market in the EU and a major source of income for organised

---

66 COM(2022) 105.

67 The proposal includes EU-level criminalisation of non-consensual sharing of intimate materials, cyber stalking, cyber harassment and cyber incitement to violence or hatred. This would be complemented by a new framework for cooperation between internet platforms to better protect women's safety online.

68 Serious and Organised Crime Threat Assessment (SOCTA) 2021.

69 An Anti-Trafficking Plan to protect people fleeing the war in Ukraine (europa.eu).

70 COM(2021) 171.

71 The 4th Progress Report on trafficking in human beings to be adopted alongside this proposal provides in-depth information on the implementation of the EU Strategy from 2019 to 2022 as well as key data and statistics.

72 20 countries spin a web to catch human traffickers during a hackathon | Europol (europa.eu)

73 COM(2020) 609.

74 COM(2021) 591.

crime groups, as well as a threat to social stability and health. In 2021, EU action and cooperation led to €7 billion worth of drugs taken off the streets[75]. The July 2020 **EU Agenda and Action Plan on Drugs 2021-2025**[76] sets out concrete actions to step up action at the EU level, including the transformation of the European Monitoring Centre for Drugs and Drug Addiction into the European Union Drugs Agency. The revised mandate of the Agency proposed in January 2022[77] would strengthen its monitoring and threat assessment capabilities and its ability to react to new challenges. The Council adopted a general approach in June 2022, the work in the European Parliament is ongoing. The Commission also initiated cooperation in the EU Internet Forum to address online drugs trafficking and proposed a specific thematic Schengen evaluation on the smuggling of cocaine into EU ports. Support to the Maritime Analysis and Operation Centre - Narcotics was increased. The EU also continues its political dialogues on drugs with third countries, with a second dialogue with China in July 2022 and a new dialogue with Colombia launched in June 2022.

According to Europol, almost 99% of criminal profits escape **confiscation** in the EU, remaining in the hands of offenders[78]. Proposals to strengthen EU's anti-money laundering and counter the financing of terrorism proposed by the Commission in July 2021 is advancing in Council[79]. In May 2022, the Commission proposed to reinforce and modernise EU rules on asset recovery and confiscation[80]. The proposal has been discussed in Council working groups with progress being made in several areas.

The **European Public Prosecutor's Office** has now had its first full year of work to protect the EU's financial interests. It received 4 006 crime reports, opened 929 investigations and granted freezing orders for a total value of €259 million. During its first seven months of activity, cases under investigation were potentially responsible for an estimated damage of €5.4 billion to the Union budget[81].

The Commission is also working on the preparation of the **EU Toolbox against counterfeiting**, as announced in the Intellectual Property Action Plan[82] and highlighted in the Organised Crime Strategy.

As well as damaging the trust between the state and the citizen, **corruption** is a threat to security. It is a key tool for organised crime and facilitates a wide variety of criminal activities. It is a core theme of the annual Rule of Law Report cycle[83]. While some EU Member States continue to be among the best performers globally in the fight against corruption, many challenges remain, in particular as regards criminal investigations, prosecutions and the application of sanctions for corruption. Many Member States have measures underway to strengthen corruption prevention and integrity frameworks, the

---

75 Eurojust annual report 2021.
76 COM(2020) 606.
77 COM(2022) 18.
78 Europol, Does crime still pay? Criminal Asset Recovery in the EU – Survey of statistical information 2010-2014, 2016.
79 COM(2021) 421, COM(2021) 420 COM(2021) 423 COM(2021) 422. A political agreement was reached on the Transfer of Funds Regulation in June 2022, and a partial general approach was also found on the on the regulation establishing the Authority for Anti-Money Laundering and Countering the Financing of Terrorism (except provisions on resources and seat) in June 2022.
80 COM(2022) 245 final.
81 EPPO First Annual Report, 2022.
82 COM(2020) 760.
83 The most recent edition of the report was adopted on 13 July 2022 (COM (2022) 500).

resources allocated to anti-corruption often fall short. The Commission is working on an anti-corruption package for 2023 which will update and streamline legislation in this area.

The 2020-2025 EU action plan against **firearms trafficking**[84]was adopted together with the Security Union Strategy in July 2020. This was followed up in an October 2022 proposal to revise the rules on export authorisation, import and transit measures for firearms[85], with a broader focus on digitalisation. Overall, this should improve the traceability of civilian firearms. Work is also ongoing to better support Ukraine and the Republic of Moldova regarding **Small Arms and Light Weapons** (SALW) in the context of the Russian aggression against Ukraine.

The illicit trafficking of cultural property is a lucrative business for organised crime groups, and in some cases for conflict parties and terrorists[86]. It therefore stimulates organised crime, as well as having a damaging impact on cultural heritage. Criminals can abuse even legally acquired cultural goods, for money laundering, sanctions evasion, tax evasion or terrorism financing. In order to strengthen the **fight against the trafficking of cultural goods** the Commission is today adopting an action plan[87].

According to Interpol and the United Nations Environment Programme, **environmental crime** is the fourth largest criminal activity in the world after drug trafficking, human trafficking and counterfeiting. Ambitious Commission proposals for a new Environmental Crime Directive,[88] a new Waste Shipment Regulation[89] and a new Regulation on deforestation[90] are currently under negotiation. Once adopted, these will strengthen the enforcement chain and provide for higher sanctions and proper investigative tools. They are also complemented by a revised Action Plan against wildlife trafficking.[91]

Key delivery examples

Encrochat: With the support of Europol and Eurojust, judicial and law enforcement authorities in Belgium, France and the Netherlands cooperated to block the use of encrypted communications by large-scale 14 organised crime groups. The service had 60 000 subscribers at the time it was closed down, an estimated 90% of them criminal.

EU judicial and police cooperation led to the dismantling of a large-scale Organised Crime Group (the 'Pollino case'): A Joint Investigation Team set up in 2016 between Italy, Germany and The Netherlands launched an action day, coordinated by Eurojust and supported by Europol, that led to 34 individuals being convicted, to a total of more than 400 years in prison. Later another 12 individuals were convicted to more than 173 years in prison, and proceedings are still ongoing in several Member States.

4. ENSURING THE SECURITY OF OUR BORDERS AND SUPPORTING LAW ENFORCEMENT AND JUDICIAL COOPERATION

84 COM(2020) 608 final.
85 COM(2022) 480.
86 See for example United Nations Security Council Resolutions 2199 (2015), 2253 (2015), 2322 (2016), 2347 (2017), 2462 (2019) and 2617 (2021); G20 Culture Ministers Rome Declaration of 30 July 2021.
87 COM(2022) 800.
88 COM(2021) 851.
89 COM(2021) 709.
90 COM(2021) 706.
91 COM(2022) 581.

Alongside the economic and social benefits, a well-functioning **Schengen area** is key to the EU's security. This requires effective management of the EU's external borders and enhanced law enforcement cooperation. In June 2021, the Commission adopted a Strategy Towards a fully-functioning and resilient Schengen area[92], setting out how measures in the field of security, police and judicial cooperation can ensure that the EU remains strong against security threats, even without controls at internal borders. The Strategy is now taken forward through an annual Schengen cycle – a new governance model for the Schengen area – with progress tracked in the first report on the State of Schengen, adopted in May 2022[93]. A key step is an amended Schengen Borders Code,[94] through the Commission proposal of December 2021, which included new provisions to support effective security cooperation and the steps to take to manage external borders more efficiently in crisis situations. With a Council general approach from June 2022, it is important for the European Parliament and Council to swiftly conclude negotiations. The Commission also underlined the benefits of including Bulgaria, Romania and Croatia in all aspects of Schengen, reinforcing security and mutual trust in the Schengen area[95]. In December 2022, the Council adopted a decision on the full application of the Schengen acquis in Croatia[96].

In an area without internal border controls, police officers in one Member State should have access to the same information available to their colleagues in another Member State. The norm must be full and effective cooperation. This is why it is essential to reinforce the tools available to law enforcement and judicial authorities across the EU for **information exchange and cross-border cooperation**. The police cooperation package in December 2021[97] offered a major enhancement of the tools available. The **Directive on information exchange** has now found a political agreement between the European Parliament and the Council, and a Council recommendation reinforcing operation cross-border police cooperation was adopted by the Council in June 2022. Negotiations continue on a Regulation revising the Prüm framework[98], seeking to allow for more efficient automated exchange of data between law enforcement authorities in specific areas such as DNA, dactyloscopic and vehicle registration data, and adding the categories of police records and facial images. Swift agreement on the **Prüm II Regulation** would make the full range of new information exchange tools become a reality on the ground for law enforcement in Member States.

In order to fight cross-border crime more effectively, Member States law enforcement and judicial systems need to work hand in hand with the support of EU agencies such as Europol and Eurojust. The new **Europol** mandate entered into force in June 2022, allowing Europol to step up its expertise and operational capabilities, to better support Member States in combating serious and organised crime and terrorism. The mandate also strengthens Europol's data protection framework and the oversight of the European Data Protection Supervisor. Investigative authorities and courts of different Member States need to cooperate and support each other in the investigation and prosecution of crimes and exchange

92 COM(2021) 277.
93 COM(2022) 301.
94 COM(2021) 891.
95 COM(2022) 636.
96 From 1 January 2023, checks on persons at internal land and sea borders between Croatia and the other countries in the Schengen area will be lifted. Checks at internal air borders will be lifted from 26 March 2023.
97 COM(2021) 782, COM (2021) 780.
98 COM (2021 784.

information and evidence securely and swiftly. The **Digital Justice Package**[99] adopted in December 2021, consisted of practical steps to improve digital information exchange on cross-border terrorism cases, to set up a cooperation platform to support the functioning of Joint Investigation Teams, and to enhance the digitalisation of cross-border judicial cooperation and access to justice in civil, commercial and criminal matters. Swift adoption of this package by the European Parliament and Council would bring a major facilitation of information exchange between judicial authorities.

Electronic evidence is part of almost every investigation. The provisional political agreement reached in November 2022 on **e-evidence**[100] will bring secure exchange on evidence of critical value to judicial authorities in the Member States in fighting crime more effectively.

Securing the EU's external borders is a common responsibility. The first teams of the European Border and Coast Guard standing corps have been successfully deployed since January 2021 and the standing corps now numbers some 4 800 Frontex and national officers.

The increase of irregular arrivals this year across most migratory routes has underlined the importance of systematic identity and security checks of all migrants arriving at external borders of the EU, as well as health checks meeting common standards. Security is an important theme in the New Pact on Migration and Asylum. Channeling migrants quickly to the appropriate procedures under the **Screening Proposal** would help to ensure that security checks are applied, in full respect of all fundamental rights obligations. A European Parliament position on this proposal is still awaited.

The **instrumentalisation of migrants** for political purposes by the Belarusian regime in the second half of 2021 raised unprecedented legal, operational and human challenges, including for security. The Schengen Borders Code proposal also addresses the issue of instrumentalisation of migrants by third countries for political purposes. Member States faced with this situation would for example be able to limit the number of border crossing points and intensify border surveillance.

A new architecture of EU **information systems** is being developed to better support national authorities' work to ensure security as well as border and migration management. Central to this is the renewed Schengen Information System, which should start its operations in March 2023. Other key tools are the Entry/Exit System (planned to start work in May 2023), the European Travel Information and Authorisation System ETIAS (due to enter into operation by the end of 2023) and the update of the Visa Information System (VIS). These will allow more checks and close security information gaps through better information exchange between Member States. Crucial to this work is the interoperability of the systems: it is essential that eu-LISA and Member States take the necessary steps without delay to deliver this ambitious project for full implementation by the end of 2024.

Controls on incoming goods have to be effective to reduce risks to the EU and its citizens, whilst ensuring competitiveness of legitimate EU businesses. Security controls have been enhanced on these goods through an upgraded EU import control system[101], to support effective risk-based customs controls and measures to protect air cargo security from terrorist

[99] COM (2021) 756, COM (2021 757, COM (2021) 759.
[100] COM (2018) 225, COM (2018) 226.
[101] The Import Control System 2 (ICS2) will be operational in three releases (March 2021, March 2022 and March 2023). Each release affects different Economic Operators (EOs) and models of transport.

threats. The Customs Control Equipment Instrument (CCEI) programme[102] is also funding the transparent purchase, maintenance and upgrading of relevant, state-of-the-art, and reliable customs control equipment.

The ability of **Advance Passenger Information (API)** to contribute to security is hampered by rules which are outdated and unevenly applied. The new Commission proposals would repeal the current API Directive to clarify and enhance the use of API for both border management and law enforcement[103]. It would expand the use of API to selected intra-EU flights, extending the toolbox available to the Member States law enforcement authorities within the Schengen area. Reflections on the external dimension of the EU's policy on **Passenger Name Records** (PNR) are ongoing, to reflect the fact that an increasing number of third countries are developing the capability to process this information for law enforcement and border security. The Commission is also preparing a legislative proposal on a framework for reciprocal access to security-related information for front-line officers in the EU and partner third countries, to efficiently detect criminals and terrorists.

Travel document fraud facilitates the clandestine movement of criminals and terrorists, and plays a key role in trafficking in human beings and in the drugs trade. This needs to be tackled alongside the need to facilitate legitimate travellers, so since August 2021, Member States are issuing identity cards with harmonised security standards, including a chip containing biometric identifiers that can be verified by all EU border authorities[104]. The Commission is preparing a further initiative on digitalisation of travel documents and facilitation of travel[105] that will enhance security and speed up travel and border processes through paperless advanced communication of travel and personal data and biometric checks at borders.

Law enforcement and new technologies

Technologies such as **Artificial Intelligence** or encryption can bring added value to law enforcement and judicial authorities, but can also hamper their work. In its Communication on Artificial intelligence (AI) and in the Artificial Intelligence Act[106], the Commission underlined that AI can significantly contribute to the objectives of the Security Union strategy, countering current threats and anticipating future risks and opportunities[107]. Under Horizon Europe, the EU's research and innovation programme for the period 2021-2027, funding is available for **civil security research** actions and innovation, including on AI or biometrics. For 2021 and 2022 alone, €413.8 million has already been programmed[108].

[102] Regulation (EU) 2021/1077 of 24 June 2021 establishing, as part of the Integrated Border Management Fund, the instrument for financial support for customs control equipment.
[103] COM(2022) 729 and 731.
[104] Based on Regulation (EU) 2019/1157 of the European Parliament and of the Council of 20 June 2019 on strengthening the security of identity cards of Union citizens and of residence documents issued to Union citizens and their family members exercising their right of free movement (OJ L 188, 12.7.2019, p. 67).
[105] EUR-lex 52022PC0658.
[106] COM(2021) 206.
[107] COM(2021) 205.
[108] Horizon Europe also invests substantial funds in innovative technologies for the benefit of law enforcement authorities in the fight against radicalization, as well as projects in detection of drugs and explosives, cultural goods trafficking, migrant smuggling, security of public spaces and identity theft.

Key delivery example

Use of the Schengen Information System (SIS): In 2021, almost 7 billion searches were performed by Member States in the SIS. Member States authorities performed almost 20 million searches in the system on average per day, leading on average to 600 hits on foreign alerts per day, contributing to solving an equivalent number of cases. For instance, after a brutal double murder in Romania in 2021, the perpetrator was tracked down in Italy only days later, thanks to a SIS alert for arrest that tipped off Italian investigators – who were able to arrest the man in Rome.

5. THE INTERNAL-EXTERNAL SECURITY NEXUS: SECURITY IN THE EU NEIGHBOURHOOD AND IN PARTNER COUNTRIES

What happens outside of the EU's borders and security within Europe is closely intertwined. Supporting and helping our neighbours and partners in enhancing their internal security and cooperating with our allies and with international organisations such as NATO or the UN is indispensable to enhance the EU's internal security.

The European External Action Service (EEAS) and the Commission services work closely with key partner countries and international organisations, through regular **counter-terrorism** (CT) dialogues. More than 30 CT Dialogues are ongoing with third states and International Organisations[109]. In parallel, the network of counter terrorism and security experts in EU delegations in key third countries has been reinforced.

To better counter internal security threats stemming from Russia's war of aggression against Ukraine, the Commission services and the EEAS, with the EU Counter-Terrorism Coordinator, agreed with **Ukraine** to establish a continuous structured security cooperation. This collaboration aims to enhance operational cooperation, including with Europol and Frontex, and to strengthen information exchange on internal security threats. EU Agencies brought immediate support to responding to the challenges following the invasion. Currently Frontex has 277 staff deployed in the region, Europol 15 and the European Union Asylum Agency, 60.

Member States' law enforcement authorities and their partners work together in the framework of the **European Multidisciplinary Platform Against Criminal Threats (EMPACT)** to organise operational actions and joint action days against new or evolving crime threats linked to Russia's aggression against Ukraine.

Cybersecurity Dialogue between the EU and Ukraine has been stepped up with coordinated political, financial and material support from the EU to help Ukraine to strengthen its cyber resilience. Overall funding of EUR 29 million to increase Ukraine's cyber and digital resilience has supported cyber security equipment, software, and resilient digital transformation.

Due to its geographical location, the Republic of **Moldova** has a key role to play in addressing the criminal and security implications of Russia's invasion of Ukraine. In July 2022, the Commission, in cooperation with the EEAS, launched an EU support Hub for Internal Security and Border Management with the Republic of Moldova. Its main role is to

[109] In 2022 CT dialogues took place with the UN, Israel, India; Turkey, Qatar and the United Arab Emirates (UAE) are upcoming. In 2023, key expected dialogues are Morocco, Tunisia, Egypt, Kenya, US, KSA, possibly also Algeria.

facilitate cooperation and operational action to address shared security threats in six priority areas jointly identified by the EU and the Republic Moldova: firearms trafficking, migrant smuggling, trafficking in human beings, preventing and countering terrorism and violent extremism, cybercrime and drug trafficking. In March 2022, the Republic of Moldova signed a status agreement with Frontex, based on its reinforced mandate.

Law enforcement cooperation between the EU and the **Western Balkan countries** – also drawing on EU Agencies – continued to intensify in the past three years. In line with Council Conclusions of March 2021, law enforcement cooperation with third countries was mainstreamed in all European Multidisciplinary Platform against Criminal Threats (EMPACT) operational action plans, resulting in a boost in the Western Balkans' participation in EMPACT activities. Significant funding under the Instrument for Pre Accession continues to be provided for law enforcement reform and performance, with EU Agencies also providing capacity-building to security actors. The Joint Action Plan on Counter Terrorism signed in 2018 has been taken forward with good progress, and in the case of North Macedonia and Albania, considering that most of the actions were completed, a revised updated version of the respective bilateral agreements has been signed in December 2022, to further upgrade our cooperation in the field of counter terrorism and prevention and countering of violent extremism.

On 18 November 2022, the Council authorised the opening of negotiations of **Frontex status agreements** between the EU and Albania, Serbia, Montenegro, and Bosnia and Herzegovina[110]. These agreements would allow Frontex to deploy border management teams to carry out border control tasks, under the command of the relevant national authorities. This will be of particular value in countering migrant smuggling. North Macedonia signed a status agreement with Frontex in October 2022, based on its reinforced mandate.

The **EU and the US** also have a long history of partnership and cooperation on security issues, aiming at a more systematic and timely exchange of information on issues such as terrorism, radicalisation and organised crime. The EU and the US hold regular joint Justice and Home Affairs meetings to deepen cooperation on matters of common interest, promote global security and update each other on legislative progress on JHA files. European judicial and law enforcement agencies cooperate closely with their US counterparts on operational and legislative matters. US law enforcement authorities are active participants of several EMPACT actions and networks, with operational cooperation agreement between the US and Europol. A powerful example of effective cooperation is the Operational Task force Greenlight/Trojan Shield, one of the largest and most sophisticated law enforcement operations to date in the fight against encrypted criminal activities. The Terrorist Finance Tracking Programme between the EU and the US provides numerous concrete leads for terrorist investigations[111]. The cooperation also relies on clear monitoring of safeguards and controls.

Regular EU-US Cybersecurity Dialogues strengthen cooperation and coordination on both cyber diplomacy and cyber resilience, including cybersecurity standardisation. The Trade and Technology Council (TTC) has also allowed cooperation to deepen, with a joint Statement on cyber security and steps for potential cooperation on research and development beyond 5G

[110] Council Decision (EU) 2022/2271 – Albania ; Council Decision (EU) 2022/2272 – BiH ; Council Decision (EU) 2022/2273 – Montenegro; Council Decision (EU) 2022/2274 – Serbia.

[111] See the sixth Joint review of the implementation of the TFTP Agreement COM(2022) 585.

and 6G, on export controls, and on investment screening, as well as on sanctions against Russia and Belarus. The TTC will also further advance EU-US cooperation on Foreign Information Manipulation and Interference.

Important security challenges in Africa directly impact Africans themselves as well as the security of the EU. Many projects are implemented to help partner countries to build capacity to address these challenges, for example through the funding of the international counter terrorism academy (AILCT) in western Africa or with the regional initiative to enhance capacity in fighting money-laundering and countering the financing of terrorism in the Greater Horn region.

The countries of **Latin America and the Carribean** (LAC) are essential partners for the EU, and a new Regional Team Europe Initiative for Security and Justice was launched in May 2022 to set up an EU-LAC partnership on strengthening the rule of law and the fight against organised crime.

The EU **Foreign Direct Investment Screening** Regulation entered into force in October 2020[112] and provides a framework to improve protection against foreign direct investments posing a risk to security or public order in more than one Member State. In its first full year of operation, more than 400 cases were notified to the Commission. The Dual Use Regulation[113] adopted in September 2021 upgraded and strengthened the EU **dual-use export control** system and introduced new provisions that allows the EU – in coordination with the Member States – to adopt autonomous controls on export of non-listed items and technologies.

In a globalised world, where serious crime and terrorism are increasingly transnational, law enforcement and judicial authorities should be fully equipped to cooperate with external partners to ensure the security of their citizens. This calls for opening the door to cooperation and information exchange between the judicial authorities of third countries for **Europol and Eurojust**. An agreement signed in June 2022 between Europol and New Zealand on the exchange of personal data to fight serious crime and terrorism[114] is being followed up by negotiations with a number of other countries, but in most cases progress remains slow. As for Eurojust, negotiations are well advanced with Armenia where agreement on the text has been found, and have started with Colombia, Algeria and Lebanon.

In April 2022, the **EU and the UN** took concrete steps to strengthen their existing partnership to fight persistent but evolving threats to international peace and security during the fourth Leaders dialogue on counter-terrorism. The strategic partnership was further strengthened through the launch of the new "EU-UN Global Terrorism Threats Facility", an EU-funded initiative to support States faced with terrorism and violent extremism, including through assistance, training, and mentoring. Other issues of common concern include emerging threats related to new technologies, including how they affect youth as a particular target group for radicalisation to violence, and terrorism based on xenophobia, racism, and other forms of intolerance, or in the name of religion or belief.

EU-NATO cooperation has also been stepped up, with tangible deliverables in all areas of cooperation[115]. The EU and NATO have intensified their work and cooperation in the wake of

[112] EU/2019/452.
[113] EU/2021/821 recast.
[114] The agreement was favourably described by the European Data Protection Supervisor (EDPS) as a model for future agreements on the exchange of personal data for law enforcement purposes.
[115] See Seventh progress report on the implementation of the common set of proposals endorsed by EU and

Russia's war of aggression, with a unified policy stance and coordination to help Ukraine defend itself and protect its population. The EU-NATO strategic partnership is more robust and relevant than ever at this critical moment for Euro-Atlantic security. On resilience, a dedicated Structured Dialogue was launched in January 2022, now being deepened on to support the protection of critical infrastructure and an EU-NATO Task Force will be set up in that context. On military mobility, further improvements have been made regarding transport and regulatory aspects, including the transport of dangerous goods. Countering hybrid threats also remains a key area of cooperation with NATO. Exchanges include counter-terrorism, as well as strategic communication, foreign information manipulation and interference and cyber issues. Exercises included the EU Integrated Resolve in November 2022 within the Parallel and Coordinated Exercise (PACE) concept, with the involvement of NATO staff, in order to improve the interaction between the respective crisis response mechanisms.

Since September 2022, the EU has been co-chair of the **Global Counter Terrorism Forum**. Priorities include addressing the terrorist threat in Africa and integrating gender and education into counter-terrorism policy.

Negotiation of a Cooperation Agreement between the Union and **Interpol** is ongoing with a view to reaching a conclusion at technical level during the first half of 2023. The main aim is to further reinforce the exchange of information between Interpol and EU agencies and bodies, to better support Member States and increase the security of citizens, not only in the EU but across the world.

Key delivery example

Operation Desert Light: European drug cartel taken down in six countries: In November 2022, coordinated raids were carried out across Europe and the United Arab Emirates (UAE), targeting both the command-and-control centre and the logistical drugs trafficking infrastructure in Europe. High-value targets had formed a 'super cartel' controlling around one third of the cocaine trade in Europe. A total of 49 suspects have been arrested following investigations in Spain, France, Belgium, the Netherlands and the UAE with the support of Europol. 30 tons of drugs were seized by law enforcement in the course of the investigations.

6. CONCLUSION

Over the past two and a half years, the Commission in close cooperation with the European External Action Service, has delivered successfully on nearly all the actions set out in the Security Union Strategy. The wide range of proposals need adoption and above all implementation. The decisions and actions of the European Parliament, the Council and individual Member States will be key to ensure that the EU delivers a robust Security ecosystem for its citizens.

At the same time, the security environment will continue to change around us. Since the Security Union Strategy was adopted, the EU has faced the COVID-19 pandemic and the impact of the Russia's aggression against Ukraine. There has been an exponential proliferation in online threats and the need for swift adaptation and foresight. The EU must continue to equip itself to deal with whatever evolving threats jeopardise the security of its citizens. Constant vigilance, determination to act, and collective responses will be key for the EU's collective success going forward.

NATO Councils on 6 December 2016 and 5 December 2017, 20 June 2022.