EUROPEAN
COMMISSION

Brussels, 23.6.2021
COM(2021) 440 final

COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT AND THE COUNCIL

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

I. Introduction

Last July, 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. The Strategy built on the European Agenda on Security 2015-2020 but provided a new focus and coordinated approach to the different strands of security policy, to ensure that the EU can respond to the rapidly evolving threat landscape. It aims to ensure that the EU plays its full role in ensuring the safety of citizens and their fundamental rights, both by addressing current risks and adapting to new challenges, and to deliver on the values that define the European way of life.

The COVID-19 pandemic has added to this context of dynamic change, creating new opportunities for online crime, stimulating cybercrime and opening the door to an increase in the counterfeiting and distribution of substandard goods, organised property crime, and various types of fraud[2]. Some of these directly undermined health systems and the provision of health services. While some criminal activities will return to their pre-pandemic state, others will be fundamentally changed by the pandemic[3].

The Strategy set out actions to be taken over a five-year period. One year in, a significant number of initiatives have been launched[4]. The Commission has adopted an EU Counter-Terrorism Agenda and initiatives to tackle organised crime, trafficking in human beings, drugs, child sexual abuse and firearms trafficking, as well as a new EU Cybersecurity Strategy. The Commission has tabled important new legislation to strengthen Europol, to protect critical physical and digital infrastructure, and to address child sexual abuse material. The European Parliament and Council have taken this programme forward and concluded on key files, most notably on terrorist content online and the fight against child sexual abuse online. Work on the legislation outlined in the Strategy should advance rapidly, while maintaining a high level of ambition.

The Commission adopted in June a new Strategy 'Towards a fully-functioning and resilient Schengen area'[5] with effective measures in the field of security, police and judicial co-operation for the functioning of the area of freedom security and justice, so that the EU remains strong against security threats, even without controls at internal borders. During the reporting period, agreement was found by co-legislators on the Funds which support many of the actions under the Security Union, in particular the reinforced Internal Security Fund (ISF) and the Border Management and Visa Instrument (BMVI) as part of the Integrated Border Management Fund (IBMF).

The success of the Security Union Strategy will rest on the quality of its implementation[6]. This requires the full engagement of the national authorities and constant cooperation between all actors concerned with Europe's internal and external security, including EU agencies. An inclusive, whole-of-society approach is being taken forward through enhanced cooperation among security stakeholders.

---

1 Communication from the Commission on the EU Security Union Strategy, COM (2020) 605.
2 Including on life saving medicines, medical devices and vaccines.
3 EU Serious and Organised Crime Threat Assessment (SOCTA) Report 2021, Europol.
4 See Annex II - Implementation Roadmap.
5 COM(2021)277.
6 Annex I provides an overview of the status of implementation of legislation on security.

This second Security Union progress report, covering the period since the first report[7] on 9 December 2020, charts the progress made in all four pillars of the Strategy: a future-proof security environment, tackling evolving threats, protecting Europe from terrorism and organised crime, and a strong European security ecosystem. It sets out how this work is being taken forward, including the specific contribution of EU agencies.

II. A future-proof security environment

1. Critical Infrastructure protection and resilience

The protection and resilience of critical infrastructure, both physical and digital, is of paramount importance for the functioning of modern societies and the European way of life. Never is this truer than at a time of public health emergency. Threats, incidents, and attacks on critical infrastructure can have very disruptive consequences.

Resilience is more essential than ever in time of pandemic

At a time when health infrastructure is already under pressure, cyber incidents targeting hospitals, medical agencies and comprehensive health services can have particularly dramatic consequences.

Ireland has recently been hit by a number of serious cyber attacks affecting its healthcare system, with hackers targeting both the Department of Health and the Health Service Executive.

The early warning and response system (EWRS)[8] national databases that support the health sector response, have been the target of intrusions attempts and ransomware attacks[9].

The cyberattack on the European Medicines Agency revealed that unlawfully accessed documents related to COVID-19 medicines and vaccine can have dramatic effects once put on the internet.

Outside the field of health, but in another area touching on citizens' daily lives, the challenge of protecting critical physical infrastructure and its link to cybersecurity was also illustrated by the Colonial Pipeline ransomware attack in the US[10].

The scale of potential risks shows the urgent need to step up preparedness at national and EU level, by building up robust capabilities to prevent, detect, and mitigate such threats, and to handle offline and online crises.
EU legislation in this area, and in particular the Directive on security of network and information systems[11] (NIS Directive) and the European Critical Infrastructure (ECI)

[7] First Progress Report on the EU Security Union Strategy, COM(2020) 797.
[8] EWRS is a rapid alert system for notifying alerts at EU level on serious cross-border threats to health, set up under Decision 1082/2013/EU, https://ec.europa.eu/health/security/surveillance_early-warning_en
[9] The EWRS data security operated by the European Centre for Disease for Disease Prevention and Control (ECDC) was not affected, but it will be reinforced.
[10] Colonial Pipeline, a critical pipeline that transports 45% of oil consumed on the east coast of the US, was the target of a ransomware cyberattack in May 2021 that disrupted its oil deliveries for days.

Directive[12], has provided a good basis for responding to recent incidents. In the case of the ransomware attack on the Irish Health Service, national cybersecurity experts used existing fora[13] established under the NIS Directive to exchange information, at both technical and policy level, enabling the Irish authorities to receive support, and other Member States to step up preparedness for such attacks.

At the same time, the increased incidence and intensity of threats shows that the current legislative framework is not fit for purpose. The evaluation[14] of the implementation of the NIS Directive showed that its scope does not reflect today's level of digitisation and interconnectedness, nor the interdependence of key economic and societal sectors. In addition, some public and private entities belonging to essential sectors are either not subject to the Directive or have to comply with non-harmonised cybersecurity and incident-reporting obligations. The evaluation[15] of the implementation of the ECI Directive showed that it focuses on asset protection in only a very limited number of sectors, as opposed to operator resilience. Both evaluations showed divergent approaches and deficiencies at national level

In December 2020, the Commission therefore proposed two key pieces of legislation: a directive on **critical entities resilience** (CER)[16] and a revised directive on measures for a **high common level of cybersecurity across the Union** (revised NIS Directive)[17]. Both directives have a broad scope, covering the same ten essential sectors: transport, energy, banking, financial market infrastructure, health, drinking water, wastewater, digital infrastructure, public administration and space. For these sectors, measures are proposed in the CER Directive to set up a physical resilience framework with minimum standards, allowing for flexibility to reflect national specificities. The proposed revised NIS Directive aims to set a horizontal standard for cybersecurity requirements in the internal market, strengthening the focus on supply chain security. It would introduce new tools for a coordinated handling and disclosure of vulnerabilities as well as more effective incident response and crisis management. It would also streamline incident-reporting obligations with more precise provisions on the reporting process, content and timeline.

In light of the continually evolving threats to our critical infrastructure, the Commission calls upon the co-legislators to show a high level of ambition and to ensure the smooth adoption of these two proposals, while preserving their consistency and complementarity. Progress towards the adoption of these proposals also needs to ensure consistency with the Commission's proposal of 2020 on digital operational resilience for the financial sector[18], which aims to strengthen Europe's ability to reinforce its strategic autonomy in financial services and, by extension, its capacity to regulate and supervise the financial system in the interests of financial stability.

---

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

[12] Council Directive 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection.

[13] CSIRTs Network and Cooperation Group.

[14] SWD(2020)345 Part II.

[15] SWD(2019) 310.

[16] Proposal for a Directive on the resilience of critical entities, COM (2020) 829.

[17] Proposal for a Directive on measures for a high common level of cybersecurity across the Union, repealing Directive EU 2016/1148, COM (2020) 823.

[18] Proposal for a Regulation on digital operational resilience for the financial sector and amending Regulations EC No 1060/2009, (EU) No 648/2012, (EU) No 600/2014 and (EU) No 909/2014, COM (2020) 595.

Energy Sector initiatives
To target more specific vulnerabilities, sector-specific initiatives are necessary. In this regard, important developments in the energy sector are to be highlighted. As part of the monitoring of the impact of the COVID-19 crisis in the energy sector, a study was completed in May 2021, identifying the energy technology supply chains critical for energy security and clean energy transition, and proposing measures to improve resilience in pandemics and other threat scenarios. Its findings will inform other relevant work streams, including the work of the NIS Cooperation Group on the energy sector. The Thematic Network on Critical Energy Infrastructure Protection continued its work on challenges to the protection of critical energy infrastructure, addressing topics such as risk assessments, information exchange information and the financing of security measures[19].

In January 2021 the Commission launched the formal procedure to establish a dedicated network code on **cybersecurity for cross-border flows of electricity,** with the Agency for the Cooperation of Energy Regulators (ACER). This network code will contain common minimum requirements on planning, monitoring, reporting and crisis management, in line with the horizontal framework set under the NIS Directive. With regard to **risk-preparedness in the electricity sector**, Member States initiated in April 2021 a consistency consultation on their draft risk-preparedness plans. These plans include measures to prevent and mitigate electricity crises and are based on national electricity crisis scenarios, identified by each Member State, as well as the regional electricity crisis scenarios identified by the European Network of Transmission System Operators in September 2020, which include cyber-attacks, as well as pandemic and extreme weather events.

2. Cybersecurity

The digital transformation of society, intensified by the COVID-19 crisis, is creating new challenges, requiring innovative responses. During the last few months, the number of cyber-attacks has continued to rise, with increasingly sophisticated attacks from a wide range of sources both inside and outside the EU. Major data breaches and recent cyberattacks like the massive SolarWinds cyber operation[20] show the scale of the risks to society if we fail to make a step change in cybersecurity. The EU needs to work to protect its governments, citizens and businesses from cyber threats while securing an open and global Internet. Important steps have been taken to deliver on the vision that every EU citizen should be able to live his or her digital life safely using the global and open Internet.

In December 2020, the Commission and the High Representative presented a new EU Cybersecurity Strategy[21]. As a key component of Shaping Europe's Digital Future and the Recovery Plan for Europe as well as the Security Strategy, it aims to bolster Europe's collective resilience against cyber threats and help to ensure that all citizens and businesses can fully benefit from trustworthy and reliable services and digital tools. Cyberspace should

[19] The discussion with operators was extended to Member States, with a technical round of bilateral discussions that took place between March and June 2021.

[20] SolarWinds, a major US information technology firm, was the subject of a cyberattack that spread to its clients and went undetected for months, giving hackers access to thousands of companies and government offices that used its products.

[21] Joint Communication to the European Parliament and the Council, The EU's Cybersecurity Strategy for the Digital Decade, JOIN (2020) 18.

remain global, open, stable and secure. The Strategy builds on three main pillars: (1) Resilience, technological sovereignty and leadership; (2) Building operational capacity to prevent, deter and respond; (3) Advancing a global and open cyberspace through increased cooperation. It addresses for the first time the cybersecurity of EU institutions, agencies and bodies. The Council has adopted Conclusions on the Strategy[22], endorsing its main strategic initiatives for implementation. The implementation of this Strategy is now under way and a detailed overview of where it stands is provided in a specific implementation report[23].

A key initiative announced in the Commission's Political Guidelines and followed up in the Cybersecurity Strategy is the establishment of a **Joint Cyber Unit**. Having consulted Member States, the Commission has adopted, together with this report, a Recommendation to better define the process, milestones and a timeline to set it up[24]. The Joint Cyber Unit will bring together all cybersecurity communities, i.e. civilian, law enforcement, diplomacy and defence. The Joint Cyber Unit will build on, and add value to, existing structures, resources and capabilities as a platform for secure and rapid operational and technical cooperation between EU entities and Member State authorities. It will also bring together all cybersecurity communities, i.e. civilian, law enforcement, diplomacy and defence. The Joint Cyber Unit will be set up in a 4-step process that will include the identification of the EU available operational capabilities, the preparation of incident and crisis response plans at national and EU levels, and expansion of activities to establish cooperation with private entities. The operationalisation of the Joint Cyber Unit is expected to be completed by 30 June 2023.

With the goal of further enhancing **detection capabilities** and leveraging AI-powered tools to shield the EU from cyber-attacks, Member States are currently increasing investments in **Security Operation Centres** (SOCs), thanks to funds under the Recovery and Resilience Facility. The Commission will complement Member States' efforts by allocating funds from the Digital Europe Programme.

Cybersecurity of 5G networks

As part of the Cybersecurity Strategy, the Commission identified three key objectives for the future work on the cybersecurity of 5G networks, given their central role in achieving the digital transformation of the EU's economy and society: (i) ensure further convergence in risk mitigation approaches across the EU, (ii) support continuous exchange of knowledge and capacity building, and (iii) promote supply chain resilience and other EU strategic security objectives. These objectives built on a report on 5G cybersecurity[25] that reviewed the intense joint work of Member States and the Commission, with the support of ENISA, the EU Agency for Cybersecurity, confirming that considerable progress has been made since the EU Toolbox of risk mitigating measures[26] was agreed. More details on the state of play of the implementation of the EU Toolbox are provided in the implementation report of the Cybersecurity Strategy[27].

---

22 Cybersecurity: Council adopts conclusions on the EU's cybersecurity strategy - Consilium (europa.eu)
23 JOIN(2021) 14.
24 C(2021) 4520.
25 SWD(2020)357.
26 https://digital-strategy.ec.europa.eu/en/library/cybersecurity-5g-networks-eu-toolbox-risk-mitigating-measures
27 JOIN(2021) 14.

A cybersecurity ecosystem

In order to help create an inter-connected, Europe-wide cybersecurity industrial and research ecosystem, the Regulation setting up the **Cybersecurity Competence Centre** and the **Network of National Coordination Centres**[28] was adopted in May 2021. It aims at strengthening European cybersecurity capacities, promoting research excellence and reinforcing the competitiveness of the Union's industry in this field[29]. The Commission is already working with the Romanian authorities preparing the establishment of the Centre in Bucharest. As part of the Action Plan on synergies between civil, defence and space industries[30], the Commission will seek to strengthen cross fertilisation between the work of the Centre, the European Defence Fund and the EU Space programme on cybersecurity and cyber defence.

The Cybersecurity Act[31] introduced in March 2021 an EU-wide **cybersecurity certification framework for ICT products, services and processes**. Companies doing business in the EU will benefit from being able to certify their ICT products, processes and services only once, with such certificates then being recognised across the European Union. The Commission has already asked ENISA to prepare three cybersecurity certification schemes: the European Common Criteria scheme, the European scheme for cloud computing services and the European scheme for 5G networks[32].

International dimension

The Cybersecurity strategy included proposals to further prevent, deter and respond to malicious cyber activities, by advancing responsible state behaviour by the EU's international partners in cyberspace[33]; by strengthening the Framework for a Joint EU Diplomatic Response to Malicious Cyber Activities (the cyber diplomacy toolbox)[34]; by stepping up EU cyber defence coordination and cooperation; and boosting cyber defence capabilities through the Cyber Defence Policy Framework[35]. The High Representative is currently preparing a review of these frameworks in consultation with the Commission and in line with the ambition of the Strategic Compass. In May, the European External Action Service (EEAS) organised a scenario-based discussion with Member States and international partners to improve the mutual understanding of diplomatic options to prevent, discourage, deter and respond to malicious cyber activities, and to identify opportunities for further strengthening international cooperation.

Beyond Europe, support for cybersecurity is being provided in the Eastern Neighbourhood, Africa, Asia, Latin America and the Caribbean through defined cooperation projects to mobilise European expertise to build cyber capacity and increase the security and resilience

[28] REGULATION (EU) 2021/887.

[29] It will do so in particular by deciding on and managing cybersecurity funds from the Digital and Horizon Europe Programs, as well as from Member States.

[30] COM (2021) 70 of 22.02.2021.

[31] Regulation 2019/881 of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification.

[32] The status of the schemes is described in the Union Rolling Work Programme.

[33] Notably by taking forward the proposal for a Programme of Action to establish a permanent infrastructure for concrete action to advance responsible state behaviour in cyberspace.

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

[35] Council Decision 14413/18.

of critical infrastructure and networks[36]. Through the Civilian CSDP Compact[37], cybersecurity has also been added as one of the priority areas for civilian CSDP missions.

To prevent cyber-surveillance technology being used in violation of human rights outside the EU, the new export regulation[38] supports a comprehensive modernisation of EU rules on exports of dual-use items[39]. The new Regulation provides a basis for the EU to implement effective controls on exports of cyber-surveillance technologies and to address security risks associated with the global trade in emerging technologies.

3. Protecting public spaces

In recent years public spaces in the EU have been the setting for unprecedented terrorist attacks on the public. Among the emerging risks for public spaces is the increasing spread of **drones**. Unmanned aircraft systems can be used by malicious actors to conduct surveillance, disrupt critical infrastructure operations or attack high-value targets. In April, the Commission adopted a **framework for the European unmanned traffic management concept** (the U-Space)[40], to make it easier for authorities to distinguish between cooperative and non-cooperative, potentially malicious, drones. The Commission is also supporting the development of guidance materials by the European Union Aviation Safety Agency, financing innovative counter-drone projects and studies, and building bridges between different affected sectors (law enforcement, aviation, critical infrastructure, prisons, customs/borders, personal protection, mass event organisers) and other stakeholders. A European Programme has been launched to facilitate a more coordinated approach to the testing of different counter-drone technologies.

Work is ongoing to develop guidelines to identify and mitigate vulnerabilities of public spaces and ensure security by design. A €20 million programme is under way under the Internal Security Fund-Police to enhance the **protection against terrorist threats of places of worship and other public spaces**, with a focus on large sports venues. In March, the Commission held a conference on the new projects starting in 2021. The Commission also supports national, regional and urban authorities and operators of public spaces in the exchange of good practice, the creation of networks and cooperation across the EU[41], through the EU Urban agenda and activities under the European Regional Development Fund[42].

The Action Plan on **rail security** adopted in 2018[43] listed concrete actions to improve passenger railway security and is now fully implemented. The EU Rail Passenger Security

---

[36] Examples include the 'Cyber4Dev', "EU4Digital" and 'EU CyberNet' projects.
[37] Doc Ref. 14305/18, 19 November 2018.
[38] Regulation setting up a Union regime for the control of exports, brokering, technical assistance, transit and transfer of dual-use items (recast), 19 May 2021.
[39] These are goods, software and technology that can be used for both civilian and military applications.
[40] Commission Implementing Regulations C(2021) 2671, C(2021) 2672, C(2021) 2673.
[41] For example, under the Urban Agenda for the EU, the Commission provided guidance and support for thematic and technical expertise to the Partnership for Security in Public Spaces to help implement its Action Plan. Interreg cross-border cooperation programmes co-financed by the European Regional Development Fund help security actors in neighbouring border regions to cooperate more effectively.
[42] https://ec.europa.eu/jrc/en/protection-public-spaces-from-terrorist-attacks/newsletter-protection-public-spaces
[43] COM(2018) 470.

Platform[44] adopted a number of best practice documents on risk assessment, insider threats, and detection technologies, fostering greater cooperation among Member States and stronger performance in the area of rail security.

III. Tackling evolving threats

1. Cybercrime

The impact of the pandemic on cybercrime[45]

Criminals have quickly capitalised on changes brought about by teleworking and increased use of online services, to adapt their illicit activities to the crisis context. The number of cyber-enabled and pandemic-related scams, using malware, ransomware and phishing attacks increased during the pandemic, targeting individuals, businesses, and the health sector in particular.

The circumstances of the pandemic provided new opportunities for fraud – shortages were exploited by fake web shops advertising and selling non-existent goods, including personal protective equipment and self-testing kits. With distribution of pharmaceutical goods shifting from the physical to online markets, fraudulent offers of COVID vaccines have even been found on the dark web.

The rise of the economic losses worldwide associated with cybercrime (expected to reach €5.4 trillion annually by 2021) reveals the need to develop secure applications and infrastructure that can anticipate and promptly react to an ever increasing menace. The Cybercrime Judicial Monitor published by Eurojust in May provides an overview of legislative developments and case law in the EU in relation to cybercrime and cyber-enabled crime[46].

Since strong cybersecurity is essential to stem the tide of cybercrime, full implementation by Member States of existing legislation is crucial. The Commission is constantly assessing the conformity of the transposition of the **Directive on attacks against information systems**[47]. In addition to the infringement proceedings previously initiated[48], the Commission opened new infringement proceedings (see Annex I of this report) concerning shortcomings in the transposition of the Directive. If necessary, the Commission will launch further proceedings. In parallel, the Commission supported Member States in the implementation of the Directive by organising a workshop on 23 February 2021 on best practice for the recording, production and publication of statistical data on reporting, prosecutions and convictions for cyberattack offences as defined in the Directive. A fully transposed Directive on attacks against information systems is crucial to disrupt criminal networks and activities such as the current rise in ransomware attacks. EU commitment in this area has been publicly underlined at both

[44] The EU Rail Passenger Security Platform is composed of Member States' authorities competent in the field of rail security and of interested stakeholders. As the mandate of the Platform expired in June 2021, the implementation of the results of the action plan on rail security will continue through a working party dedicated to rail security within the Expert group on land transport security (LANDSEC).

[45] EU Serious and Organised Crime Threat Assessement (SOCTA) Report 2021, Europol.

[46] Eurojust, Cybercrime Judicial Monitor, Issue 6 – May 2021, retrieved on 7 June 2021.

[47] Directive 2013/40/EU on attacks against information systems and replacing Council Framework Decision 2005/222/JHA.

[48] Infringement cases against Bulgaria, Italy, Portugal and Slovenia were opened in 2019.

the NATO[49] and G7[50] meetings held in June, to work with like-minded countries to address the escalating shared threat from criminal ransomware networks.

Combating child sexual abuse
Child sexual abuse is an area of increasing concern, where crime on and offline are often linked.

The COVID-19 pandemic and child sexual abuse

There are many reports providing evidence that the pandemic exacerbated abuse, especially of children who live with their abusers[51]. The pandemic has also seen a significant increase in 'self-generated' visual material, part of it resulting from online abuse where an offender lures or pressurises the child into producing that material[52].

In line with the **EU Strategy for a more effective fight against child sexual abuse**[53] **and the EU Comprehensive Strategy on the Rights of the Child**[54]**,** the Commission is now working on the specific initiatives identified to promote proactive, multi-stakeholder action in all relevant areas, covering prevention, support to enforcement, and assistance to victims.

In April, the European Parliament and the Council found a provisional political agreement on the Commission's proposal for **temporary legislation** to ensure that online service providers can continue their voluntary practices to detect and report child sexual abuse online, and to remove child sexual abuse material from their systems, provided their practices are lawful. These interim rules will be replaced in due course by longer-term legislation with detailed safeguards to fight child sexual abuse more effectively. This initiative has been the subject of an open public consultation and an impact assessment.

The Commission is currently monitoring the implementation of the **Directive on combating the sexual abuse and sexual exploitation of children and child pornography**[55]. Following the infringement procedures launched in 2019 against 23 Member States, the Commission is continuing its assessment and may initiate additional actions in the second half of 2021. The Commission also expects to close a number of procedures in the coming months as several Member States have been bringing their national legislation into full compliance with the Directive.

[49] NATO Brussels Summit Communiqué, 14 June 2021.
[50] G7 SUMMIT COMMUNIQUÉ, Our Shared Agenda for Global Action to Build Back Better, 13 June 2021.
[51] See Europol report of 19 June 2020, and NetClean (14 April 2021). According to reporting of the US National Centre for Missing and Exploited Children, the number of child sexual abuse reports globally in April 2020 were four times the figure of April 2019). See also WePROTECT Global Alliance, World Childhood Foundation, Unicef, UNDOC, WHO, ITU, End Violence Against Children and UNESCO, April 2020.
[52] See reports from Internet Watch Foundation, 12 January 2021; and Europol's serious and organised crime threat assessment of 12 April 2021.
[53] Communication from the Commission EU strategy for a more effective fight against child sexual abuse, COM(2020) 607.
[54] COM(2021) 142.
[55] Directive 2011/93/EU on combating the sexual abuse and sexual exploitation of children and child pornography.

To support law enforcement authorities and foster multi-stakeholder coordination, the Commission has initiated work to set up a **prevention network** of practitioners and researchers, to increase cooperation and exchange of best practice between all relevant actors. This contributes to raising global standards for the protection of children against sexual abuse, by promoting cooperation through the WePROTECT Global Alliance to End Child Sexual Exploitation Online, and through dedicated funding.

Online investigations and electronic data

To bring cybercriminals to justice, it is essential to ensure access to digital evidence that may provide investigative leads. While some Member States have established **data retention** frameworks for the retention and use of electronic communications metadata for law enforcement purposes, these measures raise important questions in relation to their potential interference with fundamental rights, including the right to privacy and protection of personal data. The Court of Justice of the European Union has been providing important clarifications and guidance[56]. In March, the Court delivered another ruling[57] relating to the national legislation of Estonia and reaffirmed previous case law. Also in March, the European Council[58] called for measures "better exploiting the potential of data and digital technologies for the benefit of society, the environment and the economy, while upholding relevant data protection, privacy and other fundamental rights and ensuring the retention of data necessary for law enforcement and judicial authorities to exercise their lawful powers to combat serious crime." In response to these recent developments, the Commission announced in the EU Strategy to tackle Organised Crime[59] that it would analyse and outline possible approaches and solutions, in line with the Court's judgements, which respond to law enforcement and judiciary needs in a way that is operationally useful, technically possible and legally sound, including by fully respecting fundamental rights. It is now consulting Member States with a view to devising the way forward.

Another key element to tackle cybercrime more effectively and ensure a more efficient prosecution is legislation on **cross-border access to electronic evidence**. Since the first Security Union Progress Report, negotiations with the co-legislators on the Commission proposal[60] have gained new momentum, as the European Parliament adopted its position in December 2020. On that basis, the European Parliament and the Council commenced trilogue discussions. Rapid adoption of efficient measures in line with the objective of the proposals will help law enforcement and judicial authorities obtain swift access to electronic evidence needed for criminal investigations.

To help prevent the increase of cybercrime and enable secure cross-border transactions over the internet, trust services and electronic identification play a key role. The proposal for a **European Digital Identity framework** adopted on 3 June aims to provide trusted digital identities for all EU citizens, residents and businesses. The framework will provide for the

[56] In judgments in Case C-623/17, Privacy International and Joined Cases C-511/18, C-512/18 and C-520/18 La Quadrature du Net a.o. of 6 October 2020, the CJEU confirmed its previous jurisprudence, that electronic communications data are confidential and that, in principle, traffic and location data cannot be retained in a general and indiscriminate manner. At the same time, it identified certain situations where retention is permissible, based on clear and proportionate obligations laid down in law and subject to strict substantive and procedural safeguards.

[57] Judgment in Case C-746/18 *Prokuratuur*.

[58] Statement of the Members of the European Council, SN 18/21 of 25.03.2021.

[59] Organised Crime Strategy 2021-2025, COM(2021) 170 of 14.04.2021.

[60] COM/2018/226 and COM/2018/225.

highest available security standards, addressing threats by fraud and identity theft and ensure full, user-friendly control by citizens and other holders of such identities of how much of their data is provided for any given transaction. The framework will be underpinned by a common technical architecture based on state of the art standards.

The deadline for the application of the Regulation on strengthening **the security of identity cards and residence documents** is 2 August 2021. Most Member States are on track and will issue identity cards and residence documents in the new format[61].

International dimension
Given the global nature of cybercrime, efforts at the international level are essential to find more effective approaches.

The negotiations for the Second Additional Protocol to the Council of Europe '**Budapest' Convention on Cybercrime** aim to enhance existing rules for cross-border access to electronic evidence for criminal investigations. In May 2021, the Parties to the Convention finalised the discussions and the draft Protocol will now be examined by relevant committees in the Council of Europe. Formal conclusion is expected still this year allowing for the subsequent signature and ratification of the Protocol. The Commission will work with the European Parliament and the Council to enable Member States to sign and ratify the Protocol as soon as possible.

The Protocol also includes provisions that will facilitate access for authorities to domain name registration data (also known as "**WHOIS information**") for criminal investigations. In this regard, the Commission also participates in the development and implementation of multi-stakeholder policies for the collection of and access to domain name registration data at the level of the Internet Cooperation for Assigning Names and Numbers (ICANN). These processes should be consistent with the relevant provisions in the revised NIS directive proposal, which includes provisions to ensure the collection and disclosure of accurate domain name registration data for legitimate access seekers, including law enforcement.

One important action in terms of international cooperation is the Global Action on Cybercrime Extended' (GLACY+). This would strengthen the capacity of countries worldwide to apply legislation on cybercrime and electronic evidence, based on the Budapest Convention, and enhance their capacity for effective cooperation in compliance with international human rights standards and the rule of law. The project is supporting 16 priority countries[62]. It will also work to connect criminal justice practitioners with policy-makers and legislators, to ensure stronger political support to the Budapest Convention.

---

[61] A limited number of Member States have signalled delays, mainly linked to the pandemic, but there are also reasons linked to substantial delays like tendering procedures challenged at Court.

[62] For instance, the Council of Europe is being supported by the European Neighbourhood Instrument to implement the project CyberSouth, which aims to strengthen legislation and institutional capacities on cybercrime and electronic evidence in the Southern Neighbourhood in line with human rights and the rule of law. A similar project - CyberEast - is implemented by the Council of Europe in the Eastern Partnership region. Another Council of Europe project funded under the Instrument for Pre-Accession works in the Western Balkans and Turkey to further strengthen the capacity of authorities in the Western Balkans and Turkey to search, seize and confiscate cybercrime proceeds, to prevent money laundering on the Internet and to secure electronic evidence.

2. Modern law enforcement

New technologies bring significant opportunities in the area of security. Integrating Artificial Intelligence (AI), Big Data and High Performance Computing (HPC) into security policy without weakening the effective protection of fundamental rights is essential to increase safety and security.

Artificial Intelligence can offer tools to support law enforcement authorities in their fight against crime and terrorism, keeping pace with the fast developing technologies used by criminals and their cross-border activities. The recent Commission Communication on fostering a European approach to Artificial Intelligence[63] sets out how AI can make a major contribution to the Security Union Strategy, as a strategic tool to both counter current threats and to anticipate future risks and opportunities. In April, the Commission made a proposal for harmonised rules (the "AI Act")[64] which aims to turn Europe into the global hub for trustworthy AI. An important part of these proposals focuses on high-risk AI systems that pose significant risks to the health and safety or fundamental rights of individuals. The AI Act would provide that the use of real-time remote biometric identification in publicly accessible spaces for the purpose of law enforcement is in principle prohibited, with tightly framed exceptions. These kinds of high-risk systems must comply with a set of horizontal mandatory requirements for trustworthy AI, including traceability, transparency and human oversight, and accuracy. The AI Act would have a significant impact in the area of law enforcement and border controls. It seeks to create a balanced framework of oversight throughout the life-cycle of high-risk systems used by law enforcement authorities, and puts in place a set of safeguards for the protection of fundamental rights.

The European Security Data Space for Innovation under the **Digital Europe Programme** aims to increase trust in the use of AI by law enforcement, by creating, making accessible and sharing high quality datasets to train, test and validate algorithms, an essential precondition to create AI ecosystems of excellence and trust. The importance of creating common data spaces was recognised by the European Council in March.

High Performance Computing (HPC) is a critical capability to enable key technologies like AI and data analytics to exploit the enormous potential of big data. Supercomputing simulations are central to enhancing the safety of products and services (notably through modelling), as well as for national security, defence and technological autonomy. Supercomputers are essential for uses from cybersecurity to nuclear simulation, and the combination of HPC and AI will be a game changer in defence and security. The inauguration of the European High Performance Computing Joint Undertaking[65] headquarters in May was an important step towards providing fast access to EuroHPC supercomputing resources when essential for security and defence.

The role of encryption

Encryption is a crucial technology in the area of security, essential to secure digital systems and transactions as well as protect fundamental rights, including freedom of expression,

[63] Communication "Fostering a European approach to Artificial Intelligence", COM(2021) 205.

[64] COM(2021) 206.

[65] The EuroHPC Joint Undertaking was established in 2018 to enable the EU to become a world leader in supercomputing. A new regulation is currently being discussed at EU level and is expected to enter into force in next months.

privacy and data protection. As shown by the recent EncroChat[66] and Sky ECC[67] operations, criminals exploit encrypted communications and the EU law enforcement authorities need to continuously develop their capacity to deal with encrypted information in the context of criminal investigations, while respecting applicable laws. In December 2020 Europol's new decryption facility was launched. Set up to ensure the respect of fundamental rights and to avoid limiting or weakening encryption, this initiative is available to national law enforcement authorities of all Member States to help keep societies and citizens safe and secure.

In December 2020, the Council called for an active discussion with the technology industry and development of a regulatory framework that would allow national authorities to carry out their operational tasks effectively while protecting privacy, fundamental rights and the security of communications[68]. In the EU Strategy to tackle Organised Crime[69], the Commission set out its intention to propose a way forward in 2022 to address the issue of lawful and targeted access to encrypted information in the context of criminal investigations and prosecutions, without weakening encryption or leading to indiscriminate surveillance. A first step is a thorough mapping of how Member States deal with encryption together with a multi-stakeholder process to explore and assess legal, ethical and technical options.

Judicial cooperation

An adequate response to the security challenges also requires **modernising judicial cooperation** between EU countries through the use of digital technology. Work is ongoing on a legislative proposal for the digitalisation of EU cross-border judicial cooperation. This will set up a digital communication channel between the competent authorities of the Member States and, where appropriate, EU agencies. The purpose is to leave behind paper-based communication between authorities and to ensure that data exchanges take place swiftly, securely and efficiently. A public consultation[70] indicated support for the approach from the public and stakeholders.

3. Countering illegal content online

The Security Union Strategy highlighted that security of both online and physical environments requires constant effort to counter illegal content online, and decisive steps forward have been taken during the reporting period. The long-awaited Regulation to address the **dissemination of terrorist content online** was adopted by the European Parliament and the Council[71], and will be fully applicable from June 2022. It will enable Member States to

[66] In 2020, a Europe-wide investigation brought to the dismantling of an encrypted phone solution used by organised crime groups.

[67] On 10 March 2021 Eurojust supported joint operations carried out by the judicial and law enforcement authorities of Belgium, France and the Netherlands to block use of encrypted communications by large-scale organised crime groups. Investigators managed to monitor the criminal use of the Sky ECC communication service tool. This provided invaluable insights into hundreds of millions of messages exchanged between criminals, allowing access to crucial information on over a hundred of planned large-scale criminal operations, preventing potential life threatening situations and possible victims.

[68] Council Resolution on Encryption - Security through encryption and security despite encryption, 13084/1/20 REV 1.

[69] Communication from the Commission on the EU Strategy to tackle Organised Crime 2021-2025, COM(2021) 170.

[70] https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12547-Digitalisation-of-justice-in-the-European-Union-_en

[71] Regulation (EU) 2021/784 of 29 April 2021 on addressing the dissemination of terrorist content online.

send removal orders to certain host service providers offering services in the EU and to remove within one hour material that incites or advocates commitment of terrorist offences, promotes the activities of a terrorist group or provides instructions or techniques for committing terrorist offences. It also provides for safeguards to strengthen accountability and transparency concerning measures taken to remove terrorist content, and to guard against erroneous removals of legitimate speech online.

The **Digital Services Act** (DSA) proposed by the Commission in December 2020 includes measures to counter illegal goods, services and content distributed online. It would empower users to report illegal content online and create a privileged channel for trusted flaggers to report illegal content with priority. In addition, it would require online platforms to notify suspicions of certain serious criminal offences to the competent law enforcement authorities; and includes rules for very large online platforms to carry out annual risks assessments and take mitigation measures in relation to significant systematic risks of dissemination of illegal content. The DSA proposal builds on voluntary initiatives like the **Code of Conduct on illegal hate speech** as valuable tools to tackle specific forms of illegal content.

The challenges of addressing illegal content online, including child sexual abuse material, were the heart of the discussions of the EU Internet Forum Ministerial meeting in January 2021, bringing together EU Member States and tech companies. Within the framework of the EU Internet Forum, the Commission has set up an expert process with industry, academia, public authorities and civil society organisations, to identify technical solutions that would allow companies to detect child sexual abuse online in end-to-end encrypted electronic communications whilst still safeguarding fundamental rights, including privacy and confidentiality of communications. Work is also underway to develop an EU list of violent right-wing extremist groups and symbols to support tech companies in their decisions on moderating content, given the problems raised in these discussions concerning the identification of extremist material.

4. Hybrid threats

Geopolitical tensions, including over new technologies, are leading to increased global security threats, fragmentation and a permanent battle of narratives. State and non-state actors increasingly misuse technologies to advance their objectives, threatening our societies, economy and security, and harming human rights and fundamental freedoms. The pandemic has made the EU and its Member States more vulnerable to hybrid threats, including via the intensified spread of disinformation and manipulative interference.

Health and resilience to hybrid threats

The pandemic has highlighted the weakness of emergency preparedness and response mechanisms at EU level. Both public and private capacities in the field of preparedness and crisis management, particularly regarding medical countermeasures, are fragmented, dispersed and sub-optimal when compared to other global players (e.g. US, China). This fragmentation provides a fertile ground for hybrid threats perpetrated by state and non- state actors. As presented in the Communications on 'Building a European Health Union: Reinforcing the EU's resilience for cross-border health threats'[72] and on 'Drawing the early

[72] COM(2020)724.

lessons from the Covid-19 pandemic'[73], the future European Health Emergency and Response Authority (HERA) would play a critical role in strengthening overall resilience ensuring a solid framework for EU preparedness, surveillance, risk assessment, early warning and response to all serious cross-border threats to health.

A review of the EU crisis management mechanisms is now under way, closely linked to the **EU operational protocol for countering hybrid threats (EU Playbook)**. A first step in this process was to reinforce and expand the hybrid points of contact network across Commission services, the European External Action Service, and the European Defence Agency. Another element for mainstreaming hybrid considerations into policy making is the inclusion of hybrid threats assessment of policy initiatives under Better Regulation.

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 continues, and the state of implementation is covered in the fifth annual report[74] on countering hybrid threats. The report describes progress on the creation of a restricted online platform for Member States' and EU institutions' easy reference on counter-hybrid tools and measures at EU level, measures to enhance situational awareness, in particular through the EU Hybrid Fusion Cell, and the identification of sectorial resilience baselines.

Countering increasingly complex and destructive hybrid and cyber threats remains an area of key importance of **EU-NATO cooperation**. This is also reflected in the recent NATO Brussels Summit Communiqué[75]. This cooperation has continued at a steady pace, building upon the achievements and keeping the momentum of the previous reporting periods. Key deliverables have been presented in the sixth Joint EU-NATO progress report[76]. The membership of the European Centre of Excellence for Countering Hybrid Threats in Helsinki (Hybrid CoE) continued to grow, with 30 EU Member States and NATO Allies having now joined the Centre. During the reporting period, the Hybrid CoE facilitated a number of scenario-based discussions, workshops and exercises.

Through the Civilian CSDP Compact[77], hybrid threats have also been added as a priority area for civilian CSDP missions. A corresponding mini-concept on civilian CSDP support to countering hybrid threats[78] has been drafted. The document proposes to (1) prioritise the protection of missions against hybrid attacks and (2) where appropriate, assist the host State in increasing resilience against hybrid threats.

One important part of hybrid threats is **disinformation**. The European Democracy Action Plan[79] identified several actions to strengthen the response to foreign information manipulation and interference[80]. The European Council welcomed the approach of the EDAP

[73] COM(2021) 380.
[74] SWD(2021)729.
[75] NATO Brussels Summit Communiqué, Brussels 14 June 2021.
[76] Sixth progress report on the implementation of the common set of proposals endorsed by EU and NATO Councils on 6 December 2016 and 5 December 2017, 3 June 2021.
[77] Doc Ref. 14305/18, 19 November 2018.
[78] Doc. Ref. 8077/20, 20 May 2020.
[79] COM (2020) 790.
[80] Three core areas are 1) to further sharpen the terminology that describes the challenge; 2) develop a common methodology and framework to collect systematic evidence of foreign information manipulation and

and the Council has also called to deepen EU action[81]. The EEAS is working closely with the Commission to take this forward, drawing on the EU Rapid Alert System to bring together the community of experts to set up a strong, robust, flexible and comprehensive framework against foreign information manipulation and interference. This is also supported by the Code of Practice on Disinformation online, and in May this was strengthened through Guidance on how participating online service providers and other relevant stakeholders should step up their measures to address gaps and shortcomings of the Code of Practice and create a more transparent, safe and trustworthy online environment[82].

IV. Protecting Europeans from terrorism and organised crime

1. Terrorism and radicalisation

The attacks of late 2020 showed that it as crucial as ever to address terrorism as well as its root causes. Adopted in December 2020, the new **Counter-Terrorism Agenda for the EU**[83] set out how to step up the fight against terrorism and violent extremism and boost the EU's resilience to terrorist threats. Its implementation is well under way. In addition, the Commission is evaluating Directive (EU) 2017/541 on combating terrorism, which sets minimum rules for the criminalisation of terrorist and related offences as well as sanctions, and for the protection, assistance and support of victims of terrorism.

At the end of 2020, the Commission awarded a new framework contract to a consortium for the **Radicalisation Awareness Network** (RAN) Policy Support, complementing the work of the RAN Practitioners, and to continue supporting policy makers on general prevention issues. It aims to enhance Member States' knowledge and capacities on strategic communications as well as the evidence base for further policy development, concrete approaches and interventions.

In addition, the Commission is working with Member States to combat extremist ideologies that may lead to violent extremism. In 2021, this work focuses on inter-linkages between all kinds of violent extremist ideologies (including left-wing, right-wing and Islamist extremism) and on radicalisation leading to self-segregation. Several awareness-raising initiatives have taken place in this area over the last few months. The activities of the RAN have been expanded to the Western Balkans through a dedicated contract which started in January 2021.

Another priority is avoiding terrorists' acquisition of materials that can be weaponised. The 2017 Action Plan on **chemical, biological, radiological and nuclear (CBRN)** material has been taken forward through a study looking at the feasibility of restricting access to the some high-risk chemicals, finalised in June 2021. The Commission has also launched preparatory work for cross-border exercises and workshops on the security of radioactive and biological sources in hospital and laboratories, to take place in 2022. The implementation of the CBRN Action Plan is supported by projects co-financed by the Internal Security Fund, which

interference and 3) to further develop the EU's toolbox for countering foreign information manipulation and interference to make it better fit for purpose to impose costs on perpetrators.

[81] March 2021 Statement from the European Council; Council Conclusions of December 2020.

[82] COM(2021) 262. The Guidance also specifically addresses the COVID-19 infodemic.

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

selected initiatives like the Safe Stadium project[84], looking at CBRN protection and preparedness in large sport arenas such as football stadiums. New legislation on the marketing and use of explosives precursors came into force on 1 February 2021. Implementation is well under way and the Commission continues to assist all stakeholders with fulfilling their obligations.

Part of the intrinsic link between the external and internal security of the Union is working together on threats such as CBRN. EU external financing instruments support efforts to enhance global, and regional governance and cooperation on CBRN risk detection and mitigation, building on the positive experience gained for instance through the EU CBRN Risk Mitigation Centres of Excellence Initiative and through the Export Control Programme for Dual-Use Goods. To date, 34 countries have drafted a CBRN national action plan and 10 countries officially adopted it.

Health and terrorism

EU4Health[85] is supporting actions to prevent, prepare and respond to cross-border health threats.

The third EU Health Programme co-funds "**Health preparedness against terror attack"**[86], a Joint Action with EU Health authorities, launched in May 2021. Its objectives are to protect EU citizens from intentional health crisis, by addressing the gaps in health preparedness and strengthening cross-sectoral work (health, security & civil protection sectors), in response to a biological and/or chemical terror attack.

The Health Programme 2017-2021 has supported health sector preparedness and response capacities against Chemical and biological threats. The **Strengthened International Health Regulations and Preparedness in the EU**[87] hosts a network of reference laboratories for highly pathogenic agents, that includes 41 laboratories.

Addressing the threat posed by returning **foreign terrorist fighters** (FTFs) in Syria and Iraq remains an important element of counterterrorism, and a priority in preventing radicalisation. As agreed in the Strategic Orientations on a coordinated EU approach to prevention of radicalisation for 2021, the Commission has been working on four main priorities: child returnees, strengthening and securing the return process (repatriation, prosecution and reintegration), the skills of professionals involved in the reintegration of child returnees, and female returnees. In relation to the prisons and IDP camps in North-East Syria, and in agreement with the Member States, the EEAS and the Commission are exploring new ways to enhance assistance in the region to help improve living conditions and try to halt radicalisation.

[84] https://ec.europa.eu/info/funding-tenders/opportunities/portal/screen/opportunities/projects-details/31077817/101034226/ISFP

[85] Established by Regulation (EU) 2021/522.

[86] Health preparedness against terror attack Joint Action, https://ec.europa.eu/chafea/health/funding/joint-actions/documents/ja-2019-presentation-03_en.pdf

[87] The Strengthened International Health Regulations and Preparedness in the EU (SHARP JA), https://sharpja.eu/wp7/

The Commission recently concluded the update of the Counter-Terrorism and Preventing/Countering Violent Extremism data analysis. The mapping showed that the scale and speed of financing from EU external financing instruments in such activities has been impressive[88]. As of 1 January 2021, a total number of 99 actions to anticipate, prevent, respond and protect against Counter-Terrorism in countries outside the EU, totalling €501 million were ongoing (an 8% increase to the previous year) delivering on the priorities of the EU Counterterrorism Agenda and Council Conclusions on Counterterrorism.

Further steps were taken to develop and strengthen counterterrorism partnerships and cooperation with countries in the Neighbourhood and beyond, drawing on the expertise of the network of EU Counter-Terrorism/Security Experts. In recent months, the implementation of the Joint Action Plan on Counter-Terrorism with the Western Balkan partners has progressed, with some delays due to the pandemic and internal political dynamics of the partners.

The EU has continued to use its counter-terrorism sanctions framework in the reporting period. In February 2021, the Council finalised the review of the EU terrorist list[89] and a new designation was adopted under the EU autonomous ISIL (Da'esh)/Al-Qaida counter-terrorism sanctions regime in April 2021[90].

Finally, in May 2021, Eurojust and the European Network co-organised the 6th EU Day against Impunity, with a focus on core international crimes committed in Syria by terrorist organisations and the Syrian regime. It built upon the work undertaken since last year to support cumulative prosecution of FTFs for terrorism-related offences and international crimes. It further demonstrated that strengthened judicial cooperation between Member States is key for the identification and prosecution of war criminals present in the EU.

2. Fighting organised crime

The 2021 Serious and Organised Crime Threat Assessment (SOCTA 2021) report[91] shed light on the continued threat of organised crime and its increasing complexity. Organised crime is transnational: 65% of organised crime groups are composed of members of multiple nationalities and seven out of ten are active in more than three countries. The organised crime landscape in the EU is characterised by a networked environment where different groups cooperate with each other and with providers of criminal services. 60% of criminal networks employ violence as part of their criminal businesses, but virtually all criminal activities now feature some online component. The risk of organised crime infiltration into the legal economy is also on the rise: it is estimated that more than 80% use legal business structures for criminal activities.

---

88 The EU provides substantial support to all the Global Counterterrorism Forum Initiatives including the Institute for Justice and the Rule of Law, and to the Global Community Engagement and Resilience Fund (GCERF) in order to support Preventing/Countering Violent Extremism activities in a number of countries of strategic importance to the EU.

89 Council Decision (CFSP) 2021/142 of 5 February 2021 updating the list of persons, groups and entities subject to Articles 2, 3 and 4 of Common Position 2001/931/CFSP.

90 Council Decision (CFSP) 2021/613 and Implementing Regulation (EU) 2021/612 and of 15 April 2021 concerning restrictive measures against ISIL (Da'esh) and Al-Qaeda and persons, groups, undertakings and entities associated with them.

91 https://www.europol.europa.eu/activities-services/main-reports/european-union-serious-and-organised-crime-threat-assessment

Criminals exploiting the economic vulnerabilities created by the pandemic

Learning from previous crises, it can be anticipated that a volatile economic situation with growing poverty and social inequality will serve as a breeding ground for organised and serious crime.

Businesses operating in sectors suffering particularly negative economic pressures, such as the hospitality, catering and tourism sectors, are becoming more vulnerable to criminal infiltration[92].

In 2020, Europol Serious and Organised Crime Centre (ESOCC) received and processed more than 35,183 operational contributions in the seven areas covered by the Centre[93], representing more than half (57%) of operational contributions of Europol. ESOCC supported Member States in 837 operations, a 41% increase in comparable terms in relation to 2019. These figures reflect the increased activity of organised crime groups and the increasing demand by Member States for Europol's support in this area. ESOCC organised and coordinated 11 Operational Task Forces (OTF) coordinating intelligence and investigative efforts against 60 High Value Targets (HVT), suspected members of criminal organisations posing a particularly high risk, 21 of whom were arrested.

To help respond to the mounting challenges, in April the Commission adopted the **EU Strategy to tackle Organised Crime** (2021-2025)[94]. This sets out priority actions to boost law enforcement and judicial cooperation, ensure effective investigations to disrupt organised crime structures and tackle high priority crimes, targeting the profits generated by organised crime and making law enforcement and the judiciary fit for the digital age. The Commission also published the "European Multidisciplinary Platform against Criminal Threats" (EMPACT)[95]. This sets out how to use EMPACT to its full potential and turn it into a flagship instrument for multidisciplinary and multiagency operational cooperation to fight organised crime. Additionally, the Commission is closely involved in the ongoing preparation of the next EMPACT cycle, which will cover the period from 2022 until 2025.

Fight against trafficking in human beings

Trafficking in human beings is a highly profitable crime that brings enormous profit to criminals at the expense of the victims and society as a whole. In April, the Commission adopted the EU Strategy on combating trafficking in human beings (2021-2025)[96]. As trafficking in human beings is often conducted by organised groups, this Strategy is closely linked to the EU Strategy to tackle Organised Crime. The anti-trafficking strategy proposes legal, policy, and operational initiatives to combat human trafficking from prevention to

[92] Based on the contribution by the Working Group on COVID-19 criminal threats and law enforcement responses 1st meeting; Europol 2020, Enterprising criminals: Europe's fight against the global networks of financial and economic crime.

[93] Migrant smuggling, High risk organised crime groups, environmental crime, organised property crime, drugs, trafficking in human beings and weapons and explosives.

[94] COM(2021) 170.

[95] 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. It brings together different stakeholders to improve and strengthen co-operation between Member States, EU institutions and EU agencies as well as third countries and organisations, including the private sector, where appropriate (SWD(2021) 74).

[96] Communication from the Commission on the EU Strategy on Combatting Trafficking in Human Beings 2021-2025, COM (2021) 171.

conviction of criminals, emphasising the protection of victims at all stages, taking into account in particular women and child victims, as well as trafficking for sexual exploitation. The focus is on reducing demand that fosters trafficking; breaking the criminal model to halt victims' exploitation; protecting, supporting and empowering the victims and addressing the international dimension of this form of crime. This followed a report from Eurojust setting out 18 recommendations to support Member States not only in the investigation, prosecution and judicial cooperation in trafficking cases but also in the identification, rescue and protection of victims[97].

Fight against illicit drugs

Following the adoption of the EU Drugs Strategy 2021-2025, discussions on the related Action Plan are continuing, with a view to adoption in Council by the end of the Portuguese Presidency. The legislation on new **psychoactive substances** (NPS), which became fully effective in November 2018, has been followed up with a delegated act to include two new psychoactive substances in the definition of drugs[98].

The Eurojust Report on Drug Trafficking of April 2021[99] emphasises the rise in production of synthetic drugs and in the use of darknet for their sale, which pose legal challenges for prosecutors in the EU. The report gives recommendations to increase financial investigations, asset recovery and judicial cooperation, including with third countries. In March 2021, on the occasion of the annual EU-US Dialogue on Drugs, Eurojust presented key issues and examples of successful judicial cooperation in drug trafficking cases between the Member States and the US. The first meeting of the EU-China Dialogue on Drugs took place on 22 January 2021, and included cooperation on the fight against drugs. The EU participated in the 64th UN Commission on Narcotic Drugs and reiterated its calls for accelerating of the implementation of the comprehensive commitments the international community made to address the world's drug situation.

Fight against illegal firearms trafficking

The codified Firearms Directive[100] came into force in April 2021 and the Commission followed up with rules on the systematic exchange, by electronic means, of information relating to refusals to grant authorization to acquire or possess certain firearms[101]. These should apply as of 31 January 2022 and will allow national competent authorities to know whether an applicant for a firearm license has been denied a similar authorisation in another Member State. It will therefore prevent jurisdiction-shopping to circumvent prohibitions to own a firearm.

The Commission is also supporting a pilot project to establish real-time tracking of firearms-related incidents across the EU to develop a permanently up-to-date picture. To support the work of law enforcement authorities, the Commission is leading the action on the establishment and development of Firearms Focal Points at national level.

---

97 The report is available here: https://www.eurojust.europa.eu/eurojust-report-trafficking-human-beings

98 C(2021) 1570; the scrutiny period of the European Parliament and the Council will end in mid-May.

99 The report is available here: https://www.eurojust.europa.eu/eurojust-report-drug-trafficking.

100 Directive (EU) 2017/853 on control of the acquisition and possession of weapons.

101 Delegated Directive C(2021)3400 of 21 May 2021 laying down the detailed arrangements for the systematic exchange, by electronic means, of information relating to refusals to grant authorisations to acquire or possess certain firearms.

With respect to international cooperation, the Commission has actively supported the constructive involvement of Turkey within operational activities of EMPACT related to the threat of convertible alarm and signal weapons. It also helped put back the issue of firearms trafficking on the agenda of cooperation with Middle East and North African countries. The Commission has also been very active in operational cooperation with South-East Europe, including by preparing a joint operation between Member States and Western Balkan partners, and regional meetings of Small Arms and Light Weapons Commissions.

The EU's Global Illicit Flows Programme[102] has continued to be an effective mechanism for coordinating trans-regional action against organised crime and increasing the capacities of over 80 partner countries worldwide to disrupt trafficking of illicit goods, with a focus on narcotics and firearms. It has also supported EU agencies and EU Member States to have a wider law enforcement reach.

Fight against financial crime

As part of the fight against the risk of organised crime infiltration into the legal economy, Member States are required to transpose the 2019 Directive facilitating the use of financial and other information for the prevention, detection, investigation or prosecution of certain criminal offences[103] by August 2021. The Commission will closely monitor its transposition and effective application.

Two consultation meetings were held with Member States on the revision of the Asset Recovery Offices Council Decision[104] and the Confiscation Directive[105] in May and June 2021. The discussions underlined the added value of these instruments in enhancing asset recovery in the Union and the importance of an effective management of confiscated assets, in full respect of fundamental rights, as well as the need to improve cooperation throughout the entire asset recovery process.

New legislation on controls on cash entering or leaving the EU applies from 3 June 2021[106], and essential implementing rules establishing procedures and technical rules are in place since May[107]. Further implementing rules are under way establishing criteria for the common risk management framework on cash movements.

The European Public Prosecutor's Office (EPPO) took up its investigative and prosecutorial tasks on 1 June 2021. The EPPO has now started to investigate and prosecute crimes affecting the Union's financial interests. The crimes which EPPO investigates and prosecutes include VAT fraud connected with the territory of two or more Member States with a total

[102] https://illicitflows.eu/

[103] 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.

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

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

[106] Regulation (EU) 2018/1672 on controls on cash entering or leaving the Union.

[107] Commission Implementing Regulation (EU) 2021/776 of 11 May 2021 establishing templates for certain forms as well as technical rules for the effective exchange of information.

damage of at least €10 million. Each year, fraud causes Member States to lose billions of euros in VAT revenues.

Fight against environmental crime

The **Environmental Crime Directive** 2008/99/EC is the main legal instrument of the EU to protect the environment through criminal law. Extensive consultations are under way to revise the text to improve implementation and to strengthen the functioning of the law enforcement chain (detection, investigation, prosecution, criminal courts). Work on combating environmental crime is also taken forward through the Environmental Compliance and Governance Forum[108] whose meetings in January and June 2021 focussed on the revision of the Directive and combating environmental crime in general.

Fight against trafficking in cultural goods

EU legislation on the import of cultural goods aims to stop imports of cultural goods illicitly exported from their country of origin. Implementing provisions are now being put in place for a centralised electronic system for the Import of Cultural Goods (ICG), which will allow the storage and exchange of information between Member States and the accomplishment of import formalities. The general prohibition rule provided in the Regulation[109] entered into force on 28 December 2020 allowing Member States customs authorities to control and act on shipments which may contain cultural goods illicitly exported from their country of origin.

V. A strong European security ecosystem

1. Cooperation and information exchange

The Security Union Strategy set out how EU action can make a substantial contribution to addressing increasingly complex, cross-border and cross-sectorial security threats, by helping security actors in Member States with the tools and information they need.

Europol plays a central role in this regard. The Commission proposal adopted last December to modernise and reinforce **Europol's mandate**[110] addresses specific constraints Europol faces today – such as its dealings with the private sector. In addition, the Commission is proposing to enable Europol to enter alerts in the Schengen Information System on terrorists and other criminals based on third country sourced information. These will enhance Europol's ability to support Member States in countering serious crime and terrorism. The Commission looks forward to rapid conclusion by the European Parliament and the Council on their positions with a view to starting trilogues under the Slovenian Presidency.

The **EU and Interpol** already have long-standing and deep cooperation. Interpol is a key partner for the EU in the field of internal and external security, including countering terrorism and organised crime, as well as in integrated border management. The Commission has proposed negotiations to further enhance operational and strategic cooperation through a cooperation agreement[111].

[108] Compliance Assurance - Legislation - Environment - European Commission (europa.eu)
[109] Regulation (EU) 2019/880 of 17 April 2019 on the introduction and the import of cultural goods.
[110] COM(2020) 769, COM(2020) 791.
[111] COM(2021) 177.

On an operational level, preparations for the full implementation of the revision of the **Schengen Information System** (SIS) are ongoing with the aim to finalise all required testing activities by the end of 2021. In March 2021 Europol was connected to SIRENE[112] mail relay. At the end of 2020, most Member States had deployed the new SIS fingerprint search functionality[113].

Work has started on amending legislation to improve **Eurojust**'s ability to identify links between parallel proceedings in cross-border terrorism cases[114]. In parallel, Eurojust continued to provide operational follow-up and coordination based on information submitted through the European Judicial Counter-Terrorism Register (CTR), which was set up with the aim to identify links between judicial counter-terrorism proceedings in Member States. So far, the experience with the CTR points to a significant increase in the amount of information transmitted to Eurojust and some links between proceedings previously unknown to national authorities have already been detected. The CTR has also brought major improvements to information sharing in counter-terrorism proceedings.

Preparatory work has started on the establishment of the **Joint Investigation Teams (JIT) Collaboration Platform**. Consultations with Member States, JIT Network Secretariat, Eurojust, Europol and OLAF on the design of the collaboration platform are ongoing. Since April 2021, Eurojust also provides financial assistance to JITs for urgent and/or unforeseen actions outside the scope of the regular funding scheme[115].

Passenger Name Record (PNR) data is an important source of information to identify individuals posing security risks. Building on the information gathered to prepare for a review of the legislation[116], the Commission is helping Member States to enhance the use of PNR data and to deepen cooperation[117]. The majority of national Passenger Information Units are now fully operational and the processing of PNR data is an important tool for national law enforcement authorities in their fight against terrorism and serious crime, despite the decrease in the number of air passengers during the pandemic.

Work has also intensified on the international front. On 30 December 2020 the EU-UK Trade and Cooperation Agreement[118] was signed and is in force since May. It covers the exchange of PNR data and its use for the purposes of fighting terrorism and serious crime. The Commission adopted Reports[119] on the Joint Evaluations of the existing international agreements on PNR with US and Australia, as well as on the Joint Review of the EU-Australia Agreement. Overall, these reports confirmed the benefits of the use of PNR, its effectiveness in achieving the purposes sought, and the uniqueness of the information PNR

[112] Supplementary Information Request at the National Entries. Each EU country operating SIS has set up a national SIRENE Bureau, responsible for any supplementary information exchange and coordination of activities connected to SIS alerts.
[113] Automated Fingerprint Identification System.
[114] Council Decision 2005/671/JHA and Regulation (EU) 2018/1727.
[115] https://www.eurojust.europa.eu/eurojust-launches-new-scheme-urgent-jit-funding
[116] COM(2020) 305 looking at Directive (EU) 2016/681.
[117] Slovenia is the last Member State whose national measures transposing the PNR Directive are being assessed by the Commission, while all other Member States have fully transposed the Directive.
[118] OJ L 444, 31.12.2020, p. 309 – 319.
[119] COM(2021) 17 final ; COM(2021) 18 final; COM(2021) 19 final.

provides. In January 2021, the Council adopted the Union position[120] welcoming the adoption by the International Civil Aviation Organisation (ICAO) of a new set of Standards and Recommended Practices on PNR processing and protection. On 28 February 2021, the ICAO decision became operational and binding upon all ICAO members[121]; it now represents a strong baseline for the processing of PNR worldwide, in full respect of fundamental rights.

Negotiations for the exchange of personal data between Europol and certain third countries for fighting serious crime and terrorism are ongoing. The first two rounds of negotiations with New Zealand took place in a constructive atmosphere. Progress has also been achieved in the negotiations with Turkey and constructive talks have taken place with Tunisia. Exploratory discussions at technical level with a number of additional countries are ongoing.

The Council adopted in March 2021 the mandate for the Commission to start negotiations for Agreements between the EU and thirteen third countries[122] on cooperation between Eurojust and competent authorities for judicial cooperation in criminal matters. These international agreements will become an important cornerstone of the EU security legislation and globally contribute to better fight against organised crime.

Since 2012, the **European Criminal Records Information System (ECRIS)** ensures an efficient electronic exchange of criminal records information between Member States, with over 4 million messages exchanged yearly. The Commission has adopted a report on the working of ECRIS[123] and is currently following up its findings with the Member States. The work on the development and implementation of a centralised system for the identification of Member States holding conviction information on third country nationals (ECRIS-TCN) is under way, aiming to start operations in 2023. The new system will supplement ECRIS as regards the exchange of information on third country nationals convicted in the EU.

2. *The contribution of strong external borders*

Efficient management of the EU's external borders is key to ensure the security of citizens. The Commission's Schengen Strategy[124] includes actions in this field which would protect the integrity of the Schengen area and further improve its functioning. The new architecture for EU information systems for security, border and migration management is being developed to support national authorities. It is essential that Member States take the necessary steps without delay to meet the agreed implementation timeline in order to deliver on this ambitious project.

Work on the implementation of the **Interoperability Regulations** is progressing, with a view to full implementation by the end of 2023. EU-LISA is finalising the procurement of the different interoperability components and the Commission is working with experts on a guidance handbook. The preparations for the entry into operation of the **Entry/Exit System** (EES) are ongoing with the aim to finalise testing and training in early 2022 ahead of entry into operation in May 2022. Preparations are also ongoing for the **European Travel**

[120] OJ L 37, 3.2.2021, p. 6–9.
[121] Member States introduced a difference with regard to one part of the relevant Standards and Recommended Practices (SARP).
[122] Algeria, Armenia, Argentina, Bosnia and Herzegovina, Brazil, Colombia, Egypt, Israel, Jordan, Lebanon, Morocco, Tunisia and Turkey.
[123] COM(2020)778, SWD(2020)378, 21 December 2020.
[124] COM(2021)277.

Information and Authorisation System (ETIAS), with planned entry into operation of this system by the end of 2022. The European Parliament and the Council have now also agreed on the proposal to ensure the connection between ETIAS and the relevant EU databases.

In December 2020, the European Parliament and the Council reached a provisional agreement on the Commission's proposal to revise and upgrade the **Visa Information System** (VIS). Key benefits of the agreed changes include more thorough background checks on visa applicants, closing security information gaps through better information exchange between Member States, broadening the VIS to include long-stay visas and residence permits, and combatting trafficking by lowering the fingerprinting age for minors. Together with the other new and upgraded information systems, the new VIS should be operational and fully interoperable by the end of 2023.

The first teams of the **European Border and Coast Guard** standing corps have been successfully deployed since 1 January. The standing corps composed of 10,000 Frontex and national officers will significantly enhance border security, as it gradually increases in the coming years to reach its full capacity. The recently adopted implementing Regulation on the European Border Surveillance System (EUROSUR)[125] will further improve the situational awareness and increase reaction capability at the external borders for the purpose of detecting, preventing and combating illegal immigration and cross-border crime,

Customs controls
The Commission is currently preparing a new Customs Risk Management Strategy aiming to increase the structured approach to customs risk management, making controls more effective and reducing risks to the EU and its citizens, whilst ensuring competitiveness of legitimate EU business.

As part of the EU Strategy and Action Plan for strengthening customs risk management, the Commission is also developing the new customs advance cargo risk management system, enabling collaborative safety and security risk analysis before goods arrive in the EU or are loaded for transport to the EU[126].

3. Strengthening security research and innovation

Innovation should be considered as a strategic tool for the EU: it has horizontal effects on almost all the aspects of the security community, giving new ways to address the challenges posed by technologies, reducing strategic dependence and strengthening supply chains. This is why the EU is building its main research projects taking into account the security dimension, its needs and the role of private sector.

The development of the **European Innovation Hub for internal security** is ongoing. The **Horizon Europe** programme supports EU responses to security challenges, providing €1.6 billion in funding for 2021-2027. In March 2021, the Commission adopted the first Horizon Europe Strategic Plan, setting strategic orientations for the first four years: security research will serve as a tool to move from a reactive approach in the field of security to a proactive one, based on foresight and prevention. A new work programme 2021-2022 has been agreed

[125] Commission Implementing Regulation (EU) 2021/581.
[126] Release 1 covering air express and postal went live in March. Release 2 covering air general cargo is scheduled for March 2023. The third release involving maritime, road and rail is scheduled for 2024.

which will support the implementation of the internal security dimension of the Security Union Strategy, the border management and security dimensions of migration and asylum policies, and EU policies on disaster risk reduction.

EU funding presents further opportunities to reinforce European innovation at the interface between defence, space and civil uses. In February 2021, the Commission launched the Action Plan on Synergies between **civil, defence and space industries**[127]. Three flagship projects were identified (on drone technologies, space-based secure connectivity and space traffic management). The Action Plan will support the EU's security industries with state-of-the-art, innovative solutions deriving from the cross-fertilisation and efficient synergies between civil, defence and space industries.

Space technology, data and services have become indispensable in providing security for Europeans, and play an essential role in preserving many strategic interests. The **Space Programme Regulation**[128] adopted in April with a budget of €14.6 billion, introduces a new component for governmental satellite communication, providing the stepping stone for EU space-based secure connectivity.

4. Skills and awareness raising

Awareness of security threats and the skills to face them are essential to build a more resilient society with better-prepared enterprises/businesses, administrations and individuals. On 9 February 2021, the 18th Safer Internet Day took place online in 170 countries with Better Internet for Kids Youth Ambassadors and representatives of the industry Alliance. The EU Digital Education Action Plan (2021-2027) includes an action dedicated to helping teachers and educational staff to foster digital literacy and tackle disinformation. Guidelines will be developed and rolled out across the EU in September 2022.

A good knowledge of the digital environment and the development of related competences in the private and public sector is fundamental to a resilient and competitive society. Under the Digital Europe Programme, a first call for the European Digital Innovation Hubs (EDIHs)[129] was published in May, with the aim of having the first Hubs operational from early 2022. The EDIHs will help private and public actors by providing access to technical expertise and experimentation, stimulating the broad uptake of Artificial Intelligence, High Performance Computing (HPC) and Cybersecurity as well as other digital technologies by industry (in particular SMEs and midcaps) and public sector organisations in Europe.

In a constantly changing security landscape, law enforcement officials and justice professionals' skills should be continuously updated. An evaluation of **CEPOL** will conclude in the second half of 2021. The Commission adopted the European judicial training strategy for 2021-2024[130] at the end of 2020 and organised a conference of stakeholders with the Portuguese Presidency in May 2021 to boost training of judges and prosecutors.

---

[127] COM(2021) 70.
[128] Regulation (EU) 2021/696 of 28 April 2021 establishing the Union Space Programme and the European Union Agency for the Space Programme.
[129] https://digital-strategy.ec.europa.eu/en/activities/edihs
[130] COM(2020) 713.

Awareness raising is also at the centre of the EU Strategy on **victims' rights** (2020-2025), adopted in June 2020, that aims to ensure that all victims of crime, no matter where in the EU or in what circumstances the crime takes place, can fully rely on their rights. The first Plenary Meeting of the Victims' Rights Platform took place in February 2021. The Commission is also working on the evaluation of the Victims' Rights Directive and if necessary may propose legislative amendments in 2022.

5. The role of EU Agencies

The Security Union Strategy relies on a whole-of-society approach, bringing together all institutions, organisations and authorities with a role in the protection of our citizens. Beyond the support and expertise they provide to Member States, EU Agencies play a crucial role in fostering cooperation and information exchange between Member States' national authorities at operational level. Considering the multiplicity of new and emerging threats in the current landscape, synergies and coordination of the activities of EU agencies are to be further encouraged.

Europol

Europol's annual reports on organised crime (SOCTA), terrorism (TE-SAT) and internet-organised crime (IOCTA) provide key data and analysis to support policy and operational activities in the security area. Europol also contributes to enhancing the overall operational effectiveness of law enforcement by expanding its cooperation with third countries to counter crime and terrorism in coherence with other EU external policies and tools.

The Operational and Analysis Centre is Europol's information hub. The centre monitors operations and developments 24/7, sets up cooperation with non-EU countries and organisations and deploys experts on the ground. It also provides analysis to Europol's other centres and organisations. Europol's European Serious and Organised Crime Centre supports EU countries in their fight against international criminal networks involved in drugs, weapons and explosives, property and environmental crime. The centre also hosts the European Migrant Smuggling Centre, which targets and dismantles the complex and sophisticated criminal networks involved in migrant smuggling. Europol's European Financial and Economic Crime Centre is instead in charge of providing support when dealing with highly sophisticated cases of money laundering, scams and fraud, that target individuals, companies and the public sector.

Europol's contribution is also fundamental in coordinating the EU approach on counter-terrorism. Europol has continued to support Member States in investigations linked to terrorism through the European Counter Terrorism Centre (ECTC). Despite the restrictions caused by the pandemic, ECTC supported 776 counter-terrorist operations in 2020 (compared to 632 in 2019). The EU Internet Referral Unit in Europol has also continued to play a crucial role in monitoring the activity of terrorist groups online and the action taken by platforms, as well as in further developing the EU Crisis Response Protocol. Europol remains committed to support Member States in expanding their national capabilities in the prevention of online terrorist content, through the organisation of Targeted Referral Action Days.

Eurojust

During the first months of 2021, Eurojust supported several cross-border investigations and prosecutions against Organised Crime Groups specialised in fraud. It also ensured the seizure of companies' assets or the administrative closure of enterprises used for the fraud scheme[131]. Eurojust has supported major joint international operations to bring down cybercrime networks, including targeting the criminal groups operating a cross platform mobile application called Mobdro that facilitated the streaming of illegally obtained audio-visual works, including football matches[132], or one of the most dangerous malware (EMOTET) deployed to open up the victim computers for third party infections[133]. Eurojust also engaged with judicial practitioners to help mapping legal and operational challenges in investigating and prosecuting offences committed by right-wing extremist, terrorist groups and lone actors, as well as to facilitate the sharing of experience[134].

Co-operation between agencies

At operational level, on 23 December 2020, Europol and Eurojust signed a contribution agreement[135] that will expand their partnership in supporting law enforcement and judicial authorities with cross-border access to electronic evidence. Eurojust and Europol have also signed bilateral working arrangements with the **EPPO** to regulate their future relationships to ensure close cooperation to better protect the Union's financial interests within and beyond the borders of the EU. Thanks to a close cooperation between Europol, Eurojust and the European Judicial Network, the SIRIUS project[136] supports both the EU law enforcement and judicial community by providing trainings and guidelines to improve (mainly EU-US) cooperation on cross-border access to electronic information. In March, Eurojust and the European Union Intellectual Property Office (EUIPO) agreed to build closer cooperation, to help combat counterfeiting and online piracy[137]. This new agreement marks a new era of cooperation between Eurojust, Europol and EUIPO, as will enable effective support of cases throughout their entire life cycle, from the criminal complaint to a court verdict.

ENISA

ENISA has been implementing the framework for **structured cooperation with CERT-EU**[138] to exploit synergies and avoid duplication of activities in executing its task in the field of operational cooperation, on the basis of a Memorandum of Understanding signed in March. This will result in increased effectiveness and efficiency of both the EU response mechanism and long-term capacity building. This will be supported through a local office of the agency in Brussels designed to foster cooperation with other EU institutions, agencies and bodies[139]. ENISA is helping to put in place the concrete steps to implement new cybersecurity policies. In May, it transmitted the first candidate cybersecurity certification

---

131 https://www.eurojust.europa.eu/action-counter-italian-fuel-tax-fraud-worth-almost-eur-1-billion

132 https://www.eurojust.europa.eu/eurojust-supports-spanish-action-against-illegal-streaming-football-matches

133 https://www.eurojust.europa.eu/worlds-most-dangerous-malware-emotet-disrupted-through-global-action.

134 https://www.eurojust.europa.eu/eurojust-expert-workshops-violent-right-wing-extremism-and-terrorism

135 Europol cooperates with Eurojust on the SIRIUS project, which includes an interactive knowledge-sharing platform accessible to law enforcement and judicial authorities, and aims to produce and disseminate trainings and guidelines to improve (mainly) EU-US cooperation on cross-border access to electronic information).

136 https://www.europol.europa.eu/activities-services/sirius-project

137 https://www.eurojust.europa.eu/stepping-cooperation-tackle-intellectual-property-crime

138 The Computer Emergency Response Team for the EU Institutions, bodies and agencies (CERT-EU) is composed of IT security experts from the main EU Institutions.

139 C(2021) 4626.

scheme on Common Criteria[140], while in June it launched the process to set up an Ad Hoc Working Group on 5G cybersecurity certification[141].

European Border and Coast Guard Agency (Frontex)
Frontex plays a crucial role in supporting Member States in the management of external borders and returns, contributing to the EU's security. The new Regulation[142] has made Frontex the largest EU Agency both in terms of staff and financial resources.

The European Monitoring Centre for Drugs and Drug Addiction
The European Monitoring Centre for Drugs and Drug Addiction (EMCDDA) plays an important role by continuously monitoring the EU drugs situation to provide EU institutions and Member States with the most up-to-date information. A specific focus of their recent work was on the impact of the pandemic on drug markets, use, harms and drug services[143].

VI. Conclusion

The EU has a unique capacity to respond to the threats and challenges of security today, and is progressively equipping itself to strengthen its response. The Security Union Strategy, with its comprehensive and dynamic approach, is breaking down silos to ensure that each risk is understood in the context of the broader threat landscape, that the expertise of all stakeholders contributes to the building of a more secure and resilient EU, and that all the tools at our disposal are deployed effectively in line with European values and respect for fundamental rights.

The Commission will support the European Parliament and Council in finalising important pending legislation in the security area, making sure that the level of ambition matches the challenges the EU faces now and in the future.

In an effort to address global security challenges and strengthen ties with like-minded countries, the EU will also step up cooperation with international partners in areas such as countering terrorism and extremism, malicious cyber activities, hybrid threats and other shared security risks. This is also reflected in the statement agreed at the recent EU-US Summit[144].

While the EU is maintaining a steady rhythm of progress on upgrading and adapting its legislative framework to address the various dimensions of security, rules need to be properly implemented. In this common responsibility, every Member State has its part to play in ensuring the security of Europe as a whole.

[140] Crossing a bridge: the first EU cybersecurity certification scheme is availed to the Commission — ENISA (europa.eu)
[141] Calling on you, 5G Experts! Join us on 5G Cybersecurity Certification — ENISA (europa.eu)
[142] Regulation (EU) 2019/1896.
[143] EMCDDA European Drug Report 2021, 9 June 2021.
[144] EU-US Summit Statement: Towards a renewed Transatlantic partnership, 15 June 2021.