Council of the
European Union

Brussels, 18 October 2023
(OR. en)

14372/23

JAI 1332	**COPEN 363**
COSI 179	**FREMP 292**
ENFOPOL 431	**JAIEX 66**
ENFOCUSTOM 110	**CFSP/PESC 1410**
IXIM 194	**COPS 489**
CT 155	**HYBRID 73**
CRIMORG 137	**DISINFO 85**
FRONT 327	**TELECOM 306**
ASIM 92	**DIGIT 223**
VISA 208	**COMPET 1008**
CYBER 247	**RECH 456**
DATAPROTECT 278	**CULT 122**
CATS 58	**COTER 185**
DROIPEN 151	**CORDROGUE 94**

COVER NOTE

From:	Secretary-General of the European Commission, signed by Ms Martine DEPREZ, Director
date of receipt:	18 October 2023
To:	Ms Thérèse BLANCHET, Secretary-General of the Council of the European Union
No. Cion doc.:	COM(2023) 665 final
Subject:	COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT AND THE COUNCIL on the Sixth Progress Report on the implementation of the EU Security Union Strategy

Delegations will find attached document COM(2023) 665 final.

Encl.: COM(2023) 665 final

EUROPEAN
COMMISSION

Brussels, 18.10.2023
COM(2023) 665 final

COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT AND THE COUNCIL

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

I. Introduction

Three years ago, the Commission adopted the Security Union Strategy 2020-2025[1] defining the main priorities for the Union in the field of security. Since then, we have made strong progress under all four pillars of the Strategy – delivering landmark legislation in everything from critical entities protection to enhancing cyber resilience. In the meantime, however, the security threat landscape in Europe and our neighbourhood continues to evolve. The terrorist attacks in one of our schools in France and in the streets of Brussels in recent days are a stark reminder of the urgency of continuing to adapt and reinforce our security architecture.The danger posed by cyberattacks continues to grow, fuelled also as malicious actors take sides in the ongoing conflicts. Hybrid threats, including disinformation, continue to multiply. Europol has identified the Russian war of aggression against Ukraine as the cause of a significant boost in cyberattacks against EU targets, with major attacks politically motivated and coordinated by pro-Russian hacker groups[2]. This has been felt in blocking internet access and in interruption to key services such as energy networks.[3]

The Security Union Strategy was designed to equip the EU to better withstand an evolving threat landscape. As we have faced the crises posed by pandemic and war, events have shown the importance of the approach taken in the Strategy – our determination to join the dots across the EU security ecosystem, and to break down the silos between the cyber and physical dimensions of security, including tackling organised crime and terrorism as well as combating radicalisation.

Vigilance demands, however, that we should continually probe what is missing in our efforts to keep our citizens safe. The Strategy set out priority areas where the Union can bring added value to support Member States in fostering security for all people living in Europe. Since its adoption, all the actions set out have been addressed and new ones have been incorporated to respond to ongoing security challenges.

Overall, the Commission has presented 36 legislative initiatives under the Security Union Strategy. For more than half of these proposals, inter-institutional negotiations have already concluded with robust new legislation, as described in the table in Annex. However, several key initiatives proposed by the Commission remain under negotiation by the European Parliament and the Council. With the current parliamentary term coming to an end with the European elections in June 2024, rapid work is necessary to deliver on these outstanding files, so that citizens may fully benefit from the Security Union. This 6th Security Union Progress report therefore focuses on outlining those crucial Security Union legislative and non-legislative files adopted by the Commission, for which more needs to be done towards finalisation and effective implementation.

For EU laws already agreed, their benefits will only be felt when put into practice. Work needs to concentrate on their correct and full transposition, implementation and application by Member States. In 2023, the Commission continued to ensure the EU Security Union Strategy

---

1 COM(2020) 605.

2 Distributed Denial of Service (DDoS) attacks: see Europol Spotlight Report 'Cyber-attacks: the apex of crime-as-a-service, 13 September 2023.

3 Malware wipers have been used heavily during the conflict in Ukraine to destroy data and systems for instance affecting internet access for thousands of subscribers in the EU as well as a major German energy company that lost remote monitoring access to over 5 800 wind turbines. The role of cyber in the Russian war against Ukraine: Its impact and the consequences for the future of armed conflict, European Parliament Study, September 2023 - PE 702.594.

delivers by using its institutional powers to launch infringement procedures whenever Member States had failed to transpose or had incorrectly transposed EU legislation.

This report also summarises where the action of Member States and/or EU agencies is central to delivery. EU agencies play a crucial role in supporting the implementation of Security Union initiatives, and their responsibilities have developed over the past years. The report outlines some of the main new tasks that they have been allocated to provide enhanced support for Member States in the implementation of key initiatives under the Security Union.

In addition, the geopolitical situation has underlined the significance of the external security to our internal security. A stronger EU internal framework in the field of security is intrinsically linked to stronger partnerships and cooperation with third countries. The EU must continue to actively pursue how engagement worldwide can help to secure the safety of citizens at home.

II. A future-proof security environment

Cybersecurity and Resilience of critical infrastructure

Under the Security Union, the Union is committed to ensuring that all European citizens and businesses are well protected, both online and offline, and to promoting an open, secure and stable cyberspace. The increasing magnitude, frequency and impact of cybersecurity incidents represent a major threat to the functioning of network and information systems and to the Internal Market. Russia's war of aggression against Ukraine has further exacerbated this threat, and current geopolitical tensions are compounded by interventions from a multiplicity of state-aligned, criminal and hacktivist actors. The sabotage last autumn of the Nord Stream pipelines underlined how essential sectors such as energy, digital infrastructure, transport and space depend on resilient critical infrastructure. The recent incident involving an undersea gas pipeline and data cable in Estonia and Finland illustrates the need for a high level of preparedness to face this kind of situations. While the cause of the damage remains unclear and investigations are ongoing, the sharing of information at different levels among Member States and the Commission has been encouraging. The disruptions had no immediate effect in terms of internet connectivity nor for the security of gas supply at European or local level. This is a sign of the progress made and the reinforced preparedness efforts of recent months.

A clear and robust legal framework is therefore essential to ensure the protection and resilience of these critical infrastructures. In this context, a crucial breakthrough was achieved with the parallel adoption of the revised Directive on measures for a high common level of cybersecurity across the Union (NIS2)[4], and the Directive on the resilience of critical entities (CER)[5], both of which entered into force on 16 January 2023. Now Member States are urged to transpose these fundamental pieces of legislation speedily and fully, at the latest by 17 October 2024, to put in place a robust Union framework to protect Union critical infrastructure against physical and cyber threats.

[4] Directive (EU) 2022/2555 of 14 December 2022 on measures for a high common level of cybersecurity across the Union and Directive (EU) 2018/1972 (NIS 2 Directive).

[5] Directive (EU) 2022/2557 of the European Parliament and of the Council of 14 December 2022 on the resilience of critical entities and repealing Council Directive 2008/114/EC.

In July 2023, the Commission set out in a Commission Delegated Regulation essential services in the 11 sectors covered by the CER Directive[6]. The next step is for Member States to carry out risk assessments on these services. Following the Council Recommendation[7] of 8 December 2022, work has intensified on stress tests on critical infrastructure, starting with the energy sector, and on strengthening the cooperation with NATO and key partner countries. This work led to a report by the EU-NATO Task Force on the resilience of critical infrastructure in June 2023, which maps the current security challenges for critical infrastructure in four key sectors (energy, transport, digital infrastructure and space) and makes recommendations to enhance resilience. The recommendations, including on increased coordination, information sharing and exercises, are being implemented by EU and NATO staffs in the context of the Structured Dialogue on Resilience.

In parallel, on 6 September 2023, the Commission adopted a proposal[8] for a Council Recommendation on a Blueprint to enhance coordination at EU level in response to attempts to disrupt critical infrastructure with significant cross-border relevance. On 4 October 2023 an exercise in the form of a scenario-based discussion on the Blueprint was organised, to test how it would apply in practice and inform the current negotiations on the proposal in the Council.

Following calls from the Council[9], the Commission, the High Representative and the NIS Cooperation Group have been carrying out risk evaluations and building risk scenarios from a cybersecurity perspective. This work has an initial focus on the telecommunications and electricity sectors. The involvement of all relevant agencies and networks, civil and military, creates for the first time a comprehensive and inclusive Union-wide assessment. It will further complement the coordinated security risk assessments of critical supply chains taking place under NIS2, and the risk assessments and stress tests of critical infrastructure in the energy, digital infrastructure communications, transport and space sectors. In the interest of coordination and coherence, these activities should build on one another to help establish a standard approach, and should guide the development of future exercises. The success of these actions will now depend on active engagement of the Member States.

The functioning of economies and societies are increasingly dependent on space-related services and data, especially in the field of security and defence. Space is increasingly contested strategic domain and its' importance for security has grown especially in the aftermath of the Russian invasion of Ukraine. The EU Space Strategy for Security and Defence was adopted in March 2023 to strengthen our strategic posture and autonomy in space. As a key action arising from this Strategy, the European Commission will propose in 2024 an EU Space Law regulating the safety, sustainability and resilience/security of space activities in the EU.

Looking at the external dimension, secure infrastructure underpins the resilience of global economy and supply chains[10], and for this reason the EU's Global Gateway Strategy incorporates a strong security dimension. Equally, given the interconnections between EU and

---

[6] C(2023) 4878.

[7] Council Recommendation of 8 December 2022 on a Union-wide coordinated approach to strengthen the resilience of critical infrastructure.

[8] COM(2023) 526.

[9] Council conclusions of 23 May 2022 on the development of the European Union's cyber posture and Nevers Call of 9 March 2022 to reinforce the EU's cybersecurity capabilities.

[10] JOIN(2021) 30.

partner countries' infrastructure, further international cooperation is essential to strengthen global cyber resilience, and support a free, open, safe and secure cyberspace.

Cyber Resilience Act

Ensuring that consumers and businesses can rely on secure digital products is of central importance to European cybersecurity. The Commission sought to address this need in its proposal for a Cyber Resilience Act[11], adopted on 15 September 2022. It would introduce mandatory horizontal cybersecurity requirements for products with digital elements for five years or their entire lifecycle (whatever is shorter). It would create the conditions for the design and development of secure products with digital elements, by ensuring that hardware and software products are placed on the market with as few vulnerabilities as possible. This would be a key milestone in raising Europe's cybersecurity standards in all domains and is likely to become an international point of reference, providing clear advantages for the Union's cybersecurity industry in global markets. The European Parliament and the Council adopted their respective positions in July 2023 and negotiations should advance swiftly.

Cybersecurity certification also plays a crucial role in increasing trust in ICT products and services, allowing consumers, businesses and authorities to make informed choices with an appropriate level of cybersecurity. Work is advancing on the cybersecurity certification with the EU Common Criteria-based cybersecurity certification scheme being assessed in Comitology. The candidate EU Cloud Security Certification Scheme (EUCS) is currently under preparation by the European Union Agency for Cybersecurity (ENISA) and is being discussed in the European Cybersecurity Certification Group. The intense work with experts from a range of sectors, consumers and providers should lead to a sound legal and technical approach providing the necessary security guarantees consistent with Union law, international commitments and WTO obligations. In addition, ENISA is preparing the EU5G candidate scheme and the EU Digital Identity Wallet (EUIDW). Concerted efforts by all Member States are essential to enhance the overall security of ICT products, ICT services and ICT processes.

Regulations on information security and on cybersecurity for the EU's institutions, bodies and agencies (EUIBAs)

Proposed together in March 2022, the proposed Regulations to govern cybersecurity and information security for the Union's own institutions have moved at different paces. A political agreement was reached last June on the cybersecurity Regulation, allowing a strengthening of the cybersecurity posture of all EU institutions, bodies, offices and agencies, and reflecting the importance the EU attaches to the rapid implementation of this proposal. In this situation it is of particular concern that the parallel proposal on information security, essential to complete a robust legislative framework for EUIBAs, has made unexpectedly slow progress. Both proposals should be adopted before the European parliamentary elections in order to render the European administration credible and resilient in the current geo-political context. A minimum set of information security rules and standards for all EUIBAs would create certainty for all parties involved and ensure consistent protection against the evolving threats to their information, both EU classified and non-classified. Taken together, these new rules would provide a stable basis for secure exchange of information across EUIBAs and with Member States, with standardised practices and measures to protect information flows. As such they respond to multiple calls from the Council to enhance the

[11] COM(2022) 454.

resilience of the EUIBAs and to better protect the Union decision-making process from malicious interference.

Cyber Solidarity Act

Building on the strong strategic, policy and legislative framework already in place, the proposed Cyber Solidarity Act[12] adopted on 18 April 2023 by the Commission, would further enhance detection of cyber threats, resilience and preparedness at all levels of the Union's cybersecurity ecosystem. These objectives would be implemented through three main actions:

(1) the deployment of a ***European Cyber Shield*** to build and enhance common detection and situational awareness capabilities. It would consist of National Security Operations Centres ('National SOCs') and Cross-border Security Operations Centres ('Cross-border SOCs').
(2) The creation of a ***Cyber Emergency Mechanism*** to support Member States in preparing for, responding to and immediately recovering from, significant and large-scale cybersecurity incidents. Support for incident response would include the EU cybersecurity reserve, which would also be available to European institutions, bodies, offices and agencies of the Union (EUIBAs), and third countries associated to the Digital Europe Programme provided their Association Agreement to the Digital Europe Programme provides for that.
(3) The establishment of a ***European Cybersecurity Incident Mechanism*** to review and assess specific significant or large-scale incidents. The post-incident review report would be coordinated and prepared by ENISA.

Discussions have started in the Council and in the European Parliament. Concluding negotiations before the end of the current mandate of the European Parliament would give a major boost to efforts to protect citizens and businesses across the Union.

Cybersecurity Skills Academy

While cyber threats are increasing, the EU urgently needs professionals with the skills and competences to prevent, detect, deter, and defend the EU against cyberattacks. Its cybersecurity workforce needs are currently estimated at 883 000 professionals, while unfilled vacancies ranged between 260 000 and 500 000 in 2022. All sections of society should be encouraged to help fill this gap, but in particular in 2022, women represented only 20% of cybersecurity graduates and 19% of information and communications technology specialists. As part of the 2023 European Year of Skills, the Commission adopted on 18 April 2023[13], an initiative welcomed by Member States[14] to set up a Cybersecurity Skills Academy to close the cybersecurity talent gap. The Cybersecurity Skills Academy would bring together existing initiatives on cybersecurity skills and improve coordination. The Commission encourages Member States, regional and local authorities, as well as European public entities, to adopt dedicated strategies or initiatives on cybersecurity skills, or to integrate cybersecurity skills in relevant strategies or initiatives with a broader scope (e.g. cybersecurity, digital skills, employment, etc). The involvement of private stakeholders will also be essential to narrow the cybersecurity skills gap and associated labour shortage in Europe.

[12] COM(2023) 209.
[13] COM(2023) 207.
[14] Council Conclusions of 22 May 2023 on the EU Policy on Cyber Defence

Drones

Another rising threat to public spaces and critical infrastructures is the malicious use of drones. Incidents involving drones have become more frequent inside and outside the Union, and counter-drone solutions are a key tool for law enforcement and other public authorities in the Union, as well as for private operators of critical infrastructure. At the same time, the legitimate use of drones is making an important contribution towards the twin green and digital transitions.[15] As announced in the Drone Strategy 2.0 adopted in November 2022, the Commission is adopting today a Communication on how to counter potential threats posed by drones, backed up by two handbooks with practical guidance on key technical aspects[16]. The initiative seeks to offer a comprehensive and harmonised policy framework, with a common understanding of rules in place to combat possible threats from drones and to adapt as needed to rapid developments in technology. Member States and relevant private operators are invited to work together closely with the Commission to ensure its full implementation.

Maritime and aviation security

Illicit activities, such as piracy, armed robbery at sea, smuggling of migrants and trafficking of human beings, arms and narcotics, as well as terrorism, remain challenges for maritime security, and are compounded by evolving threats including hybrid and cyber-attacks. The Commission and the High Representative adopted on 10 March 2023 a Joint Communication, updating the EU's Maritime Security Strategy[17] which should now be implemented in line with the updated Action Plan.

In the area of aviation security, the Commission adopted a Staff Working Document "Working towards an enhanced and more resilient aviation security policy"[18] on 2 February 2023, which contains an ambitious programme to (1) modernise the regulatory architecture for aviation security (2) foster the development and uptake of more innovative solutions; and (3) update the aviation security baseline so that Union airports can fully benefit from new and cutting-edge technologies to address the highest priority threats. Fourteen flagship actions need to be implemented within two years.

The Commission calls on the European Parliament and the Council to finalise the negotiations as a matter of urgency, in any case before the end of the mandate of the current European Parliament, on the following files:

- The proposal for a Cyber Resilience Act;
- The proposal for a Cyber Solidarity Act;
- The proposed Regulation on information security for EUIBAs.

The Commission calls on Member States to:

- pursue the transposition of the Critical Entities Resilience Directive as a priority, as well as the stress testing of critical infrastructure in the energy sector;
- adopt the Council Recommendation on a Blueprint to coordinate response to disruptions of critical infrastructure with significant cross-border relevance;
- transpose the NIS2 Directive fully and urgently to boost cybersecurity of essential

[15] COM(2022) 652.
[16] COM (2023) 659.
[17] JOIN (2023) 8.
[18] SWD(2023) 37.

and important entities;
- actively engage in carrying out cybersecurity risk assessments and building risk scenarios of critical infrastructure and supply chains;
- follow up on the Cybersecurity Skills Academy with strong engagement at European level and dedicated national strategies or initiatives on cybersecurity skills, bringing in key stakeholders including regional and local authorities;
- work with relevant private operators and the Commission to ensure the implementation of all the actions listed in the Communication on countering potential threats caused by drones;
- implement EU maritime Security Strategy Action Plan and report regularly on achievements;
- Implement the 14 flagship actions identified to enhance aviation security.

III. Tackling evolving threats

New geopolitical tensions have offered stark evidence of how the security challenge to the EU is not only increasing, but is increasingly volatile, and accentuated by the hybrid nature of many threats. Security also needs to respond to changes in society and technology. The COVID-19 pandemic reinforced opportunities for cybercriminals and saw in particular an increased threat of child sexual abuse material online. Criminals and malicious actors are always ready to exploit technological developments. In the face of such often complex and multi-dimensional threats, strong and consistent EU action is required.

Regulation on fighting Child Sexual Abuse Online

Europol's Internet Organised Crime Threat Assessment revealed that in 2022, child sexual exploitation and abuse had been further increasing in terms of frequency and severity, with offenders continuing to take advantage of technical possibilities to mask their actions and identities[19].The current system based on voluntary detection and reporting by companies has proven insufficient to protect children. An interim regulation allows the voluntary detection and reporting by companies, provided this is lawful under the General Data Protection Regulation (GDPR). This Regulation will expire in August 2024. In May 2022, the Commission proposed a Regulation[20] to address the misuse of online services for the purposes of child sexual abuse. The framework proposed puts a strong emphasis on prevention. Companies would be obliged to assess the risk of child sexual abuse via their systems, and to take preventive measures. As a measure of last resort, in case of a significant risk only, national courts or independent administrative authorities could issue targeted detection orders to service providers. A new independent EU Centre would facilitate the efforts of service providers acting as a hub for expertise, providing reliable information on identified material, receiving and analyzing child sexual abuse online reports from providers to identify erroneous reports as well as providing support to victims. It is essential that the new rules are adopted and implemented as soon as possible to protect children from further abuse, prevent material from reappearing online, and to bring offenders to justice. Negotiations are ongoing in the

[19] Europol (2023), Internet Organised Crime Threat Assessment (IOCTA) 2023.
[20] COM (2022) 209.

Council and in the Parliament with the objective of finding an agreement on the file before the end of the Parliament's mandate.

Directive on combating violence against women and domestic violence

Cyber violence against women, including in the context of domestic violence, has emerged as a new form of such violence, spreading beyond individual Member States via the internet and IT tools. In March 2022, the Commission proposed a Directive to address violence against women and domestic violence, including specific rules on cyber violence and measures to fill gaps in protection, access to justice, and prevention. Early adoption and implementation would give Member States additional tools to combat this form of crime. The co-legislators entered inter-institutional negotiations in July 2023 and are aiming to finalise the negotiations before the end of the current European Parliament mandate.

5G Cybersecurity

The security of 5G networks is a major priority for the Commission and an essential component of its Security Union Strategy. 5G networks are a central infrastructure, providing the foundation for a wide range of services essential for the functioning of the internal market and for vital societal and economic functions. On 15 June 2023, EU Member States authorities represented in the NIS Cooperation Group, with the support of the Commission and ENISA, published a second progress report on the implementation of the EU Toolbox on 5G cybersecurity. According to the report, 24 Member States have adopted or are preparing legislative measures giving national authorities the powers to perform an assessment of suppliers and issue restrictions, and 10 Member States have imposed such restrictions. However, further action is needed to avoid vulnerabilities for the Union as a whole, with potentially serious negative impacts on security for individual users and companies across the Union and the Union's critical infrastructure. All Member States need to implement the Toolbox without delay. On the same day, the Commission adopted a Communication on the implementation of the Toolbox by Member States and on the Commission's own corporate communications and Union funding activities. This underlined strong concerns about the risks to EU security posed by suppliers of mobile network communication equipment Huawei and ZTE. In this context, the Commission is taking measures to avoid exposure of its corporate communications to mobile networks using Huawei and ZTE as suppliers. Procurements will exclude new connectivity services that rely on equipment from those suppliers and the Commission will work with Member States and telecom operators to make sure that those suppliers are progressively phased out from existing connectivity services of the Commission sites. The Commission is also exploring how to reflect this decision in relevant Union funding programmes and instruments, in full compliance with Union law.

Access to Data for effective law enforcement

In today's digital age, almost every crime has a digital component. Technologies and tools are also being used for criminal purposes, including those that are necessary to guarantee our society's need for cybersecurity, data protection and privacy. This makes it increasingly challenging to maintain effective law enforcement across the EU to safeguard public security and to prevent, detect, investigate, and prosecute crime, although significant efforts have been made at Union and national levels, including through legislation as well as capacity building and innovation initiatives, legal and technical challenges persist. The Commission, associating the Presidency of the Council, has set up a High-Level Group on access to data for effective law enforcement to provide a collaborative platform for a wide range of stakeholders and experts to explore challenges that criminal law enforcement practitioners face (e.g., encryption, data retention, 5G and standardisation). The Commission expects the High-Level

Group to formulate balanced, solid and achievable recommendations by June 2024, reflecting the complexity of these issues, including from the cybersecurity and data protection perspectives. Member States and participating experts are therefore encouraged to actively engage in this process and work towards effective, lawful and commonly accepted solutions.

Hybrid threats

In a geopolitical context where hybrid threats are growing in complexity and sophistication, the EU Strategic Compass for Security and Defence[21] (Strategic Compass) provided a shared assessment of the threats and challenges the Union faces, as well as a strategic plan of action. The increase of malicious behaviour in cyberspace by States and non-state actors, including in the context of the war against Ukraine, has further underlined cyberspace as a foreign and security policy field. The potential risks of malicious actions and disinformation call for particular vigilance in election periods, including in the run up to the European elections in 2024.

Considering the high risks of spillover effects, the EU has continued to develop cyber capacity-building activities and foster partnerships with third countries, including through dedicated cyber dialogues, to actively contribute to its overall resilience. A number of tools have been developed, revised and strengthened to enhance the Union ability to effectively address hybrid threats, as described in the 7th Progress Report on Hybrid Threats published on 14 September 2023[22]. These include:

- the EU Hybrid Toolbox to ensure a framework for a coordinated and well-informed response to hybrid threats and campaigns;
- the ongoing work to set up EU hybrid rapid response teams for short-term tailored support to Member States, partner countries and common security and defence policy (CSDP) missions and operations;
- the revised EU Protocol for countering hybrid threats ('EU Playbook')[23] that describes the Union's processes and structures dealing with hybrid threats and campaigns;
- the revised implementing guidelines of the Framework for a Joint EU Diplomatic Response to Malicious Cyber Activities [24]("Cyber Diplomacy Toolbox ") that enables the development of sustained, tailored, coherent and coordinated strategies against persistent cyber threat actors;
- the Foreign Information Manipulation and Interference (FIMI) Toolbox, to strengthen the Union's existing tools to prevent, deter and respond to FIMI;
- the EU Policy on Cyber Defence[25], to boost the EU cyber defence capabilities, enhance situational awareness and coordinate on the whole range of defensive options available, in order to strengthen resilience, respond to cyber-attacks and ensure solidarity and mutual assistance.

Member States are therefore encouraged to continue and enhance their cooperation in this area, by ensuring effective implementation of the above-mentioned toolboxes, including through regular exercises, and by reaching agreement on the concept of hybrid rapid response teams, which will provide guidance for further steps towards establishing the teams.

[21] Council document 7371/22.
[22] SWD(2023) 315.
[23] SWD(2023) 116.
[24] 10289/23 of 8 June 2023.
[25] JOIN(2022) 49.

AI in the law enforcement context

Artificial intelligence (AI) has rapidly become a common feature of daily life. The effects of the use of AI on cybercrime and cybersecurity are not yet fully known, but will clearly pose new challenges. While AI can bring benefits when used in a safe and controlled manner, it may have dangerous potential in the hands of malicious actors, including by helping criminals hide their identities in crimes such as terrorism and child sexual abuse. It is therefore crucial for authorities to stay up to date with developments to prevent abuse and respond to misuse[26]. Negotiations on the proposed Artificial Intelligence Act aim to address these issues and have entered a crucial stage, with co-legislators now discussing technical and political issues that will determine interactions with this technology in the years to come. It will be essential to find balanced solutions, especially with regard to high-risk applications, including in the law enforcement area.

The Commission calls on the European Parliament and the Council to finalise the interinstitutional negotiations as a matter of urgency, in any case before the end of the mandate of the current European Parliament on the following pending files:

- Proposal for a Regulation on fighting child sexual abuse online;
- Proposal for a Directive on combating violence against women and domestic violence;
- Proposal for a Regulation laying down harmonised rules on Artificial Intelligence (AI Act).

The Commission calls on Member States to:

- achieve the full implementation of the EU Toolbox on 5G cybersecurity without delay;
- support the work of the High-Level group on access to data for effective law enforcement, with a view to formulate clear, solid and achievable recommendations to address in a proportionate way current and anticipated challenges;
- take steps, in cooperation with the High Representative, to ensure the effective implementation of the EU Hybrid Toolbox, the revised Cyber Diplomacy Toolbox and the FIMI Toolbox, including through regular exercises and taking into account global dynamics;
- reach agreement on the concept of hybrid rapid response teams.

IV. Protecting Europeans from terrorism and organised crime

The risk that global or local events spark new outbreaks of terrorism is ever-present. In parallel, organised crime and drug trafficking are among the most serious threats to the EU's security. In order to step up the Union's collective efforts in the fight against these threats, collective work is ongoing in the implementation of the EU Strategy to Tackle Organised Crime[27], the EU Strategy on Combatting Trafficking in Human Beings[28]the EU Agenda and

[26] See for example Europol's report published on 17 April 2023: ChatGPT - the impact of Large Language Models on Law Enforcement.

[27] COM(2021)170.

Action Plan on Drugs[29] and the EU Agenda on Counter-Terrorism[30]. However, to respond to a worryingly deteriorating situation in terms of organised crime and drug trafficking, a further intensification of work by Member States and EU is needed to strengthen our collective response to criminal networks and better protect victims of crime, and an EU Roadmap to fight drug trafficking and organised crime is being published at the same time as this report[31].

In the field of counter-terrorism, the EU is reinforcing also its external toolbox[32], by making full use of the High Level Counter-Terrorism Dialogues and the network of Counter-Terrorism/Security Experts in EU Delegations, as well as through its engagement in multilateral fora, including as Co-Chair of the Global Counter-Terrorism Forum (GCTF).

Drug trafficking

With the new mandate of the EU Drugs Agency that will apply as of July 2024, the EU will be better equipped to address a complex security and health problem affecting millions of people in the EU and globally. The Commission is also revising[33] the drug precursors regulations[34] to address the main challenges identified by the 2020 evaluation[35], which highlighted the need to address the challenges posed by designer precursors[36]to reduce the supply of illegal drugs.

However, in the face of an unprecedented increase of illicit drugs available in Europe, the fight against drug trafficking must intensify, in cooperation with international partners. Additional action by Member States and the EU is needed to dismantle criminal networks and better protect victims of crime. The Commission presents today an EU Roadmap to fight drug trafficking and organised crime. It sets out 17 actions in four priority areas: to strengthen the resilience of logistic hubs with a European Ports Alliance, to dismantle criminal networks, to increase prevention efforts and to strengthen cooperation with international partners. These actions are to be implemented in 2024 and 2025.

Firearms

Firearms trafficking feeds organised crime within the EU as well as its in neighbourhood. As many as 35 million illicit firearms are estimated to be in the hands of civilians in the EU, and around 630,000 firearms are listed as stolen or lost in the Schengen Information System. With the development of fast parcel delivery and of new technologies such as 3D printing, trafficking of firearms is taking new forms to escape controls. Russia's war of aggression against Ukraine has also increased the risk of proliferation of firearms. In October 2022, the Commission adopted a proposal to update existing legislation on the import, export and transit of civilian firearms, to close loopholes in the existing rules which can increase the number of firearms smuggled and diverted into the EU[37]. In the medium term, these new rules will help

---

28 COM(2021) 171.
29 COM(2020) 606.
30 COM (2020) 795.
31 COM (2023) 641.
32 As called for by the Strategic Compass and the Council Conclusions on "Addressing the external dimension of a constantly evolving terrorist and violent extremist threat focusing on the external dimension" adopted in June 2022.
33 Drug precursors – EU legislation (revised rules) (europa.eu)
34 Regulation (EC) No 273/2004 on drug precursors and Council Regulation (EC) No 111/2005 laying down rules for the monitoring of trade between the Community and third countries in drug precursors.
35 COM(2020) 768.
36 Action 23 of the Action Plan on Drugs , COM(2020) 606.
37 COM (2022) 480.

reduce the risk of circumvention of embargos in the case of exports of firearms for civilian use and increasing the controls of the import of this kind of firearms from non-EU countries. Both co-legislators still need to adopt their positions on this file with the objective to find an agreement on this file before the end of this Parliament's mandate.

Trafficking in human beings

Trafficking in human beings is a particularly serious form of organised crime and a grave violation of fundamental rights. Victims are trafficked within the EU, mainly for sexual and labour exploitation, but also for forced begging and criminality and other forms. The Commission proposed in December 2022 to amend the Anti-trafficking Directive[38] with updated rules to address shortcomings in the current legal framework. In particular, once adopted, the revised Directive would add forced marriage and illegal adoption to the scope of the Directive and introduce an explicit reference to the online dimension of trafficking in human beings. It would also include a mandatory regime of sanctions for perpetrators and formalise the establishment of National Referral Mechanisms to improve early identification and cross-border referral for assistance and support to victims. Knowingly using services provided by victims of trafficking would become an offence and annual data collection on trafficking in human beings, to be published by Eurostat, would become obligatory. The Council adopted its general approach in June 2023 while the European Parliament still needs to adopt its position. Rapid action will be necessary to find an agreement before the end of this Parliament's mandate.

Environmental Crime

Environmental crime has become a global threat, growing at an estimated rate of between 5 to 7% every year. The significant profits that can be generated, legal loopholes between Member States and a low risk of detection all attract organised crime. According to Europol, there are indications that the proceeds of these activities are used to finance terrorism. In December 2021, the Commission adopted a proposal to replace the 2008 Directive on protecting the environment through criminal law. The proposal focuses on refining and updating the definitions of environmental crime categories and defining effective, dissuasive and proportionate sanction types and levels for natural and legal persons. New crimes include offences linked to illegal deforestation, breaches of EU chemicals legislation, illegal extraction of surface or groundwater and illegal ship recycling. The proposal aims to significantly strengthen the law enforcement chain and cross-border cooperation between Member States' authorities and EU agencies and bodies. The European Parliament and the Council have adopted their respective positions on the proposal and are in a process of negotiations on which they should be able to conclude by the end of the year. A revised Action Plan[39] against wildlife trafficking requires implementation to further strengthen prevention and enforcement.

Asset recovery and confiscation

Depriving criminals of their illicit revenues is key to disrupting organised crime. This is why, in addition to the proposal giving law enforcement access to bank account information across the EU[40] (for which a political agreement was reached in June 2023), the Commission put

[38] COM(2022) 732.
[39] COM(2022) 581.
[40] COM(2021) 429.

forward a proposal on asset recovery and confiscation[41] in May 2022, to strengthen asset tracing, identification, freezing, confiscation and management capabilities. Key provisions of the proposal concern the requirements for financial investigations, and additional powers and tools of Asset Recovery Offices, as well as more effective freezing and confiscation measures for a broadened set of crimes. One of the new criminal offences for which these measures would be made applicable is the violation of Union restrictive measures. In December 2022, the Commission adopted a separate proposal to harmonise the criminal definitions of and penalties for the violation of Union restrictive measures. The effective implementation and enforcement of Union restrictive measures remains a top priority for the Commission, strengthened by the work of the Freeze and Seize Task Force set up by the Commission in response to Russia's war of aggression against Ukraine. For both proposals, the European Parliament and the Council have adopted their positions with the aim of finding an agreement by the end of this year.

Anti-money laundering package

Money laundering is connected to virtually all criminal activities generating criminal proceeds in the EU[42] and is thus a key lever to tackle crime in the EU. In July 2021, the Commission put forward ambitious proposals to strengthen EU's measures to prevent money laundering and terrorism financing[43], with four legislative proposals to strengthen prevention and detection of attempts by criminals to launder illicit proceeds or finance terrorist activities through the financial system. One of the four initiatives of the package, to ensure traceability of crypto-asset transfers, was adopted by the co-legislators in May 2023[44]. This Regulation will become applicable on 30 December 2024, by which date all crypto-asset service providers will have to collect and hold information about the originator and beneficiary of transfers of crypto assets. The remaining three proposals aim to (i) establish a new EU anti-money laundering authority to ensure consistent high-quality supervision across the internal market, including of the riskiest cross-border entities, supporting and coordinating the work of Financial Intelligence Units, (ii) set out harmonised rules for the private sector, including the introduction of an EU-wide limit of EUR 10 000 for large cash payments in exchange for services and goods, and (iii) strengthen the powers and cooperation tools for competent authorities. This package is expected to significantly enhance the EU's ability to fight money laundering and protect EU citizens from terrorism and organised crime. The three outstanding proposals are currently under negotiation by co-legislators with the objective of finding an agreement on this file before the end of this Parliament's mandate.

The Commission calls on the European Parliament and the Council to finalise the interinstitutional negotiations as a matter of urgency, in any case before the end of the mandate of the current European Parliament, on the following pending files:

- Proposal for a Directive on asset recovery and confiscation;
- Proposal for a Directive to harmonise the criminal definitions of, and penalties for, the violation of Union restrictive measures;
- Proposal for an Anti-Trafficking Directive;

[41] COM (2022) 245.

[42] Europol, Enterprising criminals – Europe's fight against the global networks of financial and economic crime, 2020.

[43] COM (2021) 420.

[44] Regulation (EU) 2023/1113 of 31 May 2023 on information accompanying transfers of funds and certain crypto-assets and amending Directive (EU) 2015/849.

- Proposal for a Directive improving environmental protection through criminal law;
- Proposal for an Anti-Money laundering package;
- Proposal to update existing legislation on import, export and transit of civilian firearms.

The Commission calls on Member States, EU agencies and bodies:

- To work together toward the implementation of the 17 actions of the EU Roadmap to fight drug trafficking and organised crime in 2023 and 2024.

V. A strong European security eco-system

In recent years, security threats have become increasingly cross-border in nature, calling for further synergies and closer cooperation at all levels. Since the adoption of the Security Union Strategy, important initiatives have been taken to maximise cross-border cooperation, streamlining and upgrading the available instruments and procedures both at the external borders and within the Schengen area, as well as enhancing the exchange of information between law enforcement and judicial authorities to better fight organised crime. Against this background, the effective implementation of the interoperability framework for the exchange of data is an important pillar to enhance security and an effective European response to cross-border threats, while guaranteeing internal free movement.

Enhanced exchange of information within the Schengen area: Advance Passenger Information (API), Passenger Name records (PNR) and Prüm II

The two API proposals adopted by the Commission in December 2022[45] would enhance the internal security of the Union by providing Member States' law enforcement authorities with additional tools to fight serious crime and terrorism. In particular, advance passenger information on intra-EU flights, used together with PNR of air travellers, would enable Member States' law enforcement authorities to significantly increase the efficiency of their investigations with more targeted interventions. It is important that the proposed rules are adopted as soon as possible: this would not only support the fight against organised crime and terrorism but also significantly reduce the need for systematic checks on all travellers in case of a temporary reintroduction of internal border checks, facilitating air travel and freedom of movement. On 6 September 2023, the European Commission recommended that the Council authorize negotiations with Switzerland, Iceland and Norway for agreements on the transfer of PNR data. The adoption of these three Recommendations would support a consistent and effective EU external PNR policy.

Prüm exchanges are used on a daily basis by the police to combat organised crime, drugs, terrorism, sexual exploitation, and trafficking of human beings. The proposal for a regulation on automated data exchange for police cooperation ("Prüm II")[46] revises the existing Prüm framework with a view to closing information gaps and boosting the prevention, detection and investigation of criminal offences in the EU. The revised rules on automated data exchange for police cooperation complete the Police Cooperation proposals in this mandate, alongside

[45] COM(2022) 729, COM(2022) 73.
[46] COM(2021) 784.

the already-adopted Council recommendation reinforcing operational cross border cooperation and the Directive on information exchange between law enforcement authorities. Rapid adoption and implementation of these related instruments would improve, facilitate and accelerate data exchange between law enforcement authorities and help identify criminals.

Fully interoperable border management system for a secure, strong, digital and united Schengen Area

A well-functioning Schengen area without internal borders relies on the mutual trust among the Member States. This in turn rests on efficient controls, whether at the external borders of the Union or as alternative measures on the territory of the Member States. The amendment proposed by the Commission to the Schengen Borders Code[47] sets out how Member States can make better use of alternatives to internal border controls, which can offer a high level of security. It is important that the amendment to the Schengen Borders Code is adopted and implemented in full to ensure a high and proportionate level of security within the Schengen area. The new architecture of EU information systems also continues to be developed to better support national authorities' work to ensure security and border management. It comprises the renewed Schengen Information System, the European Travel Information and Authorisation System, the Entry/Exit System, the update of the Visa Information System, and the interoperability framework to link systems together in full security. Once fully complete, this new architecture would provide national authorities with more comprehensive and reliable security information. All components of the interoperability framework are essential, which means that a delay in one aspect or in one Member State leads to a delayed roll-out for everyone. Delays in the technical development of the Entry/Exit system should be reduced to the minimum, so that the Entry/Exit System can start operating as soon as possible and all key elements of the interoperability framework can be put in place.

The Screening proposal[48] would enhance the security within the Schengen area by creating uniform rules concerning the identification of third-country nationals who do not fulfil entry conditions as referred to in the Schengen Borders Code, and submitting them to the health and security checks at the external borders. The proposed Eurodac system would support these objectives indicating where it appears following screening that an individual could pose a threat to internal security. This would in turn facilitate the implementation of the proposed Regulation on Asylum and Migration Management. The Commission encourages the co-legislators to swiftly conclude the negotiations on these files before the end of the current legislative period.

Anti-Corruption

Corruption is highly damaging to our democracies, to the economy and to our security, as it acts as an enabler for organised crime and hostile foreign interference. Successfully preventing and fighting corruption is essential both to safeguard EU values and the effectiveness of EU policies, and to uphold the rule of law and trust in those who govern and public institutions. As announced by President von der Leyen in the State of the Union Speech of 2022, the Commission adopted on 3 May 2023 a package of anti-corruption measures[49]**.** The Commission's proposal for a Directive on combating corruption includes strengthened rules criminalising corruption offences and harmonising penalties across the EU.

[47] COM(2021) 891.
[48] COM(2020) 612.
[49] COM(2023) 234.

It also enables effective investigations and prosecutions and places a strong focus on prevention and creating a culture of integrity in which corruption is not tolerated. Discussions on this proposal have started in the European Parliament and the Council. In addition, Member States are invited to implement the recommendations stemming from the anti-corruption pillar of the 2023 Rule of Law report adopted on 5 July 2023. A proposal from the High Representative, supported by the Commission, also proposes to establish a dedicated Common Foreign and Security Policy (CFSP) sanctions regime to target serious acts of corruption worldwide.

Strengthening of victims' rights

On 12 July 2023, the Commission proposed amendments to the Victims' Rights Directive, to strengthen victims' access to information, support and protection, participation in criminal proceedings and access to compensation. One of the overall objectives of the revision is to contribute to a high level of security by creating a safer environment for victims to encourage reporting of crimes, reducing fears of reprisals.

The Commission calls on the European Parliament and the Council to finalise the interinstitutional negotiations as a matter of urgency, in any case before the end of the mandate of the current European Parliament on the following pending files:

- Proposal on the Prüm II regulation;
- Proposals on Advanced Passenger Information (API);
- Proposals on Anticorruption and in particular to establish a dedicated Common Foreign and Security Policy (CFSP) sanctions regime;
- Proposal for an Amendment to the Schengen Border Code Regulation;
- Proposal for a Victims' Rights Directive;
- Proposal on Screening.

The Commission calls on Member States to:

- ensure the entry into force of the Entry/Exit system as soon as possible in order to complete the implementation of the EU architecture on information exchange.

VI. Implementation

Ensuring the security of Europe as a whole is a shared responsibility, where every actor has to play its part, from the Commission and the co-legislators adopting new, strong, comprehensive and practical rules, to the timely transposition, implementation and application of such rules by Member States, and the operational work carried out on the ground by a variety of authorities, organisations and stakeholders. EU agencies in the areas of justice, home affairs, and cybersecurity also play a key role, which has increased through recent extensions of their responsibilities.

Enhanced screening of beneficiaries of EU funding

When implementing the EU budget, the Commission has a responsibility to ensure that beneficiaries of EU funding respect EU values. The mechanisms and control systems determining who may benefit from EU funding are already robust, and the ongoing recast negotiation of the Financial Regulation also seeks to give stronger legal means to the Commission to act if needed. In addition, the Commission is currently working on ways to further enhance the screening of current and potential future beneficiaries of EU funding, by improving the guidance on obligations concerning respect for EU values and the

consequences that should follow a breach of EU values. This will clarify the responsibilities both of beneficiaries and those conducting controls at EU level and may serve as a source of inspiration for the national level. In case of a breach of the funding conditions, the Commission does not and will not hesitate to halt cooperation with the beneficiaries of the project concerned, and to recover funds if necessary. It is important that Member States proactively share information with the Commission when they are aware of possible risks regarding organisations applying for EU funding.

Infringements

In the area of security, the Commission has conducted many infringement procedures. For example, in 2023, a large number of infringement cases were initiated due to failures to fulfil obligations under the 2021 Regulation on dissemination of terrorist online content (16 Member States)[50], and over the course of the years 2022 and 2023, 20 Member States received additional letters of formal notice due to the incorrect implementation of the 2011 Directive on combating child sexual abuse[51]. A significant number of infringement cases are still open for non-conformity of national legislation with the 2017 Directive on combating terrorism[52] and for failure to transpose rules that facilitate the use of financial and other information for the prevention, detection, investigation or prosecution of certain criminal offences[53]. Other areas where infringement proceedings are ongoing include firearms legislation; rules on psychoactive substances used in drugs, combating fraud and counterfeiting of non-cash means of payments, fighting money laundering, exchange of criminal records between the EU Member States, and the Victims' Rights Directive. Support (technical and financial) has been made available to Member States implementing agreed initiatives and actions and the Commission remains available to work with Member States to optimise implementation.

Monitoring through Schengen evaluations and its new governance system

The Schengen evaluation and monitoring mechanism has continued to contribute to the effective implementation of the Schengen rules aimed at enhancing security within the area without internal controls. In 2023, the first evaluations under the reinforced Schengen evaluation and monitoring mechanism were carried out allowing for the timely identification and remedying of strategic vulnerabilities, which have a cross-border impact on security and safety within the EU. Furthermore, in 2023, the Commission launched a thematic Schengen evaluation to assess the practices of Member States that face similar challenges in combating drug trafficking into the EU, particularly focusing on high volume drug trafficking. These evaluations introduced a reinforced and more comprehensive focus to the security elements of Schengen. Based on the results of the periodic, thematic and unannounced Schengen evaluations, the Council established in June 2023 the 2023-2024 Schengen cycle priorities. It sets out focus areas requiring additional impetus for a more secure and stronger Schengen area. An effective and swift implementation of these priorities together with increased policy

[50] Regulation (EU) 2021/784 on dissemination of terrorist content online.

[51] Directive (EU) 2011/93 on combating child sexual abuse.

[52] Directive (EU) 2017/541 of the European Parliament and of the Council of 15 March 2017 on combating terrorism and replacing Council Framework Decision 2002/475/JHA and amending Council Decision 2005/671/JHA.

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

coordination of the Schengen Council will further strengthen the fight against organised crime and maximise cross-border operational cooperation.

Role of EU agencies and bodies

Partnership is key for the implementation of Security Union initiatives as the work of different national and European authorities and bodies is needed to bring concrete results. For instance, EMPACT (the European Multidisciplinary Platform Against Criminal Threats) enables structured multidisciplinary cooperation of Member States, supported by all EU institutions, bodies and agencies (such as Europol, Frontex, Eurojust, CEPOL, OLAF, EU-LISA). The operations performed by EMPACT including through dedicated Operational Task Forces (OTFs) coordinate the efforts of Member States and operational partners in fighting criminal networks and serious crime. In 2022 alone, EMPACT resulted in a total of 9922 arrests, over EUR 180 million in assets and money seized, 9263 investigations initiated, 4019 victims identified, over 62 tonnes of drugs seized, 51 High Value Targets (HVT) identified and 12 arrested, operations in the context of the war of aggression against Ukraine, notably to tackle trafficking in human beings and firearms-related threats[54].

Frontex, the European Maritime Safety Agency (EMSA) and the European Fisheries Control Agency (EFCA), continue to strengthen their cooperation on coastguard functions to support national authorities in increasing the safety and security at sea. These agencies will be major contributors to the implementation of the EU maritime security strategy.

Several of Security Union initiatives have brought new responsibilities and tasks for relevant Agencies, sometimes with implications for human resources.

European Union Agency for Cybersecurity (ENISA)

As regards preparedness and incident response to enhance cybersecurity, the Commission has set up a short-term action to support Member States, transferring funding from the Digital Europe Programme (DEP) to the **European Union Agency for Cybersecurity (ENISA)** to reinforce preparedness and capacities to respond to major cyber incidents. The proposal for the Cyber Solidarity Act adopted in April 2023 builds on this action and, once adopted by co-legislators, may entrust ENISA with additional tasks such as the operation and administration of the future Union cybersecurity reserve or the preparation of an incident review report following large scale cybersecurity incidents. The proposed Cyber Resilience Act would task ENISA to receive notifications from manufacturers of vulnerabilities in products with digital elements, and incidents impacting on the security of those products, which ENISA would be expected to forward to the relevant CSIRTs or to the relevant single points of contact of the Member States. ENISA is also expected to prepare a biennial technical report on emerging trends regarding cybersecurity risks in products with digital elements and submit it to the NIS Cooperation Group.

European Cybersecurity Competence Centre

[54] EMPACT factsheets of results in 2022: https://www.consilium.europa.eu/media/65450/2023_225_empact-factsheets-2022_web-final.pdf

The **European Cybersecurity Competence Centre (ECCC)**, together with the Network of National Coordination Centres (NCCs), is the Union's new body to support innovation and industrial policy in cybersecurity. This ecosystem will strengthen the capacities of the cybersecurity technology community, maintain research excellence and reinforce the competitiveness of the Union industry in this field. The ECCC and the NCCs will make strategic investment decisions and pool resources from the Union, its Member States and, indirectly, industry to improve and strengthen technology and industrial cybersecurity capacities. The ECCC therefore has a key role to play in delivering on the ambitious cybersecurity objectives of the Digital Europe and Horizon Europe Programmes.

The ECCC has recruited more than half its staff, and will soon recruit its Executive Director. Work already underway includes /the cybersecurity part of the DIGITAL programme and a new strategic agenda[55] for technology development and deployment which sets out priority actions to support SMEs in the development and use of strategic cybersecurity technologies, services and processes; to support and grow the professional workforce; and strengthen research, development and innovation expertise in the broader European cybersecurity ecosystem.

Europol

With a brand-new mandate, **Europol** will be better equipped to support Member States in the fight against organised crime. The fight against drugs trafficking is a key priority in view of its growing importance and increasing negative impact on the security of EU citizens. Following the authorisation of the Council of the European Union on 15 May 2023 the Commission has been actively working towards the conclusion of international agreements with Bolivia, Brazil, Ecuador, Mexico and Peru on the exchange of personal data with Europol with the aim of preventing and combating serious crime and terrorism.

Eurojust

With over 20 years' experience in providing judicial support to national authorities to combat a wide range of serious and complex cross-border crimes, **Eurojust** has cemented its position in the EU's area of freedom, security and justice. To strengthen cooperation across the board, the Commission is negotiating international agreements to facilitate cooperation between Eurojust and 13 third countries to exchange personal data to fight organised crime and terrorism[56]. Negotiations have already been completed with Armenia and Lebanon, are ongoing with Algeria and Colombia and have started with Bosnia and Herzegovina. The Commission encourages the European Parliament and the Council to finalise conclusion of agreements with these countries before the end of the parliamentary term, so as to strengthen transnational judicial cooperation and broaden the fight against cross-border crime.

EPPO

Since the start of its operational activities in June 2021, the **European Public Prosecutor's Office (EPPO)** has proved to be a powerful tool in the Union toolbox to investigate and prosecute offences affecting the Union budget, including offences related to the participation in a criminal organisation, when the focus is on crimes against the Union budget. The Commission encourages Member States who do not yet participate in the EPPO's enhanced

[55] https://cybersecurity-centre.europa.eu/strategic-agenda_en

[56] Algeria, Argentina, Armenia, Bosnia and Herzegovina, Brazil, Colombia, Egypt, Israel, Jordan, Lebanon, Morocco, Tunisia and Turkey.

cooperation to do so as soon as possible in order to achieve EPPO's full potential in protecting the EU's taxpayers' money.

EUDA

With a new mandate adopted by the co-legislators in June 2023, the existing European Monitoring Centre for Drugs and Drug Addiction (EMCDDA) will turn into a fully-fledged agency – the **European Union Drugs Agency (EUDA*)*** – with a strengthened role. The agency will be able to assess new health and security challenges posed by illicit drugs in a more comprehensive way, and contribute more effectively to work at Member States and international level. The collection, analysis and dissemination of data will continue to be the main task of the agency, but the enhanced mandate will also allow the agency to develop general health and security threat assessment capabilities to identify emerging threats, including poly-substance use, strengthen its cooperation through national focal points, and put in place a network of laboratories providing the agency with forensic and toxicological information. This will help the agency to issue alerts when particularly dangerous substances appear on the market and raise awareness.

The Commission calls on the European Parliament and the Council to finalise the interinstitutional negotiations as a matter of urgency, in any case before the end of the mandate of the current European Parliament, on the following pending files:

- Proposal on the recast of the Financial Regulation.

The Commission calls on Member States to:

- proactively share information with the Commission when they are aware of possible risks regarding organisations applying for EU funding;
- swiftly implement the priorities of the 2023-2024 Schengen cycle for a more secure and stronger Schengen area;
- address the infringement procedures open against them in order to ensure the proper transposition of the legislation concerned.

VII. Conclusion

The past three years have been marked by a constant and determined effort to give life to the ambition of creating a Security Union for the EU. Huge strides have been made across the full spectrum of the security policy field. Now, the reality of constantly evolving threats calls for continuous efforts with renewed motivation. Work on the legislative framework needs to be concluded in good time before the end of the parliamentary term in spring 2024. Member States have constant responsibilities to transpose, implement and apply new laws. Implementation calls for concerted efforts including with the support of the EU agencies – and very often for ever stronger cooperation with our international partners.

It is only with the collective and determined efforts of all concerned that we will achieve the levels of safety and security in the EU that citizens expect – and in today's circumstances, it should be a priority for every actor to play their part in strengthening EU security.