European Commission

The EU
Security Union Report

#SecurityUnion

May 2024

Printed by OIB in Belgium;

Manuscript completed in April 2024

Luxembourg: Publications Office of the European Union, 2024

Design: Marcus Marlowe and Joel Lepers — SG.A.5 — Foresight & Strategic Communication

PRINT	ISBN 978-92-68-15549-3	doi:10.2792/06445	KA-09-24-285-EN-C
PDF	ISBN 978-92-68-15550-9	doi:10.2792/59907	KA-09-24-285-EN-N

CONTENTS

I INTRODUCTION

In July 2020, the EU adopted its 2020-2025 Security Union Strategy ([1]). Designed at the peak of the COVID-19 pandemic, this Strategy was set against a backdrop of an increasingly complex security landscape, with hybrid and terrorist threats targeting the security of European citizens and businesses both in the physical and cyber spaces. The EU's response to these challenges was based on a holistic, whole-of-society approach to security, aiming at breaking down the silos between various security policies and connecting the dots across the whole European security ecosystem.

Four years on, the geopolitical, economic and security context within the EU and in its neighbourhood has profoundly and durably changed. The risks we face today are very different from those that dominated when the Security Union Strategy was first conceived. The COVID-19 pandemic shed light on the reliance of our societies and economies on information and communication networks as well as on connected products, and the need to ensure their cybersecurity in the face of booming and extremely adaptable cybercrime.

The level of terrorist threat on European soil remains and a number of Member States have recently raised their national threat rating to the highest level. The threat to stability from organised crime has continued to intensify, with the move online of much commerce and human interaction opening new avenues for criminal activity. As millions have been made more vulnerable by the instability in the EU's neighbourhood, smuggling of migrants and trafficking in human beings have become a key focus for those who make criminal profits by exploiting others. The instrumentalisation of migrants at our external borders highlighted new, hybrid forms of threats which, coupled with disinformation campaigns, aim to plant the seeds of division and mistrust in European societies. Finally, the potential exploitation by malicious actors of new technologies such as artificial intelligence, whether for cybercriminal purposes or information manipulation, raises new security challenges for our democracies, especially in a year marked by major electoral processes all across Europe.

Internal and external security are inter-connected. The Russian war of aggression against Ukraine has brought an increase in cyberattacks ([2]) and exposed the potential vulnerability of some EU critical infrastructure. The current situation in the Middle East and the unprecedented scale of violence in the region have intensified the challenges of maintaining the EU's internal security, with an intensified risk of terrorist attacks, whether by lone actors or organised groups, fuelled by attempts to spread terrorist content via online platforms and networks.

In this changing threat landscape, the vision set out in the Security Union Strategy has proven particularly relevant. While not all risks can be eliminated, vulnerabilities can be addressed, and the Security Union Strategy has provided a robust framework to build the EU's capacity to face existing and emerging threats with unity of purpose, and with improved collective mechanisms for action. This seventh Security Union progress report aims to provide an overview of the implementation of the Strategy since its adoption in 2020. While all the items initially highlighted in the Security Union Strategy have been addressed by the Commission, new initiatives have been incorporated to respond to evolving security challenges. The completion of outstanding files still pending approval by Parliament and Council, as well as enforcement and implementation of agreed legislation by Member States, is now crucial for the effective protection of EU citizens against security threats.

II A BETTER PROTECTED AND MORE RESILIENT PHYSICAL AND DIGITAL INFRASTRUCTURE

II.1. Critical infrastructure

Citizens, businesses and authorities in the EU rely on critical infrastructure, which underpins essential services like energy supply, water and food provision, transport and telecommunications. The everyday life of citizens, and the long-term health of the economy, are dependent on the delivery of these services. However, the geopolitical context in which critical infrastructure operates in the EU is highly volatile. This has been exacerbated by Russia's war of aggression against Ukraine, as increased hybrid attacks and the sabotage of the Nord Stream pipeline and the damage to the Baltic-connector gas pipelines have shown.

Since the beginning of this Commission's mandate, the EU has taken a variety of measures to enhance the protection of critical infrastructure and the resilience of the entities operating it, to avoid or mitigate the impact of disruptions to essential services. The EU has reinforced the legal framework to address current and future online and offline risks, from cyberattacks to natural disasters, with the adoption of the **Directive on the Resilience of Critical Entities** ('CER Directive') ([3]) and the revised **Directive on Network and Information Security** ('NIS2 Directive') ([4]). The Directives, once transposed by Member States, will ensure that risks and vulnerabilities affecting entities in a range of key sectors ([5]) are better taken into account. To speed up implementation of both Directives, a Council Recommendation ([6]) served as a basis for conducting stress tests with entities operating critical infrastructure, starting in the energy sector, where results are now being analysed by the Commission.

Recent events have also shown the need for urgent action at EU level when an incident occurs. The Commission has proposed ([7]) a **Council Recommendation on a Blueprint** setting out EU level coordination to respond to attempts to disrupt critical infrastructure with significant cross-border relevance. The **Internal Market Emergency and Resilience Act** will provide the means to ensure continued functioning of the internal market during a crisis.

The Commission has also taken action to enhance the resilience of critical infrastructure at **sectorial level**, building on the baseline established by the horizontal legislation. In the **energy sector**, work on the establishment of a Network Code on sector-specific rules for cybersecurity aspects of cross-border electricity flows will help make the EU's electricity system more resilient and secure. The Commission also announced the **Wind Power Action Plan** to reinforce the cyber-resilience of wind installations. In the **transport sector,** the Commission has continued work on the aviation and maritime security inspections system, with over 100 aviation inspections and 60 maritime inspections. Regarding **maritime security**, the revised EU Maritime Security Strategy ([8]) with its Action Plan was approved in October 2023 to better protect critical maritime infrastructure and ships from physical and cyber threats. The Commission is also developing a **Common Information Sharing Environment**, to facilitate information exchange between maritime authorities across borders and sectors. The review of the **trans-European transport network** Regulation ([9]) provides for new risk-proofing requirements for Member States to ensure that the Union's key transport infrastructure is effectively protected. Following an in-depth risk assessment of the EU's **connectivity infrastructure sector** with Member States and ENISA, the Commission made a number of recommendations to increase cybersecurity and resilience, such as setting out in February 2024 ([10]) actions to improve the security of the submarine cables infrastructures essential to our communication networks. The Communication on Managing **Climate Risks** identified main categories of action including the improved use of available satellite data and services to bolster the resilience of critical infrastructure ([11]).

In the **space sector**, the **EU Space Strategy for Security and Defence** ([12]), adopted in March 2023, includes actions to enhance the resilience of space sector systems and services, and to develop further EU space-based dual-use services. On **water systems**, the **Water Security**

Plan manual covers security measures to counter hostile actions against the physical and cyber integrity of water supply systems and deliberate waterborne contamination ([13]). In the **financial sector**, the adoption of the **Digital Operational Resilience Act (DORA)** ([14]) strengthens the digital resilience of EU financial sector entities by streamlining and upgrading existing rules. Finally, in the **health sector** as part of a European Health Union ([15]), the **Health Emergency and Response Authority (HERA)** supports the research and development, production and delivery of medical counter-measures. In addition, the EU early warning and response system's crisis management module is being scaled up to support the coordination of serious threats to health and health systems and ensure continuous coordination on health threats within the EU and at global level. The first six European Reference Laboratories for public health were nominated in March 2024 and the Union prevention, preparedness and response plan is under development and will be finalised and tested by the end of 2024.

II.2. Cybersecurity

The cyber threat landscape has significantly worsened over recent years, illustrated by the dramatic rise in supply chain attacks and the exploitation of vulnerabilities in software, operating systems for mobile devices or personal computers, and virtual private networks. Cyberattacks are increasing ([16]), targeting heavy industry, information services, government, and health. Ransomware continues to be a challenge, not only in terms of the number of attacks, but also of the increasing collusion of criminal gangs and of state actors driven by interests beyond financial gains ([17]). In the face of these increasing and evolving cyber threats, the EU has taken significant steps to enhance cybersecurity in Member States, reinforce the security of supply chains and products, strengthen solidarity at EU level and boost capacities to better detect, prepare for and respond to cybersecurity threats and incidents.

The current mandate has laid a strong foundation for the EU's ongoing efforts to safeguard its digital infrastructure. The **revision of the NIS Directive** extended its scope significantly to include all medium and large entities operating in 18 critical sectors, with stronger cyber security requirements, mandatory reporting of incidents and a European cyber crisis coordination structure laid down by law. Other achievements include the agreement reached on the **Cyber Resilience Act** ([18]) and the adoption of the **EU Digital Identity Regulation** ([19]), which will significantly bolster our overall cybersecurity. The Cyber Resilience Act will introduce mandatory cybersecurity requirements "by design" and "by default" for hardware and software, throughout the product's lifecycle, ensuring that products are delivered to the market without known vulnerabilities. The EU Digital Identity Regulation will facilitate the development of the digital single market on the basis of trusted services and will be a crucial element in efforts to address phishing attacks and improve authentication and access management. In the meantime, new rules under the **Radio Equipment Directive** will enter into force on 1 August 2025, setting obligations for the manufacturers of wireless devices to improve their level of cybersecurity, privacy and protection from fraud.

The **Cyber Solidarity Act** ([20]) will be a game-changer in terms of cyber threat detection, preparedness and incident response at EU level. It foresees a European Cybersecurity Alert System, which will consist of a pan-European network of Cyber Hubs, to build up coordinated EU detection capabilities and common situational awareness. A Cybersecurity Emergency Mechanism will reinforce preparedness and enhance response and recovery capacities of the Member States. The EU Cybersecurity Reserve will be created to support significant and large-scale cybersecurity incidents response and initial recovery, available to Member States, EU institutions and third countries associated to the Digital Europe Programme.

The **European Cybersecurity Competence Centre** should become fully autonomous this year and will increase Europe's cybersecurity capacities and competitiveness, shielding its economy and society from cyberattacks and enhancing its technological sovereignty through joint investments in strategic cybersecurity projects.

The adoption of the first-ever European **cybersecurity certification scheme** ([21])**,** with EU Common Criteria, is another important step to creating an environment across the internal market that businesses and consumers can trust. The Union Work Programme for European cybersecurity certification ([22]), adopted in February 2024, identifies strategic priorities for future European cybersecurity certification schemes. The Cybersecurity Act was amended to allow for cybersecurity certification schemes for managed security services which the Commission will request from ENISA once it enters into force. Work is underway on other schemes such as the European Cybersecurity Certification Scheme for Cloud Services, that will help users make informed decisions about the services they buy. The higher the levels of sensitivity of the data and of the assurance sought, the stricter the requirements in these schemes should be.

Meanwhile, the EU has taken steps to reinforce the **cybersecurity of EU institutions, bodies, offices and agencies** putting in place a framework for cybersecurity risk management, governance and control, strengthening the role of CERT-EU and establishing a new Inter-Institutional Cybersecurity Board to monitor and support its implementation. However, the lack of progress in the negotiations of the parallel proposal on information security, which is essential to complete a robust legislative framework for EU institutions, agencies and bodies and thus contribute to a secure European administration, should be addressed as a priority.

To complement the intense legislative work of recent years, the Commission has worked to step up **operational cooperation with Member States.** The establishment of the first cross-border networks of Security Operation Centres as well as the assistance provided to Member States

through the ENISA Support Action with EUR 35 million under the Digital Europe programme over the last two years have shown how the EU can build security for its citizens by pooling resources to boost cybersecurity capabilities.

To ensure economic security and open strategic autonomy, the EU has also taken a proactive approach to **addressing cybersecurity risks in emerging technologies**. Under the Economic Security Strategy, common risk assessments are being conducted on critical technologies such as AI, advanced semiconductors, and biotechnologies and quantum ([23]). To safeguard data and secure sensitive communication the Commission issued a Recommendation ([24]) calling on Member States to develop and implement a coordinated Roadmap for the transition to Post-Quantum Cryptography (PQC) across the EU. The Recommendation encourages Member States to support the development of relevant Post-Quantum Cryptography algorithms and standards to be implemented across the Union.

The **implementation of the EU 5G Cybersecurity Toolbox** ([25]) is key to ensuring 5G and post-5G networks and technologies linked to them are trustworthy and cybersecure. In line with the Toolbox, the Commission will seek to avoid exposure of its corporate communications to mobile networks using high-risk suppliers as well as to reflect its assessment in all relevant EU funding programmes and instruments ([26]). The EU's approach to cybersecurity now not only covers prevention and protection of critical infrastructure but also **crisis management,** including with the creation and formalisation of the **European Cyber Liaison Officers Network (EU-CyCLONe)**. The development of an ecosystem of stakeholders and networks for crisis management has stepped up the EU's preparedness for collective response in the event of a major cyber incident. Good coordination between the different levels (technical, operational and political) and strong synergies between the different cybersecurity communities requires regular exercises and interactions across sectors, risk assessments, stress-tests and documentation that is clear, up to date, and well understood by all actors.

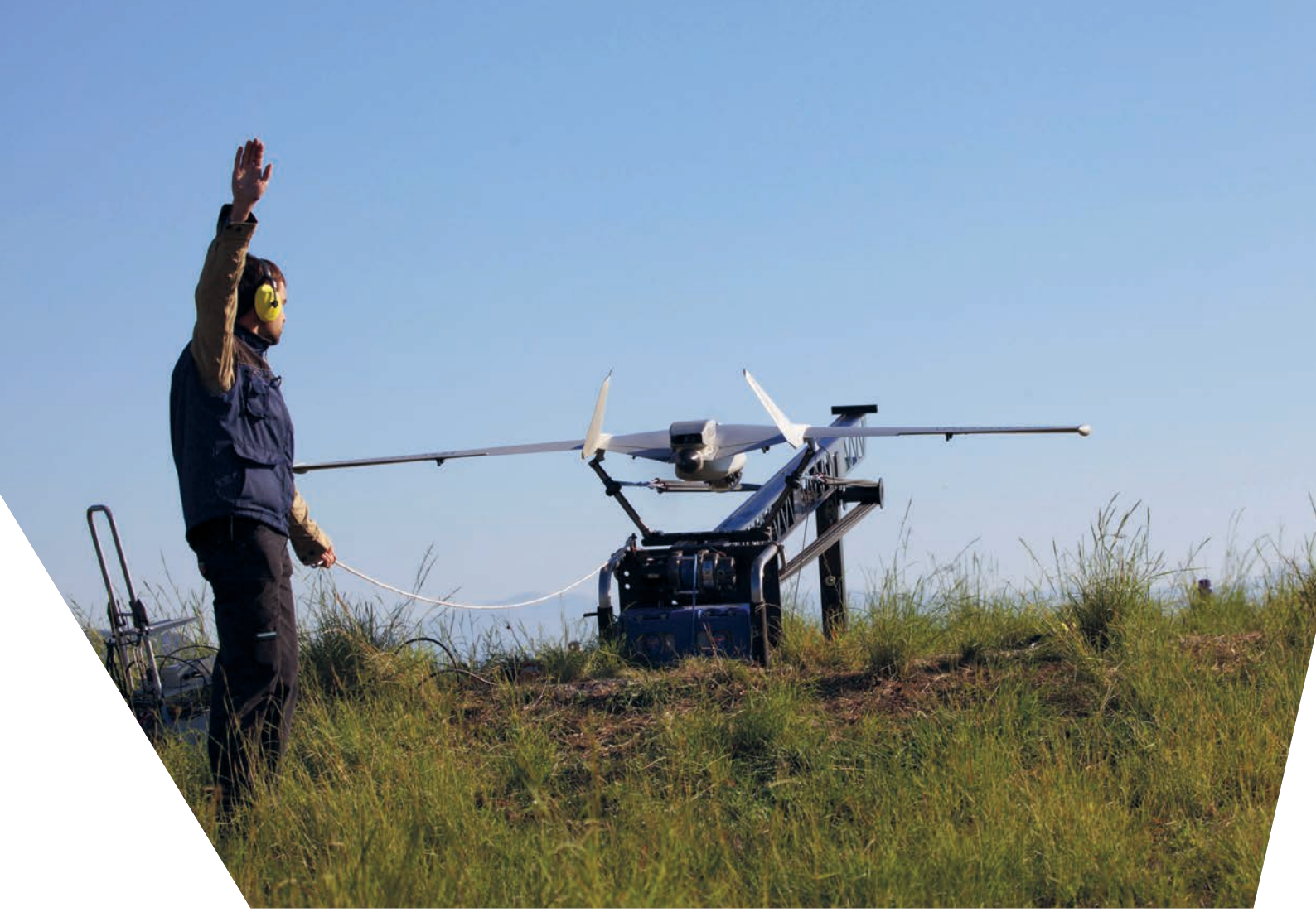
The EU's security and competitiveness depend on having a professional, skilled cybersecurity workforce. However, the EU faces a substantial shortage of cybersecurity professionals, which increases the risks to the EU, its Member States, businesses and citizens from cybersecurity incidents that may not be identified quickly or met with an adequate and timely response ([27]). The establishment of the **Cybersecurity Skills Academy** will help address this issue, by bringing together and improving the coordination of existing cybersecurity skills training initiatives. The increasing number of pledges to the Academy demonstrate the willingness of industry and the academic community to become major contributors in encouraging more professionals, including young women, to join the cybersecurity field.

The new EU **Cyber Defence Policy** establishes the means to improve coordination between the cybersecurity civilian communities with the military/defence eco-system, and the connections between these two fields are likely to grow in the future. The Policy also enables the EU and its Member States to strengthen their ability to protect, detect, defend and deter, making appropriate use of the whole range of defensive options available to the civilian and military communities for the broader security and defence of the EU, in accordance with international law. The new policy highlights the need for stronger collaboration between public and private sectors and proposes ways to make this happen.

The EU in action

Since the establishment of the Agency, ENISA has produced 70 situational awareness reports, with more than 4000 incidents analysed. It has handled 22 calls on large scale incidents. ENISA has co-organised a number of table-top cyber exercises, the most recent of which, co-hosted with the Commission, tested the preparedness of the European Cyber Crisis Liaison Organisation Network (EU-CyCLONe), which brings together Member States' national authorities in charge of cyber crisis management, and the Commission. Such exercises enhance coordination and thereby mitigate the impact of potential future attacks in the EU.

Under the Digital Europe Programme, the Commission is deploying a budget of EUR 84 million to support actions supporting cyber security under new EU legislation, including application of AI and other enabling technologies for Security Operation Centres, as well as Europe's transition to post-quantum cryptography. The European Cybersecurity Competence Centre will help ensure these projects benefit businesses, SMEs, and public administrations in Member States and associated countries.



III FIGHTING TERRORISM AND RADICALISATION

III.1. Counter-terrorism measures

The threat of terrorism remains acute and risks being affected by conflicts outside the EU. According to Europol ([28]), 28 completed, failed or foiled attacks were reported by Member States in 2022, an increase compared to 2021 (18 attacks) but well below the 56 attacks reported in 2020. Increased tensions in some communities in the Member States since the Hamas attack on 7 October 2023 have been seen in three terrorist attacks (Arras in France on 13 October, Brussels on 16 October and Paris on 2 December 2023). In parallel, some Member States face a significant threat from violent right-wing extremism. The glorification of terrorism as well as hate speech in particular in the form of antisemitism and anti-Muslim hatred are reported to be on the rise in the EU since 7 October 2023 ([29]).

Under the Security Union Strategy, a set of measures and tools have been adopted to support Member States in the fight against terrorism. Since its adoption in December 2020, the **EU Agenda on Counter-Terrorism** ([30]) has equipped the EU to better anticipate, prevent, protect and respond to terrorist threats. The Directive on combating terrorism ([31]) adopted in 2017 is now implemented by all Member States, criminalising training and travelling for terrorism, as well as terrorist financing. Shortcomings in the transposition of the Directive in a number of Member States are being addressed through infringement procedures and several workshops have been organised to ensure the legislation achieves its full impact through implementation.

Some **foreign terrorist fighters** have returned to the EU, but a significant number remain in camps and prisons in northeast Syria. While the primary responsibility lies with Member States, cooperation at EU level has helped Member States address challenges such as prosecution of those who have committed terrorist crimes, prevention of undetected entry into the Schengen area with systematic checks in the Schengen Information System making full use of its functionalities and the reintegration and rehabilitation of returned Foreign Terrorist Fighters. Both Europol and Eurojust played a key role in coordinating these investigations and prosecutions.

Depriving terrorists of the means to perform an attack is key in the fight against terrorism. New **legislation on firearms**

will impact the ability of terrorists to access weapons in the EU. New legislation designed to limit the accessibility of **explosive precursors** that terrorists could use to produce bombs came into force in February 2021 ([32]). Building on the approach used to regulate access to explosive precursors, the Commission has conducted an impact assessment on regulating the access to **high-risk chemicals.** Moreover, rapid advances in AI and biotechnology lower the barriers to access hazardous chemicals and pathogens, increasing the risk of chemical and biological events.

To **increase preparedness**, the Commission is building European strategic reserves of capacities through rescEU and the HERA to respond to chemical, biological, radiological, and nuclear threats. These strategic reserves ensure countermeasures, including equipment, are available to protect against the effects of incidents. The EU has continued to strengthen the EU framework to **prevent and combat money laundering and terrorist financing,** and closely monitors implementation to ensure that legislation contributes to detecting funds destined for the financing of terrorist organisations more effectively. In order to support investigations related to terrorist financing, the Commission also established **a network of counter-terrorism financial investigators** in 2021. The network, chaired by the Commission, supports exchanges among Member States' investigators on techniques and experiences in tackling terrorism financing.

The **protection of people and public spaces** is a priority of the Counter-Terrorism Agenda. Through the EU Protective Security Advisor Programme, more than 100 specially trained national and Commission experts are available to conduct, at the request of a Member State authority and funded by the Commission, vulnerability assessment missions to help keep public spaces, high-risk events and critical infrastructures in the EU safe from terrorist threats. As reflected in the Joint Communication by the Commission and the High Representative of 6th December 2023 ([33]) on "No Place for Hate: a Europe united against hatred", funding has been increased for the protection of public spaces and places of worship of all faiths. Since 2020, a budget of EUR 30 million has been provided through the **Internal Security Fund** to the PROTECT programme, which includes a particular focus on the protection of places of worship including synagogues and mosques: an additional EUR 5 million is helping to address specific threats from rising antisemitism. The Commission is working with civil society to combat hate speech, for example through the European Citizens' Panel on Tackling Hatred in Society.

Drones are an increasingly common and accessible tool that can be used for legitimate but also malicious purposes, including attacks on public spaces, individuals and critical infrastructure. In October 2023, the Commission adopted a Communication on countering threats posed by non-cooperative drones designed for civilian use ([34]). Among the key actions already implemented are the establishment of a counter drone expert group which will provide advice at policy and operational level, as well as a dedicated risk assessment on the threat posed by uncooperative unmanned aerials to civil aviation and airports facilities. The Commission has also carried out a **comprehensive mapping of aviation security risks** to take stock of existing and evolving threats and vulnerabilities with a view to updating the EU's aviation security regime baseline in EU airports ([35]).

III.2. Preventing and fighting radicalisation

Preventing radicalisation is the first step to preventing terrorist attacks. The Commission has strengthened its support to Member States to help prevent citizens being exposed to harmful extremist and terrorist content on and offline, including in prisons. Through the Radicalisation Awareness Network, the Commission brings together 6,500 practitioners (policy makers, law enforcement, researchers) from across Europe to develop best practice to address violent extremism. As of June 2024, the Radicalisation Awareness Network will be integrated into the EU Knowledge Hub for the Prevention of Radicalisation. With the **EU Knowledge Hub**, the EU aims to break down silos between relevant policy makers, practitioners and researchers, providing in-depth studies, foresight scenarios, support for response to geopolitical developments, training in strategic communication, as well as tools to develop counter radicalisation policies and practice. The Commission has also adopted a Recommendation on the procedural rights of suspects and accused subject to pre-trial detention and on material detention conditions ([36]), which includes measures to address the issue of radicalisation in prisons.

The EU is also working to prevent foreign influence and funding fostering radical/extremist views in the Member States. The Commission remains vigilant to prevent EU funds being used to support any project incompatible with European values or pursuing an illegal agenda. The revised Financial Regulation ([37]) now includes conviction for "incitement to hatred" as a ground for exclusion from EU funding. In January 2024, the Commission issued new guidelines to financial programme managers on the consequences of breaches of EU values.

Disinformation intended to incite hatred, and terrorist content circulates online, including AI-generated images, and may inspire acts of violent extremism. A key instrument to prevent terrorist content from circulating online is the **Regulation on addressing the dissemination of terrorist content online** ([38]), which obliges hosting service providers to take terrorist content down or block access to it within one hour of receiving a removal order from Member States' authorities. In its evaluation report adopted in February 2024, the Commission reported that the Regulation has been effective in preventing the spread of terrorist content online So far, 23 Member States have appointed competent authorities to issue removal orders and approximately 500 removal orders were issued between June 2022 and April 2024. In parallel shortcomings in the transposition of the Regulation in a number of Member States are being addressed through infringement procedures.

The Commission has also published a set of Guidelines for teachers and educators on tackling disinformation and promoting digital literacy through education and training.

What is illegal offline must also be outlawed online. The enforcement of the **Digital Services Act** ([39]), applicable from 17 February 2024, is a decisive step in this direction with obligations on all online platforms to counter illegal content. Another element of the EU Counter-Terrorism toolbox is the **EU Internet Referral Unit in Europol** which refers terrorist content to over 300 platforms and increasing awareness of and action on terrorist propaganda. The **EU Internet Forum** also supports the tech industry in moderation of extremist content and is currently addressing the risk terrorist exploitation of generative AI, complementing legislative developments, notably the Artificial Intelligence Act ([40]). Following the Christchurch attack in March 2019, the EU Internet Forum endorsed the EU Crisis Protocol to ensure cooperation between law enforcement and industry in the aftermath of a crisis.

III.3. Protecting victims of terrorism

The Commission set up the EU Centre of expertise for **victims of terrorism** in January 2020 to offer expertise, guidance and support to national authorities and victim support organisations. The EU Centre is helping to ensure that the EU rules on victims of terrorism are correctly applied, promoting exchange of best practice and sharing of expertise.

The EU in action

In 2022, 28 terrorist attacks were completed, failed or foiled. 380 individuals were arrested in Member States in 2022 for terrorism-related offences. 14 of them concerned terrorism financing, all related to jihadist terrorism**. Eurojust** supported actions in 203 cases, including the work of 8 Joint Investigation Teams. Under the Regulation on preventing the dissemination of terrorist content online 350 removal orders have been carried out since June 2022.

With the support of the Commission, Member States have put in place risk assessment tools, special detention regimes, rehabilitation and reintegration programmes, training for prison and probation staff, structures for information exchange and multidisciplinary cooperation for management of ex-offenders after release.

The Regulation on addressing the dissemination of terrorist content online has shown its worth, for example in enabling the swift removal of terrorist content after the attack perpetrated by Hamas against Israel on 7 October 2023.

IV FIGHTING ORGANISED CRIME

Organised crime is a threat to European citizens, businesses, state institutions as well as the economy as a whole. Criminal networks are involved in a variety of criminal activities, including drugs trafficking, organised property crime, environmental crime, fraud, migrant smuggling and trafficking in human beings. Cybercrime and gender-based cyber violence have been further stimulated by the increased use of internet and online services. In addition, the disruption caused by the Russian war of aggression against Ukraine has created new openings, swiftly exploited by organised crime groups. Criminals easily operate online and across borders, which creates a need for consistent European-level and transnational action. **The EU Strategy to tackle Organised Crime 2021-2025** ([41]), adopted by the Commission in April 2021, highlights the importance of dismantling organised crime structures, targeting the individuals at the top of criminal organisations in particular those groups that pose the greatest risk to Europe's security.

IV.1. Cybercrime

While technological developments bring important and rapid improvements to our society, they also enable cybercriminals to exploit the border-free nature of the digital world. Between May 2021 and June 2022, there were 3,640 reported ransomware attacks against EU businesses and institutions and in 2023, the total ransomware payments rose above EUR 1 billion for the first time ([42]). Crimes ranging from large scale cyber-attacks to activities using malware, spyware, phishing and spam interfere with the functioning of digital and physical infrastructures and seriously impact on people's lives. To tackle these crimes, the EU has adopted a number of legislative and non-legislative measures to boost cross-border cooperation at EU and international level.

In 2021 the EU joined the **International Counter Ransomware Initiative** which brings together the efforts of more than 50 EU and third-country partners to hold **ransomware** actors accountable for their crimes and deny them a safe haven. The initiative helps prevent ransomware actors from profiting from illicit proceeds, to disrupt their activities and bring them to justice.

With over a hundred million pictures and videos depicting child sexual abuse reported worldwide in 2023 alone, and many more unreported, **child sexual abuse** is alarmingly pervasive. Children spending more time online has made them more susceptible to grooming, leading to an increase of self-produced exploitation material. In line with the **EU Strategy for a more effective fight against child sexual abuse** ([43]) and the **EU Comprehensive Strategy on the Rights of the Child** ([44]), the Commission adopted a proposal laying down rules to prevent and combat child sexual abuse ([45]), with new obligations on online service providers. Where prevention fails to reduce a significant risk, service providers could be ordered to detect, report, remove and block child sexual abuse online. The proposal would also create a **dedicated EU Centre** to facilitate implementation of the regulation. Temporary legislation adopted to allow online service providers to continue voluntary detection and reporting of child sexual abuse online has been extended until 3 April 2026, to allow enough time to find an agreement on the long-term regulation. This initiative was complemented by a proposal to update the **2011 Directive on combating sexual abuse and sexual exploitation of children and child sexual abuse material** ([46]). The revised rules expand the definitions of offences notably to keep pace with increasing online criminal activity and introduce higher penalties and more specific requirements for prevention and assistance to victims.

It has been estimated that half of all young women experience **gender-based cyber violence** ([47])**.** The **Directive on combating violence against women and domestic violence** adopted in May 2024 criminalises certain forms of violence that disproportionately affect women notably the non-consensual sharing of intimate images (including deepfakes), cyber stalking, cyber harassment and misogynous hate speech. The Directive will also strengthen victims' access to justice.

IV.2. Drug trafficking

The **drugs** illicit trade is one of the most significant security threats faced by the EU today. The EU retail drug market is estimated to be worth at least EUR 30 billion annually ([48]). Seizures of cocaine in the EU are hitting record levels ([49]). There is growing concern over the production and proliferation of synthetic drugs in Europe and the link of drugs trafficking to violence ([50]). The **EU Agenda and Action Plan on Drugs 2021-2025** ([51]) sets out concrete actions to step up action at the EU level, including efforts underway to reinforce international cooperation on drugs trafficking, and the transformation of the European Monitoring Centre for Drugs and Drug Addiction into the **EU Drugs Agency** ([52]). The Agency will start its operations in July 2024.

The Agenda has been complemented by the **EU Roadmap** adopted by the Commission in October 2023 ([53]),which sets out additional measures to fight drugs trafficking and organised crime, including the establishment of a new **European Ports Alliance** to increase the resilience of ports against criminal infiltration by reinforcing the work of customs authorities, law enforcement, public and private actors in ports across the EU. Implementation of the Roadmap has also led to a thematic Schengen evaluation which assessed Member States' capabilities regarding police cooperation, protection of external borders, and management of IT systems to combat drug trafficking identifying 40 best practices.

IV.3. Illegal trafficking of goods

Illegal trafficking of goods is a highly profitable business, and the costs to society do not come only from missing revenue, but in dangers to citizens' health and safety, requiring a coordinated response from governments, law enforcement, and private actors.

Firearms trafficking feeds organised crime within the EU as well as in its neighbourhood. An estimated 35 million illicit firearms are 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 new technologies such as 3D printing, trafficking of firearms is finding new ways to escape controls. Together with the **2020-2025 EU action plan against firearms trafficking** ([54]), all Member States have now transposed the **Firearms Directive** ([55]) in their national law, which brings substantial improvements to security by making it harder to legally acquire the most dangerous weapons. The Council and the European Parliament have also reached an agreement on the revised **rules on export authorisation, import and transit measures for firearms** ([56]) to improve the traceability of civilian firearms, with a broader focus on digitalisation.

The illicit trafficking of cultural property is also a lucrative business for organised crime groups, and in some cases for conflict parties and terrorists ([57]). The Commission adopted an EU action plan in December 2022 to strengthen the fight against the **trafficking in cultural goods** ([58]), including a dialogue with stakeholders to foster a fair and reputable art market that protects cultural heritage.

IV.4. Migrant smuggling and trafficking in human beings

It is estimated that more than 90 % of migrants who arrive in the EU without authorisation, use the services of smugglers. Profits from smuggling migrants are estimated between EUR 4.7-6 billion worldwide annually, while deaths from this criminal trade in the Mediterranean Sea alone since 2014 are estimated to have been over 28 000.

To enhance efforts against **migrant smuggling**, the Commission proposed to update the current legislative framework ([59]) with a proposed directive, which aims to ensure a more effective pursuit and prosecution of smugglers and a proposed regulation to strengthen EU coordination by reinforcing the **European Centre Against Migrant Smuggling** in Europol and improving the sharing of information between responsible authorities. The Commission calls on the European Parliament and the Council to find

an agreement on these files as soon as possible. In parallel, the Commission launched a **Global Alliance to Counter Migrant Smuggling** on 28 November 2023, with a **Call to Action**, which is now being implemented with relevant stakeholders. In April 2024 the Commission hosted an event to create a community of stakeholders and competent authorities to tackle the use of digital services in migrant smuggling. The Commission is also supporting law enforcement and judicial authorities of key third countries to boost their capacity to investigate and prosecute organised smuggling and trafficking groups.

Many of the criminal networks engaged in migrant smuggling are also involved in **trafficking of human beings**. Europol estimates the global profits from trafficking in human beings to be more than EUR 29.4 billion annually ([60]). The majority of victims are women and girls, but trafficking in men is also on the rise particularly for labour exploitation. In April 2021, the EU Strategy on Combatting Trafficking in Human Beings 2021-2025 ([61]) provided a comprehensive framework for action. The recently revised Anti-trafficking Directive covers new forms of exploitation (exploitation of surrogacy, of forced marriage and of illegal adoption), reinforces the tools for law enforcement and judicial authorities and requires Member States to sanction people who knowingly use services reliant on the victims of trafficking. Eurojust, in cooperation with the EU Anti-trafficking Coordinator, has put in place a Focus Group of specialised prosecutors against human trafficking.

IV.5. Environmental crime

Environmental crimes often cause irreversible and long-term damage to people's health, as well as ecosystems and the environment. They are highly lucrative and often involve organised crime but are hard to detect and prosecute. Environmental crime is the third largest criminal activity in the world in terms of proceeds, with illicit conduct and profits increasing significantly each year ([62]), and currently.

While the criminal profits related to this crime are estimated at EUR 200 billion annually, with significant negative impacts on the economy, the damage to our environment, biodiversity, human health and security has no price. EU level action to crack down on environmental crime has been strengthened through **the new Environmental Crime Directive** ([63]), which expands the scope of offences to be investigated and prosecuted and provides for concrete types and levels of penalties for natural and legal persons who committed environmental crimes. Further action has been taken by adopting the regulation on waste shipments and by targeting illegal logging more effectively by introducing new rules on deforestation-free products. In addition, the revised **EU Action Plan against wildlife trafficking** updates the EU's priorities to better prevent and address root causes of this phenomenon.

IV.6. Economic and financial crime

Money laundering and the financing of terrorism pose a serious threat to the integrity of the EU economy and financial system and the security of its citizens. Europol has estimated that around 1% of the EU's annual Gross Domestic Product is involved in suspect financial activity ([64]).

The EU has agreed upon new rules to **prevent money laundering and terrorism financing**, to enhance the prevention and detection of attempts by criminals to launder illicit proceeds or finance terrorist activities through the Union's financial system ([65]), laying down directly applicable Union-wide requirements for private sector operators, including the carrying out of customer due diligence and reporting of suspicions. Tasks and powers of national supervisors and Financial Intelligence Units will be reinforced and harmonised to ensure that responsible authorities perform their tasks more effectively and cooperate more efficiently. In addition, clear rules strengthen the preventive function of beneficial ownership and bank registers. A **new Anti-money Laundering Authority** will be established and will have direct supervisory powers over the riskiest cross-border entities in the financial sector and provide operational support to the Financial Intelligence Units' joint analysis of cross-border cases.

In addition to the new anti-money laundering rules, the recently adopted **directive on asset recovery and confiscation** will be an important tool in the fight against serious and organised crime, establishing stronger measures to confiscate illicit profits from a broad range of crimes. Asset Recovery Offices will have a mandate to identify, trace and freeze criminal assets. In combination with the recently adopted **directive on the criminalisation of the violations of Union restrictive measures**, which harmonises the definition and penalties for such criminal offences across the Union, these rules will also allow for the tracing, freezing, management and confiscation of benefits gained by criminal actors through the violation of Union sanctions.

IV.7. Anti-corruption

Corruption brings major societal damage, undermining public institutions, their delivery of public policies and services, and the trust of citizens in democratic institutions. Corruption in the private sector undermines the single market and gives new opportunities to organised crime.

To address the risks and challenges linked to corruption, the Commission proposed ([66]) a **Directive on combating corruption**, to strengthen rules criminalising corruption offences and harmonising penalties across the EU. The European Parliament adopted its position in February 2024. To ensure there are no hiding places for corruption in the EU the Commission calls on the Council to move forward with its discussions and support the objectives of the Commission's proposal.

Specific rules to protect the EU budget from criminal activities, including corruption, are laid down in the **PIF Directive** ([67]). Together with the proposed anti-corruption directive, robust implementation of this measure is imperative to keep the EU's finances safe from fraud

and corrupt activities, and the Commission plays its part in this through infringement procedures when necessary. OLAF and the **European Public Prosecutor's Office** play a key role in this, investigating irregularities and prosecuting crimes affecting the Union's financial interests ([68]). The new **EU network against corruption** ([69]), which serves as a forum for all stakeholders in the EU to exchange good practices, opportunities, ideas and plans for further work, met for the first time in September 2023.

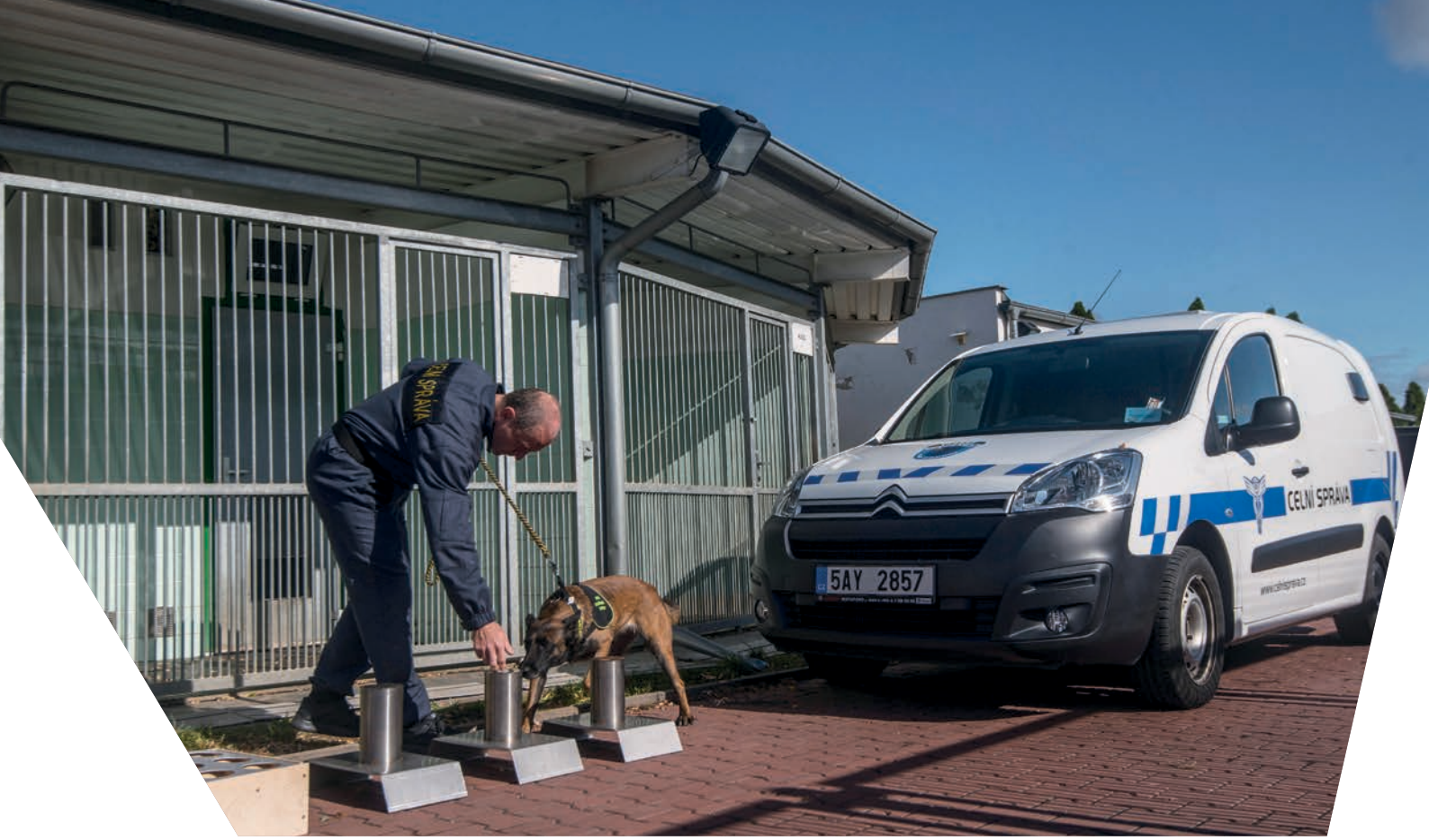
IV.8. Protecting victims of crime

Victims of all kinds of crime deserve support and attention. The Commission has already achieved most of the actions under its first **EU Strategy on victims' rights (2020-2025)** ([70]). On 12 July 2023, the Commission proposed a Directive amending the 2012 **Victims' Rights Directive** ([71]), to further strengthen the rights of all victims of crime in the EU, in particular the rights of the most vulnerable victims.

The EU in action

On 5 April 2024, as a key deliverable of the EU Roadmap to fight drug trafficking and organised crime, Europol published a report with a first mapping of the most threatening criminal networks. The findings show that 821 high-risk criminal networks, composed of altogether 25,000 members, pose the greatest threat. 34% of high-risk criminal networks are active in the EU for more than 10 years, 76% of them are present or active in up to 7 countries, and their members represent 112 nationalities.

In a crackdown on cross border crime ("Operation Mobile 6"), 400 law enforcement officers from 25 countries recovered 505 stolen cars, 2000 car parts, 16 boats, 32 outboard engines and 248 forged documents. 209 alleged people smugglers were stopped. In 2022 and 2023, the EPPO conducted a major investigation, extending over 30 countries, into organised crime groups suspected of being responsible for cross-border VAT fraud estimated at EUR 2.2 billion (Operation Admiral).



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

In an area without internal border controls, police officers in one Member State should have access to the information available to their colleagues in another Member State. The norm must be effective cooperation. This is why it is essential to reinforce the tools available to law enforcement and judicial authorities across the EU for information exchange and cross-border cooperation.

As highlighted in the 2024 State of Schengen report ([72]), the continuous strengthening of the **Schengen area**, tackling shortcomings revealed in evaluations, and targeting collective efforts with more concerted Schengen governance, contributes not only to free movement but to the security of citizens across Europe. Underpinning the well-functioning of the Schengen area are three pillars: effective management of the EU's external borders, strengthening internal measures to compensate for the absence of internal border controls, in particular on police cooperation, security and migration management, and ensuring robust preparedness and governance. ([73])

External border management will be strengthened with new legislation on screening ([74]) of irregular arrivals. The new definition of instrumentalisation of migrants ([75]) will help tackle exploitation of migrants in hybrid attacks at the EU external border, as seen for example at the border with Belarus in 2021. Effective migration management with a seamless process at the border ([76]) will reinforce the Schengen area by ensuring closer cooperation and responsibility-sharing among Member States. The Schengen Borders Code, once adopted, will bring greater EU coordination and will better equip Member States to deal with emerging challenges at the EU's common external border and within the Schengen area, while the EU Agencies will continue helping Member States to maintain a high level of internal security in the Schengen area.

The **police cooperation package** ([77]) offered a major upgrade of the tools available to improve cross-border operations, provide clear channels and timeframes for exchanging information between law enforcement forces across Member States and give **Europol** a stronger role. In addition, revised rules on **automated exchange** will help close information gaps, boost the prevention, detection and investigation of criminal offences in the EU. Important progress was made as well in developing effective tools to ensure the smooth travel by air to, from and within the EU, while enhancing the capacity for authorities to detect security threats, by revising the legal framework for the use of **Advance Passenger Information**.

Concerning terrorism, the amendment to the **Eurojust Regulation** regarding digital information exchange in terrorism cases adopted in 2023 ([78]) will make the exchange of information between the national authorities responsible and Eurojust more efficient through the Judicial Counter-Terrorism Register.

Prosecuting cybercriminals requires particular forms of evidence and vital progress has been made to enhance cross-border cooperation in **exchanging electronic evidence**. The Second Additional Protocol to the Council of Europe's Budapest Convention ([79]) is expected to step up the fight against cybercrime by strengthening the possibilities for judicial authorities to collect electronic evidence of a criminal offence (for example, through setting up joint investigation teams). The EU internal **e-evidence rules** ([80]), adopted in 2023, will introduce a new system for obtaining electronic evidence in criminal proceedings by allowing law enforcement and judicial authorities to directly address private service providers located in another Member State.

Artificial intelligence has become a versatile and crucial component in the technologies available to law enforcement and other internal security actors; at the same time, its deployment for this purpose should respect fundamental rights. Generative AI can, however, also be used by cybercriminals to organise sophisticated cyber-attacks and other malevolent activities. The **Regulation on Artificial Intelligence (AI Act)** is a first step to regulate AI use within the EU, providing guardrails for the responsible use of AI systems in this area whilst safeguarding the fundamental rights and safety of citizens. The AI Office will support implementation of the Act, ensuring respect of its safeguards and procedural requirements. The Commission will contribute to the development of appropriate guidance to support law enforcement and other security actors on appropriate and effective use of AI in their work.

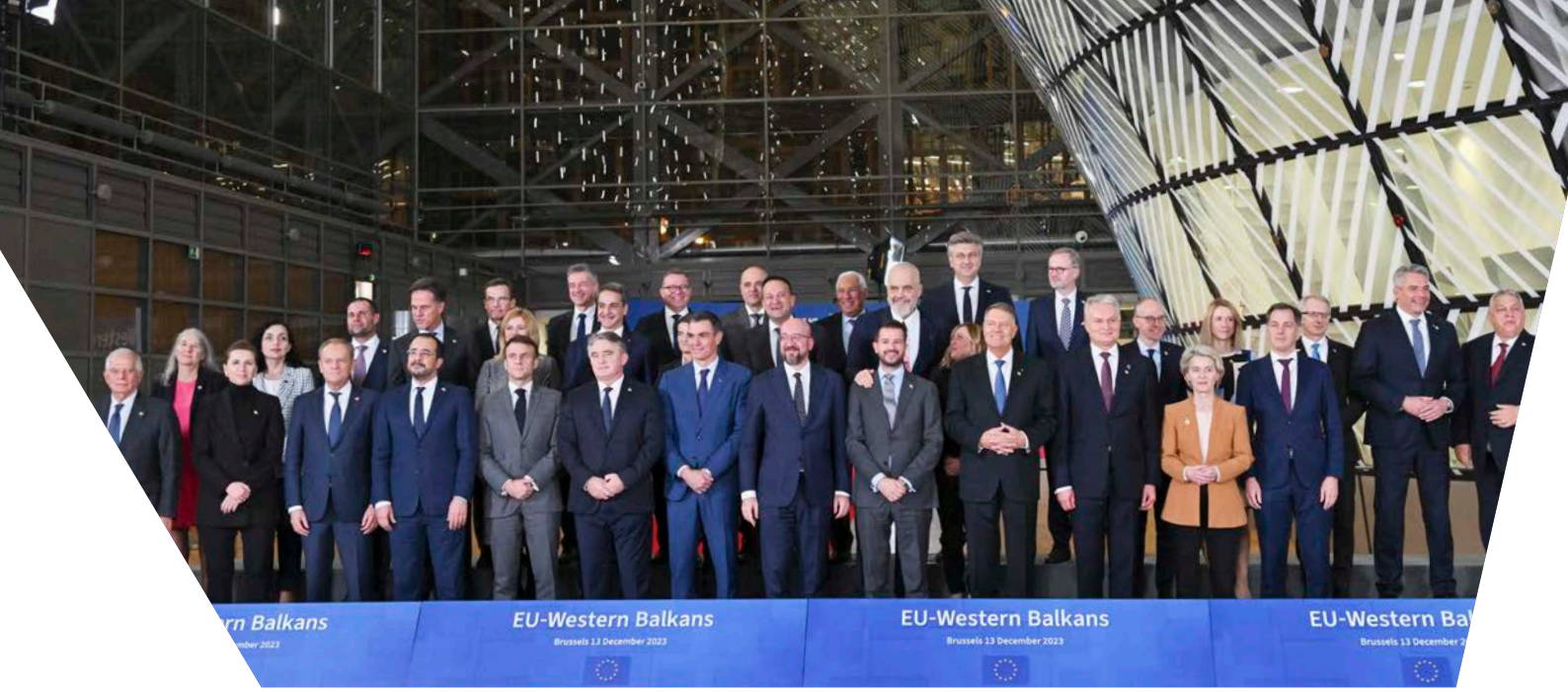
While work continues towards an **EU critical communication system,** a new regulation establishing a collaboration platform for joint investigation teams ([81]) provides those involved with secure means for exchange of evidence and information, efficient communication and easy cooperation with third countries.

With an increase of cross-border crime, the EU is increasingly confronted with situations where several Member States have jurisdiction to prosecute the same case. The new rules **on the transfer of proceedings in criminal matters** will help prevent inefficient duplication of proceedings and avoid cases of impunity where surrender under a European arrest warrant is refused, while ensuring that the rights of suspects and victims are duly respected. Efficient cross-border judicial cooperation requires secure, reliable and time-efficient communication between courts. This will now be possible thanks to the **Digital Justice Package**. Authorities will be able to communicate with each other and exchange case-related data in civil, commercial and criminal matters through secure, reliable digital channels. This will facilitate the fight against crime and swift implementation by the Member States will be key.

The EU in Action

In 2022, the EMPACT led to:

- 9922 arrests
- identification of 4019 victims of trafficking of human beings
- arrest of 3646 migrant smugglers
- seizure of over EUR 180 million in assets and money seized
- seizure of over 62 tonnes of drugs



VI INTERNAL-EXTERNAL SECURITY NEXUS: SECURITY IN THE EU, ITS NEIGHBOURHOOD AND IN PARTNER COUNTRIES

The increasing interconnection between internal and external security has only become more evident in the past few years given the current geopolitical context. The EU is safer when its partners are safer too. In 2023 alone, around EUR 700 million were spent to assist the capacities of third countries and reinforce our cooperation with them on countering terrorism and preventing and countering violent extremism, 72% being devoted to Africa given growing instability and the presence of terrorist groups in Sahel. This is five times the expenditure 10 years ago. Meanwhile, law enforcement cooperation with third countries has been mainstreamed in all EMPACT operational action plans.

The Commission acted quickly to pre-empt internal security threats stemming from Russia's war of aggression against **Ukraine,** ensuring maximum vigilance regarding exploitation of the conflict and flows of those seeking safety in Europe by organised crime and trafficking groups. The Commission services and the EEAS, with the EU Counter-Terrorism Coordinator, agreed with Ukraine to establish a structured internal security dialogue, including in areas such as trafficking of firearms and border management. The Cyber Dialogue between the EU and Ukraine, together with coordinated political, technical, financial and material support from the EU, has helped Ukraine to strengthen its cyber resilience. The announced EU Defence Innovation office in Kyiv will act as a bridge between EU start-ups and innovators and Ukrainian industry and Armed Forces, including in the cyber defence realm. It will help transmit technological breakthroughs that can have an impact on the battleground.

The Republic of **Moldova** is also very much exposed to the criminal and security implications of Russia's invasion of Ukraine and a range of hybrid and cyber threats. In July 2022, the Commission services, in cooperation with the EEAS, launched an EU support Hub for Internal Security and Border Management with the Republic of Moldova. The EU is supporting Moldova to improve its resilience and ability to counter hybrid and cyber threats, including through the implementation of the recommendations of the relaunched hybrid risk survey, and through the EU Partnership Mission in the Republic of Moldova.

Given their proximity, the security of Western Balkans partners is closely related to the EU's internal security, and law enforcement cooperation between the EU and the **Western Balkan countries** has continued to intensify during this mandate. The Joint Action Plan on Counter Terrorism signed with all Western Balkan partners in 2018 has been taken forward with good progress, and where most actions were completed in North Macedonia, Albania, and Montenegro, updated arrangements have been signed. The EU also continues to enhance the collective cyber resilience of Western Balkans partners, through operational and technical support, training and involvement of the region in EU cybersecurity mechanisms.

The current situation in the **Middle East** also has a potential impact on the EU's internal security including a significant increase of incidents in some Member States. The Counter Terrorism Financial Investigators Network has enabled Member States to share information on cases related to the fundraising activities of Hamas in the EU, providing investigators with a better understanding of how to tackle such threats.

In the light of developments in **Afghanistan**, in coordination with the Commission, the High Representative, the Presidency and key EU Agencies, the EU Counter Terrorism Coordinator drew up a Counter-Terrorism Action Plan on Afghanistan, endorsed by the Council in October 2021. The EU remains engaged in Afghanistan and is strengthening its role in the broader region through enhanced cooperation on security-related matters **with Central Asian countries** and a Counterterrorism Dialogue with **Pakistan**.

The EU has boosted cooperation with countries in **Latin America and the Caribbean,** in particular regarding the fight against organised crime, drugs trafficking and financing of terrorism.

Multilateral cooperation lies at the core of the EU's approach. The EU works closely with the UN, with the United Nations Office of Counter-Terrorism and the Counter-Terrorism Committee Executive Directorate in particular. The EU also works with the 40+ UN entities which make up the UN Global Counter-Terrorism Coordination Compact. Since September 2022, the EU has co-chaired the Global Counterterrorism Forum with Egypt, as a multilateral forum supporting civilian aspects of countering terrorism and violent extremism, with a strong focus on Africa. The EU is also a non-military partner of the Global Coalition against Da'esh and actively engages with NATO, Interpol, and the OSCE. In the field of anti-money laundering and counter terrorism and proliferation financing, the Commission actively contributes to the work of the Financial Action Task Force. Engagement in the Global Coalition on countering Da'esh is an important component of the EU's foreign policy response to terrorism/violent extremism and related threats.

The EU has substantially deepened and expanded its **cooperation with NATO** in particular in areas such as resilience, critical infrastructure, health security, countering cyber and hybrid threats, including disinformation, military mobility, space, emerging and disruptive technologies, and climate and defence. A Structured Dialogue on Resilience was launched in January 2022, reinforced by the EU-NATO Task Force on the resilience of critical infrastructure. In June 2023, the Task Force published a report mapping the current security challenges for critical infrastructure in four key sectors (energy, transport, digital infrastructure and space). The implementation of the recommendations for further EU-NATO cooperation contained in the report is progressing at pace, with a focus on exercises, civil-military coordination, and engagement with the private sector.

The revised implementing guidelines of the **EU Cyber Diplomacy Toolbox** allow for the development of sustained, tailored, coherent and coordinated strategies towards persistent cyber threat actors, better addressing the challenges of continued lower-level grey-zone threats and activities stemming from persistent cyber threat actors. The EU continues work on enhancing cyber resilience, supporting partners, and promoting the UN framework of responsible behaviour in cyberspace, and secure digital infrastructure through Global Gateway. The EU has intensified **cooperation on cyber security with NATO** through a dedicated Structured Dialogue, **and with international partners**. The dialogue with the United States, leading to the EU-US Joint Cyber Safe Action Plan, the joint technical work to map and compare legislation and efforts on standardisation is a good example of the EU's concrete cooperation with partners to support global cybersecurity. In 2023, the EU also resumed cyber dialogues with Japan and India and launched the first one with the United Kingdom, enabling exchanges on the threat landscape, cyber capacity building and cooperation in multilateral and regional forums.

In recent years, the EU has established **Counter-Terrorism Dialogues** with key partner countries and multilateral organisations, including the UN, Australia, Egypt, India, Pakistan, Saudi Arabia, Turkey, and the US. The EU also has a Network of 20 Counter Terrorism/Security Experts deployed in EU Delegations throughout the world to support EU foreign and security policy objectives relating to countering terrorism and violent extremism. The Commission continues to work to eliminate online terrorist content from the internet while respecting fundamental freedoms in the spirit of the Christchurch Call to Action ([82]). As part of the implementation of the Trade and Cooperation Agreement, the first round of EU-UK dialogues on cyber and counter-terrorism took place in December 2023 and February 2024.

In relation to **drug trafficking**, the High-Level meeting of the EU-CELAC Coordination and Cooperation Mechanism on Drugs in February 2024 led to the adoption of a Declaration ([83]) identifying priorities for cooperation for the five years to come. The EU contributes to the work of the Global Coalition to Address Synthetic Drug Threats launched by the United States. The European Monitoring Centre for Drugs and Drug Addiction is increasing cooperation with Colombia, Ecuador and Chile through the conclusion of Working Arrangements.

Effective **asset recovery and confiscation measures** at global level are essential in the fight against serious and organised crime. The Commission is committed to ensuring a common EU approach in the upcoming negotiations on an additional protocol to the Council of Europe's Warsaw Convention on Laundering, Search, Seizure and Confiscation of the Proceeds from Crime and on the Financing of Terrorism, which needs updating, considering the rapidly evolving criminal landscape and international developments. The Commission adopted in April 2024 a Recommendation for a Decision seeking the Council's authorisation for the Commission to negotiate the protocol on behalf of the EU.

In a context of **hybrid threats** that are growing in complexity and sophistication, implementing the EU Strategic Compass for Security and Defence is of crucial importance. The Commission services and the European External Action Service have contributed to creating the EU Hybrid Toolbox, which provides a framework for a coordinated response to hybrid campaigns, bringing together all relevant internal and external tools and measures. The EU Operational protocol for countering hybrid threats updated in April 2023

helps to ensure an effective application of processes and tools in response to hybrid threats throughout the whole crisis management cycle. EU hybrid rapid response teams are being set up to provide short-term tailored assistance in countering hybrid threats in EU Member States and partner countries.

The strategic and coordinated use of **foreign information manipulation and interference** (FIMI) poses a clear threat to our own security, and that of our partners as half the globe heads to the polls in 2024. In recent years, building on the European Democracy Action Plan and through implementation of the EU Strategic Compass for Security and Defence, the EU has stepped up its action in countering FIMI and set up a Commission taskforce on Strategic Communication to help to advance responses.

Foreign interference attempts have been put into stark relief by allegations of corruption through payments made by third countries to politicians in the EU. The risk of foreign interference is particularly intense in the run-up to the European elections. To streamline information sharing ahead of the elections, the Council has activated in April 2024 the integrated political crisis response (IPCR) arrangements.

The **EU Strategic Compass and the Threat Analysis** recognise that climate change and environmental degradation have growing impact in the fields of peace, security, and defence. These factors combined with water scarcity pose a threat for fragile contexts in EU neighbourhoods and can lead to displacement crises, internal turmoil or interstate disputes. In June 2023, the Commission and the High Representative for Foreign Affairs and Security Policy adopted a Joint Communication on the Climate and Security nexus ([84]).

In December 2023, the **Defence of Democracy** package set out how to use transparency standards for interest representation to protect EU democracies from the risk of covert interference ([85]) and explained the work of the EU on tackling disinformation, such as intensive real-time exchanges between the institutions, use of fact-checking networks, and intensive work with the key platforms through the Code of Practice on Disinformation and now the Digital Services Act.

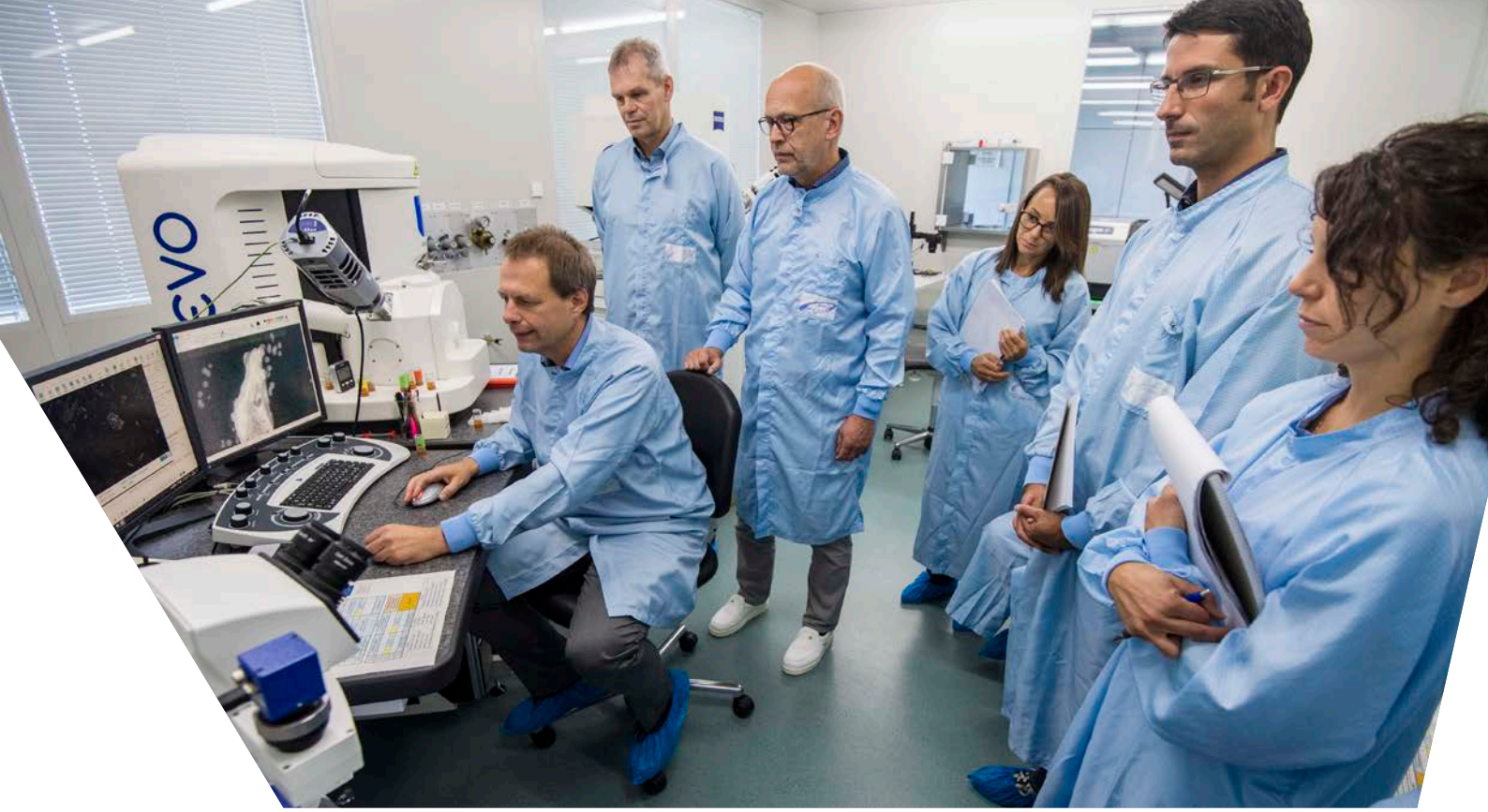
The EU in action

In a globalised world, where serious crime and terrorism are increasingly transnational, cooperation and information exchange between law enforcement and judicial authorities of third countries is essential.

Europol and Eurojust have signed cooperation agreements with third countries to enhance the exchange of information in their fight against terrorism and organised crime. An agreement between the EU and New Zealand on the exchange of personal data with Europol entered into force in July 2023 and agreements are under negotiation with Europol with Bolivia, Brazil, Mexico, Peru and Ecuador.

Eurojust facilitates judicial cooperation to fight serious crime also with third countries, through 13 Cooperation Agreements, with international judicial networks, through working arrangements, and within a network of over 70 jurisdictions worldwide and through contact points. 12 liaison prosecutors from third countries are seconded to Eurojust. Agreements are under negotiation on international judicial cooperation with Eurojust with Brazil, Argentina and Colombia.

ENISA has also strengthened its cooperation and international outreach and it has recently signed Working Arrangements with the Ukrainian and the USA cybersecurity agencies.



VII IMPLEMENTING THE SECURITY UNION

The proper implementation of the Security Union is a shared responsibility, where every actor has to play its part. The Commission supports Member States' strategies, policy, legislation, organisation and capacity building to implement the work of the Security Union, including through the Technical Support Instrument.

VII.1. Infringements

While EU law has now cemented robust new rules to better protect EU citizens, it is the responsibility of Member States to timely transpose, implement and apply such rules. The level of implementation by Member States of EU legislation in the Security Union area is mostly satisfactory, but in this sensitive area, there is no room for weak links.

Whenever necessary, the Commission fulfills its duty to make use of infringement procedures and refers Member States to the Court of Justice of the EU to address breaches of EU law. Thanks to close cooperation between the Commission and Member States, many of the infringement procedures launched for legislation under the Security Union Strategy have been addressed.

VII.2. Role of EU agencies and bodies

EU agencies and bodies in justice, home affairs, and cybersecurity play a key role in the implementation of the EU security acquis which continues to increase as their responsibilities expand. This cooperation has led to concrete results, as shown for instance by **EMPACT,** which facilitates structured multidisciplinary cooperation of Member States, supported by all EU institutions, bodies and agencies. The operations performed by EMPACT including through dedicated Operational Task Forces coordinate the efforts of Member States and operational partners in fighting criminal networks and serious crime.

ENISA has been key in strengthening EU capacities to prevent, detect, deter and respond to cyberattacks, while promoting cyber resilience, safeguarding our communication and data and keeping online society and economy secure. Through expert advice and support on cybersecurity issues, including through situational awareness reports and risk assessments, it facilitates cooperation and information sharing among Member States, EU institutions, and other stakeholders. Its tasks have been strengthened in line with the new cybersecurity rules. The recent update of the Compendium on Elections Cybersecurity and Resilience or the report on best practices for cyber crisis management are some examples of ENISA's contribution to cybersecurity.

The **European Cybersecurity Competence Centre**, together with the Network of National Coordination Centres, is Europe's new framework to support innovation and industrial policy in cybersecurity. Once fully established, the Centre and the Network will make strategic investment decisions and pool resources to improve and strengthen technology and industrial cybersecurity capacities. The Centre will thus play a key role in delivering on the cybersecurity objectives of the Digital Europe and Horizon Europe Programmes.

Europol has since 2022 a reinforced mandate to better support the EU Member States in combating terrorism,

serious and organised crime. Europol is now able to support Member States in using emerging technologies and developing common technological solutions. It is also now able to receive data directly from private parties (helping to tackle, for example, online dissemination of child sexual abuse material). In addition, Europol's Executive Director can now propose a national investigation if a crime in a single Member State affects a common interest covered by a Union policy. The mandate also strengthens Europol's data protection framework and the oversight of the European Data Protection Supervisor. The continuous work of Europol has led to many successful operations such as the Encrochat case which has so far led to over 6,500 arrests worldwide. The mandate also strengthens Europol's data protection framework and the oversight of the European Data Protection Supervisor.

In October 2023, an amendment of the **Eurojust** Regulation entered into force, enhancing Eurojust's ability to identify links between terrorism investigations and prosecutions, to establish a modern Case Management System, to provide a secure digital communication channel between Member States and Eurojust, and to facilitate cooperation with third countries. The amendment also ensures that Eurojust has powers for to the preservation, analysis and storage of evidence relating to core international crimes.

Since the start of its operational activities in June 2021, the **European Public Prosecutor's Office** has proved to be essential to investigate and prosecute offences affecting the financial interests of the Union, when the focus is on crimes against the Union budget. By 31 December 2023, the EPPO had 1 927 active investigations, for estimated damage of over EUR 19.2 billion. With 139 indictments filed in 2023, the EPPO started to bring more suspects of EU fraud to judgment in front of national courts.

Frontex has also been active in security matters while performing its border related tasks, particularly in the field of migrant smuggling, as well as maritime security and trafficking in human beings. In January 2024, Frontex and Europol signed an agreement outlining how the two Agencies can better coordinate activities to complement each other and identify concrete priority actions to be achieved in the short and long term. In practice, Frontex's role is to provide intelligence from its border surveillance and monitoring. Europol's role on the other hand is to provide a law enforcement response to organised cross-border crime and terrorism within the EU. Moreover, Frontex, the **European Maritime Safety Agency**, and the **European Fisheries Control Agency** strengthened their cooperation with the renewal of the tripartite working arrangement on coast guard functions in 2021, contributing to enhanced security at sea.

VIII LOOKING AHEAD

The wealth of legislative and operational measures taken in the last four years have left the EU better equipped to face security challenges than it was at the beginning of this Commission's mandate. However, the constantly evolving landscape of threats means that every opportunity must be taken to address potential vulnerabilities. **The current strategy was adopted with a horizon up to 2025. Work will need to be taken forward after that date with constant vigilance and determination.**

The concept of security, traditionally centred on military and home affairs, has to keep pace with changing threats. Risks and vulnerabilities have to be taken into account from economic security, to supply disruptions and crisis preparedness, and encompassing practically every sector of our society, from health, environment/climate to energy and transport. The digital dimension is now fundamental to all aspects of security, and divisions between online and offline threats are progressively being overtaken by new realities, with most threats including a cyber element and a hybrid character. The current situation has also shown more than ever the intrinsic links between the internal and external dimensions of security. Therefore, **constant efforts are needed to ensure that security aspects are embedded in all EU policies** and decision-making processes.

The European Economic Security Strategy of 20 June 2023 complements the "whole of society approach" proposed in the EU Security Union Strategy by adding a strategic component that focuses on defending the interests of the EU, its Member States and citizens against threats to our economy or using economic means. It sets out a framework for achieving **economic security** by promoting the EU's economic base and competitiveness; protecting against risks; and partnering with the broadest possible range of countries to address shared concerns and interests and this will be **a key element in considerations of the EU's security in the future**.

The new EU Cyber Defence Policy is just one area that demonstrates the need to **improve coordination between civilian communities and the military/ defence eco-system**, and the connections between these two fields are likely to grow in the future.

Criminals are quick to adapt and deploy new technologies in their activities. A **High-Level Group on access to data for effective law enforcement**, co-chaired by the Commission and the Presidency of the Council, has been considering challenges faced by law enforcement practitioners, in particular the access to data. Future reflections on security will need to **explore how law enforcement can make use of digital technologies,** while ensuring that fundamental rights are fully respected when it comes to access to data in areas such as quantum communication infrastructure, Artificial Intelligence and advanced surveillance technologies.

Future security policies will have to continue seeking effective responses to developing risks. This will require a re-thinking of how EU institutions and bodies as well as Member States should respond to challenges and guarantee the EU's capacity to respond swiftly when necessary. **Silos and response mechanisms that duplicate risk assessment or complicate crisis response must be avoided**.

Furthermore, as the EU continues to show its ability to adapt to changing risks, new vulnerabilities should not be allowed to develop through unequal implementation of instruments already agreed. **Effective implementation and application of legislation at national level is essential**.

While the EU's capacity has been strengthened by the growing role in security of the EU agencies, it **can be optimised by further enhancing coordination and complementarity between the agencies**. Consideration could be given to deepening cooperation not only between Agencies traditionally working in security matters such as Europol, Eurojust, and ENISA, as well as Frontex and the European Public Prosecutor Office, but also sectorial agencies, including the new EU Drugs Agency, the Anti-money Laundering Authority, the EU Aviation Safety Agency, the European Maritime Safety Agency, and the European Fisheries Control Agency.

The 2020-2025 Security Union Strategy consolidated the EU's security toolbox and now provides a powerful foundation for the protection of Europeans in the future. Going forward, actions taken on all Security Union strands will remain essential to ensure that the EU is able to adapt, even in the face of exceptional and unexpected threats.

Endnotes

.(1) COM(2020) 605.
(2) ENISA Threat Landscape 2023, pp. 10-11.
(3) Directive (EU) 2022/2557 of 14 December 2022 on the resilience of critical entities.
(4) Directive (EU) 2022/2555 of 14 December 2022 on measures for a high common level of cybersecurity across the Union.
(5) Sectors covered by the NIS2 and CER Directives include energy, transport, banking, financial market infrastructure, digital infrastructure, health, drinking water, wastewater, public administration, space and food production, processing and distribution.
(6) The Commission proposal COM(2022) 551 was followed by Council recommendation 2023/C 20/01.
(7) COM(2023) 526.
(8) JOIN (2023) 8.
(9) **Provisional agreement of 24 April 2024 on the Regulation of the European Parliament and of the Council on Union guidelines for the development of the trans-European transport network**.
(10) C(2024) 1181.
(11) COM (2024) 91.
(12) JOIN(2023) 9 final.
(13) JRC Publications Repository — Water Security Plan Implementation Manual for Drinking Water Systems.
(14) Regulation (EU) 2022/2554 of 14 December 2022 on digital operational resilience for the financial sector.
(15) Communication on the European Health Union.
(16) ENISA Threat Landscape 2023, pp. 10-11.
(17) See for instance: **https://www.nationalcrimeagency.gov.uk/news/ransomware-criminals-sanctioned-in-joint-uk-us-crackdown-on-international-cyber-crime**
(18) Provisional agreement was reached on 30 November 2023. It is expected to enter into force in 2024.
(19) Provisional agreement was reached on 8 November 2023.
(20) COM(2023) 209.
(21) C(2024) 560, adopted on 31 January 2024.
(22) SWD(2024) 38.
(23) C(2023) 6689.
(24) C(2024) 2393.
(25) NIS Cooperation Group 1/2020, *Cybersecurity of 5G networks EU Toolbox of risk mitigating measures.*
(26) C(2023) 4049.
(27) ENISA, *Foresight Cybersecurity Threats for 2030 – Update 2024.*
(28) Europol 2023, European Union Terrorism Situation and Trend report 2023.
(29) See: isdglobal.org, 31 October 2023; isdglobal.org, 2 November 2023.
(30) COM(2020) 795.
(31) Directive (EU) 2017/541 of 15 March 2017 on combating terrorism.
(32) Regulation (EU) 2019/1148 of 20 June 2019 on the marketing and use of explosives precursors.
(33) JOIN(2023) 51.
(34) COM/2023/659.
(35) SWD(2023) 37 final.
(36) Commission Recommendation (EU) 2023/681 of 8 December 2022.
(37) A provisional political agreement was reached on 7 December 2023.
(38) Regulation (EU) 2021/784 of 29 April 2021 on addressing the dissemination of terrorist content online.
(39) Regulation (EU) 2022/2065 of 19 October 2022 on a Single Market for Digital Services (Digital Services Act).
(40) Provisional political agreement was reached on 08 December 2023.
(41) COM(2021) 170.
(42) ENISA Threat Landscape for Ransomware Attacks.
(43) COM(2020) 607, adopted in July 2020.
(44) COM(2021) 142, adopted in March 2021.
(45) COM/2022/209, adopted in May 2022.
(46) COM/2024/60, adopted in February 2024.
(47) European Parliamentary Research Service (EPRS), Combating gender-based violence: Cyberviolence, European added value assessment, 2021.
(48) Europol, 2024.
(49) 303 tonnes of cocaine were seized in 2021. European Drug Report 2023, EMCDDA.
(50) In early 2024 two officers were killed in Barbate (Spain) by suspected drug traffickers and a number of shootings connected to drugs violence took place in Brussels (Belgium), with several injured and dead.
(51) COM(2020) 606.
(52) Regulation (EU) 2023/1322 of 27 June 2023 on the EU Drugs Agency (EUDA).
(53) COM/2023/641 final.
(54) COM(2020) 608 final.
(55) Directive (EU) 2021/555 on control of the acquisition and possession of weapons.
(56) COM(2022) 480.
(57) See for example United Nations Security Council Resolutions 2199 (2015), 2253 (2015), 2322 (2016), 2347 (2017), 2462 (2019) and 2617 (2021); G20 Culture Ministers Rome Declaration of 30 July 2021.
(58) COM(2022) 800.
(59) COM/2023/754 and COM/2023/755.
(60) Study on the economic, social and human costs of trafficking in human beings within the EU (2020).
(61) COM(2021) 171.
(62) **Organized crime groups pushing environmental security to tipping point (interpol.int)**.
(63) Directive 99/2008/EC on the protection of the environment through criminal law.
(64) Europol Financial Intelligence Group, From suspicion to action (2017).
(65) COM/2021/420, COM/2021/421, COM/2021/422 and COM/2021/423.
(66) COM/2023/234.
(67) Directive (EU) 2017/1371 of 5 July 2017 on the fight against fraud to the Union's financial interests by means of criminal law. Since December 2021, the Commission launched 19 infringement proceedings for non-compliance with the PIF Directive.
(68) Poland formally joined the European Public Prosecutor's Office in February 2024.
(69) JOIN(2023) 12.
(70) COM(2020) 258.
(71) COM/2023/424.
(72) COM(2024)173.
(73) In March 2024, Bulgaria and Romania became Schengen members who fully apply the Schengen acquis and internal border controls have been lifted at air and sea borders.
(74) COM(2020)612.
(75) COM(2020) 613.
(76) Regulation establishing a common procedure for international protection in the Union, COM(2016) 467 final and COM(2020) 614 final.
(77) COM/2021/780, COM/2021/782, and COM/2021/784.
(78) Regulation (EU) 2023/2131 as regards digital information exchange in terrorism cases.
(79) Adopted by the Committee of Ministers on 17 November 2021.
(80) Regulation (EU) 2023/1543 of 12 July 2023 on European Production Orders and European Preservation Orders for electronic evidence in criminal proceedings and for the execution of custodial sentences following criminal proceedings, and Directive (EU) 2023/1544 of 12 July 2023 laying down harmonised rules on the designation of designated establishments and the appointment of legal representatives for the purpose of gathering electronic evidence in criminal proceedings.
(81) Regulation (EU) 2023/969 of 10 May 2023 establishing a collaboration platform to support the functioning of joint investigation teams.
(82) Christchurch call to action launched by France and New Zealand in 2019.
(83) EU-CELAC Coordination and Cooperation Mechanism on Drugs — La Paz declaration, 22 February 2024.
(84) JOIN(2023) 19.
(85) COM(2023) 637.

KA-09-24-285-EN-N

Publications Office
of the European Union

Design by SG.A5
Printed by OIB
ISBN 978-92-68-15550-9