Council of the European Union

Brussels, 3 April 2025
(OR. en)

7750/25

JAI 415	**COPEN 79**
COSI 55	**FREMP 76**
ENFOPOL 109	**RELEX 413**
CRIMORG 59	**CFSP/PESC 530**
ENFOCUSTOM 53	**PROCIV 32**
IXIM 73	**CIVCOM 85**
CT 42	**COPS 157**
COTER 48	**IPCR 22**
CORDROGUE 43	**HYBRID 29**
CYBER 87	**DISINFO 20**
MIGR 121	**TELECOM 104**
FRONT 80	**DIGIT 58**
ASIM 28	**MI 197**
VISA 51	**COMPET 226**
SCHENGEN 20	**UD 73**
JAIEX 32	**ENV 237**
CATS 13	**TRANS 114**
DATAPROTECT 59	**CULT 27**
DROIPEN 36	**RECH 138**

COVER NOTE

From:	Secretary-General of the European Commission, signed by Ms Martine DEPREZ, Director
date of receipt:	2 April 2025
To:	Ms Thérèse BLANCHET, Secretary-General of the Council of the European Union
No. Cion doc.:	COM(2025) 148 final
Subject:	COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS on ProtectEU: a European Internal Security Strategy

Delegations will find attached document COM(2025) 148 final.

Encl.: COM(2025) 148 final

EUROPEAN
COMMISSION

Strasbourg, 1.4.2025
COM(2025) 148 final

COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS

on ProtectEU: a European Internal Security Strategy

1. ProtectEU: A European Internal Security Strategy

Security is the bedrock upon which all our freedoms are built. Democracy, the rule of law, fundamental rights, the wellbeing of Europeans, competitiveness and prosperity – all hinge on our ability to provide a basic security guarantee. In the new era of security threats that we now live in, EU Member States' ability to guarantee security for their citizens is more than ever contingent on a **unified, European approach to protecting our internal security**. In an evolving geopolitical landscape, Europe must continue to make good on its enduring promise of peace.

The first steps towards building a European security apparatus have already been taken. In the last decade, we have equipped the Union with improved collective mechanisms for action in the areas of law enforcement and judicial cooperation, border security, the fight against serious and organised crime, counter terrorism and violent extremism and the protection of the EU's physical and digital critical infrastructure. The proper implementation of previously adopted legislation and developed policies remains key.

The nature of today's threats and the intrinsic link between the EU's internal and external security require us to go further.

The threat picture is stark. Lines between **hybrid threats** and open warfare are blurred. Russia has been waging an online and offline hybrid campaign against the EU and its partners, to disrupt and undermine societal cohesion and democratic processes, and to test the EU's solidarity with Ukraine. Hostile foreign states and state-sponsored actors seek to infiltrate and disrupt our critical infrastructure and supply chains, to steal sensitive data and position themselves for maximum disruption in the future. They use crime as a service and criminals as proxies. Moreover, our dependencies on third countries in terms of supply chains make us more vulnerable to hybrid campaigns by hostile states.

Powerful **organised crime networks** are proliferating in Europe, nurtured online and spilling into our economy and affecting our society, as highlighted in the EU Serious and Organised Crime Threat Assessment (SOCTA) recently presented by Europol[1]. Once organised crime has a foothold in a community or economic sector, eradicating it becomes an uphill battle: one third of the most threatening criminal networks are active for over ten years. Cryptocurrencies and parallel financial systems help them launder and hide their criminal proceeds.

The **terrorist threat level in Europe continues to loom.** Regional crises outside the EU create a ripple effect, providing new motivation for terrorist actors across the entire ideological spectrum to recruit, mobilise or build up their capacities. They target their radicalisation and recruitment efforts specifically towards the most vulnerable sections of our societies and in particular certain young people. They inspire lone actor attacks and a surge in anti-system extremism whose goal is to disrupt the democratic legal order.

The leaps and bounds of **technological advancement** are providing essential tools for enhancing our security apparatus. But cyberattacks and foreign information manipulation are increasingly prevalent, exploiting new technologies like artificial intelligence. Children, young and elderly people are particularly at risk online and the spread of online hate threatens freedom of expression and social cohesion.

Our lives have become less secure, and this is increasingly felt by Europeans, whose **perception of safety and security in the EU** has been eroded to the point that, when asked about the future,

[1] https://www.europol.europa.eu/cms/sites/default/files/documents/EU-SOCTA-2025.pdf

64 percent tend to be worried about the EU's security.[2] Businesses are also increasingly concerned; misinformation and disinformation, crime and illicit activity and cyber espionage all feature among the top ten risks identified in the World Economic Forum Global Risks Report 2025[3].

Europeans should be **able to go about their lives free from fear**, whether on the streets, at home, in public places, on the metro, or on the internet. The protection of people, especially those most vulnerable to attacks, which tend to disproportionately affect children, women and minorities, including Jewish and Muslim communities, is at the heart of the EU's work on security. This is essential to build resilient and cohesive societies.

The Commission is setting out a **European Internal Security Strategy** to better counter threats in the years to come. With a sharper legal toolbox, deeper cooperation and increased information sharing, we will enhance our resilience and collective ability to anticipate, prevent, detect and respond effectively to security threats. A unified approach to internal security can support Member States to harness the power of technology to strengthen, not weaken security, while promoting a secure digital space for all. In addition, it supports a common response by Member States to global political and economic shifts affecting the Union's internal security.

This strategy is guided by **three principles** and embeds in its core the respect for the rule of law and fundamental rights.

First, it sets the ambition of a change of culture on security. We need **a whole-of-society approach** involving all citizens and stakeholders, including civil society, research, academia and private entities. The actions under the strategy therefore take an integrated, multi-stakeholder approach wherever possible.

Second, **security considerations need to be integrated and mainstreamed across all EU legislation, policies and programmes**, including EU external action. Legislation, policies and programmes will need to be prepared, reviewed and implemented with a security perspective in mind, making sure that the necessary security considerations are addressed so as to promote a coherent and comprehensive approach to security.

Finally, a safe, secure and resilient Europe requires **serious investment by the EU, its Member States and the private sector**. The priorities and actions set out in this Strategy require sufficient human and financial resources to ensure their implementation. As laid down in the Communication on the road to the next multiannual financial framework[4], Europe will need to increase public spending for security and promote security research and investment, enhancing its strategic autonomy.

This Strategy complements the **Preparedness Union Strategy**[5], which sets out an integrated all-hazards approach to preparedness for conflicts, human-induced and natural disasters, and crises, and the **White Paper for European Defence Readiness 2030**[6], which supports the development and acquisition of defence capabilities across the EU to deter foreign adversaries. The Commission will also propose a **European Democracy Shield** to strengthen democratic resilience in the EU. Together, these initiatives set out a vision for a safe, secure and resilient EU.

[2] Flash Eurobarometer FL550: EU Challenges and Priorities.
[3] https://reports.weforum.org/docs/WEF_Global_Risks_Report_2025.pdf, p.17.
[4] COM (2025) 46 final.
[5] JOIN (2025) 130 final.
[6] JOIN (2025) 120 final.

A new European internal security governance

The Commission will work closely with the Member States and EU agencies to upgrade the EU's approach to internal security at both strategic and operational level.

This will be done by:

- **consistently identifying potential security and preparedness implications of new and revised Commission initiatives from the start and throughout the negotiation process**
- **regular meetings of the Commission Project Group on European Internal Security, supported by strategic cross-sectoral collaboration across the Commission**
- **presentations of the threat analyses related to internal security to support the work of the Security College**
- **discussions with Member States in the Council on the evolving internal security challenges based on the threat analysis and exchange on key policy priorities**
- **regular reporting to the European Parliament and the Council to track and support systematic implementation of key security initiatives**

2. Integrated situational awareness and threat analysis

We will equip the EU with new ways of sharing and combining information and provide a regular EU internal security threat analysis, contributing to a comprehensive risks and threats assessment.

Security starts with **effective anticipation**. The EU must rely on comprehensive, sufficiently autonomous, and up-to-date situational awareness and threat analysis. Actionable intelligence, which Member States are encouraged to enhance further through the Single Intelligence Analysis Capacity (SIAC), as the single point of entry for Member States' intelligence, is vital for assessing and countering threats, ultimately informing policy and legislative actions[7]. We need to leverage **intelligence-based analysis** and **threat assessments** at the EU level more effectively and collaboratively.

Building on the various risk and threat assessments produced at EU level and for specific sectors[8], the Commission will prepare **regular EU internal security threat analyses** to identify the main security challenges, with a view to informing policy priorities. These will help develop an agile and responsive internal security policy that effectively addresses evolving threats, better protects people and businesses against attacks, and enables targeted policy interventions in a timely manner. These EU internal security threat analyses will also contribute to **the EU comprehensive (cross-sector, all-hazards) risks and threats assessment** developed by the Commission and the High Representative, as set out in the Preparedness Union Strategy.

Trust and secure handling are essential for information sharing, and this requires reliable and secure infrastructure. EU institutions, bodies and agencies need to ensure their ability to use **secure communication channels** for exchanging sensitive and classified information between themselves and with Member States. Investments in **interoperable secure systems** and reliable technology will reinforce the EU's autonomy and strengthen the EU's ability to manage crises

[7] Safer Together – Strengthening Europe's Civilian and Military Preparedness and Readiness, p. 23.

[8] Sectoral Threat Assessments that will contribute to inform this threat analysis include the EU Serious and Organised Crime Threat Assessment (SOCTA), the EU Terrorism Situation & Trend Report (TE-SAT), the Joint Cyber Assessment Report (JCAR), and future assessments of money laundering and terrorist financing threats, risks and methods to be carried out by the Commission and the Anti-money Laundering Authority.

and ensure operational resilience. In this context, the Commission urges co-legislators to finalise negotiations on the **proposed Regulation on information security in the institutions, bodies, offices and agencies of the Union**, notably to ensure a common framework for the handling of sensitive non-classified and classified information[9].

To ensure its own operational security and situational awareness, the Commission will revise its corporate security governance framework and establish an **Integrated Security Operations Centre (ISOC)** to protect people, physical assets, and operations across all Commission sites. The Commission will also boost its operational and analytical capacities for identifying and mitigating hybrid threats.

In line with the Preparedness Union Strategy, preparedness and security considerations will be integrated and mainstreamed across EU legislation, policies and programmes. When preparing or reviewing legislation, policies or programmes with a preparedness and security perspective in mind, the Commission will consistently identify potential impacts of the preferred policy option on preparedness and security. This will be underpinned with regular training for policy makers in the Commission.

To support Member States, the Commission will discuss the evolving internal security challenges and key policy priorities with the Council and regularly update it on the implementation of the Strategy. Additionally, the Commission will keep the European Parliament and relevant stakeholders informed and engaged in all relevant actions.

Key actions

The Commission will:

- **develop and present regular threat analyses for EU internal security challenges**

Member States are urged to:

- **enhance intelligence sharing with SIAC and ensure better information sharing with EU agencies and bodies**

The European Parliament and the Council are encouraged to:

- **finalise negotiations on the proposed Regulation on information security in the institutions, bodies, offices and agencies of the Union**

3. Strengthened EU security capabilities

We will develop new tools for law enforcement, such as a revamped Europol, and better means of coordinating and ensuring secure data exchange and lawful access to data.

To effectively counter evolving threats, the EU must enhance its security capabilities and foster innovation. As the primary actors against internal security threats, law enforcement and judicial authorities need the right operational tools and capabilities to act promptly and effectively. It is important that these authorities are able to communicate and coordinate across borders and across services to efficiently prevent, detect, investigate and prosecute.

EU agencies and bodies for internal security

EU agencies and bodies in justice, home affairs, and cybersecurity play a key role in the EU's security architecture – a role that continues to increase as their responsibilities expand.

[9] COM (2022)119 final

Today, 25 years after its establishment, **Europol** is more central than ever to the EU's security framework. It supports complex cross-border investigations, facilitates information exchange, develops innovative tools for policing and provides advanced expertise for law enforcement. However, several factors prevent Europol from fully reaching its operational potential in supporting investigative and operational activities to counter cross-border crime: they range from an insufficient level of resources to the fact that its current mandate does not cover new security threats, such as sabotage, hybrid threats or information manipulation. This is why the Commission will propose **an ambitious overhaul of Europol's mandate**, to turn it into a truly operational police agency, better supporting Member States. The aim is to bolster Europol's technological expertise and capacity to support national law enforcement agencies, to enhance coordination with other agencies and bodies and with Member States, to reinforce strategic partnerships with partner countries and the private sector, and to ensure a strengthened oversight of Europol.

Furthermore, the Commission will work to further **improve the effectiveness and complementarity of EU agencies and bodies for internal security and bolster seamless cooperation** between them.

Eurojust's mandate will be assessed and strengthened for more effective judicial cooperation, enhancing complementarity and cooperation with Europol. This includes enhancing Eurojust's efficiency as well as its capacity to provide proactive support and analysis to Member States' judicial authorities. Furthermore, given the **EPPO's** unique competence to investigate and prosecute crimes affecting the Union's financial interests, the Commission will consider how best to improve the EPPO's capacity to protect Union funds. This will include strengthening cooperation between the EPPO and Europol.

Efficient and secure information exchange between agencies is crucial for cooperation. Europol and Frontex need swift mutual exchange of information, including for operational purposes, following up on the Joint Statement of January 2024[10]. **eu-LISA** has a central role in ensuring secure storage and availability of data for better coordination and more efficient information exchange between agencies. The **EU Agency for Fundamental Rights** provides expertise on protecting fundamental rights in the development and implementation of security policies.

The **EU Anti-Money Laundering Authority (AMLA)** has been empowered to crossmatch information, on a hit/no-hit basis, against information made available by Europol, the EPPO, Eurojust and the EU Anti-Fraud Office to carry out joint analyses of cross-border cases.

ENISA plays a central role in the implementation of European cybersecurity legislation. In the upcoming **revision of the Cybersecurity Act**, the Commission will assess its mandate and propose to modernise it to strengthen its EU added value.

Cooperation between customs and other law enforcement authorities will be increased with the proposed creation of the **EU Customs Authority** and the **EU Customs Data Hub** under the EU Customs Reform package. Information from the future Hub and related data from Europol, Eurojust, the EPPO, OLAF, AMLA and Frontex, in the framework of their respective competences, will enhance joint analysis and contribute to more coherent operational activities, in particular at the external borders. The Commission encourages the co-legislators to quickly complete the negotiations on the EU Customs Reform and will continue to assist them to this end.

[10] https://www.europol.europa.eu/cms/sites/default/files/documents/europol-frontex_joint_statement_signed_31.1.2024.pdf.

The enhancement of the complementarity between the EPPO, OLAF, Europol, Eurojust, AMLA and the proposed EU Customs Authority will also build on the results of the ongoing review of the **EU Anti-Fraud Architecture**. Internal security can benefit from this holistic approach, focusing on better use of both criminal and administrative means, interoperability of IT systems and improved cooperation.

Critical Communication

Today, **critical communication systems**[11] are operated, in most cases, in isolation at national level. This means first responders often cannot communicate with their counterparts when crossing the border into other Member States. In some Member States, there are also limitations on communications between different types of first responders (e.g. police and ambulances). The standards of most systems do not meet today's requirements in terms of functionality and resilience, significantly limiting the reaction capacity of first responders, especially across borders.

To improve the EU's capacity to react to crises, the Commission will propose legislation to create a **European Critical Communication System (EUCCS)** to link Member States' next generation critical communication systems in the EU. The aim is for the EUCCS to be based on three strategic pillars: operational mobility, strong resilience and strategic autonomy. The EUCCS initiative will set harmonised requirements and help modernise Member States' critical communication systems, allowing them to function in a seamless way. It will also extend system coverage by means of the future IRIS^{2} [12] multiorbital system. EU-funded projects will build the technical capabilities for EUCCS, relying primarily on European technology providers, to foster the EU's strategic autonomy in this sensitive sector.

Lawful access to data

Law enforcement and the judicial authorities need to be able to investigate and take action against crime. Today, nearly all forms of serious and organised crime have a digital footprint[13]. Around 85% of criminal investigations now rely on law enforcement authorities' ability to access digital information.[14]

The **High-Level Group on Access to Data for Effective Law Enforcement** highlighted in its concluding report[15] that law enforcement and the judiciary had been losing ground to criminals over the past decade as criminals avail themselves of tools and products provided from other jurisdictions, by providers that have put in place measures that deprive them of the means to cooperate with lawful requests in individual criminal cases. Systematic cooperation between law enforcement authorities and private parties, including service providers, is therefore essential in future efforts to disrupt the most threatening criminal networks and individuals in the Union and beyond.

As digitalisation becomes more pervasive and provides an ever-growing source of new tools for criminals, a framework for access to data which responds to the needs to enforce our laws and protect our values is essential. At the same time, ensuring digital systems remain secure from unauthorised access is equally vital to preserve cybersecurity and protect against emerging

[11] That is, the networks used by law enforcement, border guards, customs authorities, civil protection, firefighters, medical emergency responders and other key actors for public security and safety.
[12] EU Infrastructure for Resilience, Interconnectivity and Security by Satellite
[13] https://www.europol.europa.eu/cms/sites/default/files/documents/EU-SOCTA-2025.pdf
[14] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52019PC0070.
[15] Concluding report of the High-Level Group on access to data for effective law enforcement- 15/11/2024, 4802e306-c364-4154-835b-e986a9a49281_en.

security threats. Such access frameworks must also respect fundamental rights, ensuring inter alia that privacy and personal data are adequately protected.

Over the last years, the EU has taken action both to tackle **online crime and to facilitate access to digital evidence for all crimes**, with the adoption of electronic evidence rules that will apply fully from August 2026[16]. These will be complemented by international instruments for information and evidence exchange. The Commission will soon propose the signature and conclusion of the new **UN Convention against Cybercrime**.

To follow up on the recommendations of the High-Level Group[17], the Commission will present in the first half of 2025 a **roadmap setting out the legal and practical measures** it proposes to take **to ensure lawful and effective access to data**. In the follow-up to this Roadmap, the Commission will prioritise an assessment of the impact of **data retention rules** at EU level and the preparation of a **Technology Roadmap on encryption,** to identify and assess technological solutions that would enable law enforcement authorities to access encrypted data in a lawful manner, safeguarding cybersecurity and fundamental rights.

Operational cooperation

The Commission will work with Member States, EU agencies and bodies and partner countries to strengthen operational cooperation, which is essential for a more effective approach to fighting transnational organised crime and terrorism.

As the main EU framework for joint action against serious and organised crime, the **European Multidisciplinary Platform Against Criminal Threats (EMPACT)** has achieved substantial operational results. The next EMPACT cycle 2026-2029 presents an opportunity to strengthen this framework even further. To disrupt the most threatening criminal networks and individuals, the Union must streamline and focus its efforts on the most pressing priorities, enhancing the commitments of the Member States and ensuring an effective use of resources.

To that end, the Commission will work with the Council Presidencies and the Member States to **maximise EMPACT's potential and tackle the key priorities for the next EMPACT cycle 2026-2029.** Across these priority areas, there is a need for intelligence on the most threatening criminal networks, joint investigations and operational task forces and a strong judicial response, including a 'follow-the-money' approach. Moreover, the Union needs to tackle criminal recruitment and infiltration and strengthen multi-agency and international law enforcement cooperation and training.

The Commission will also support other forms of **cross-border operational law enforcement cooperation among Member States and Schengen Associated Countries**. The Schengen area, with no controls at the internal borders, requires close cooperation and exchange of information among Member State law enforcement authorities to ensure a high level of internal security. Today, law enforcement officers still face challenges when surveilling or performing urgent interventions across borders[18], and countering hybrid threats also requires enhanced cross-border cooperation. A **High-Level Group on the future of operational law enforcement cooperation** should be created to develop a shared strategic vision.

---

[16] Regulation (EU) 2023/1543 of the European Parliament and of the Council 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, OJ L 191, 28.7.2023.

[17] Council conclusions on access to data for effective law enforcement (12 December 2024) https://data.consilium.europa.eu/doc/document/ST-16448-2024-INIT/en/pdf.

[18] As reported in the Commission Assessment of the effect given by the Member States to Council Recommendation (EU) 2022/915 of 9 June 2022 on operational law enforcement cooperation (5909/25).

Efficient data exchange among law enforcement authorities is also essential for effective cross-border cooperation. Once established, the **interoperability architecture** will provide law enforcement authorities and Europol with effective access to crucial information. At the same time, the EU and its Member States should prioritise the bilateral and multilateral exchange of information, through the legal and technical implementation of the **Prüm II Regulation**[19], in cooperation with eu-LISA and Europol. This will enable secure automated exchanges of fingerprints, DNA profiles, vehicle registration data, facial images, and police records through EU routers. At national level, Member States need to implement the **Information Exchange Directive**[20] enhancing information exchange channels for seamless cross-border information flow, while ensuring their integration with Union-level systems, such as SIENA[21].

Effective cross-border cooperation also relies on fostering a **common EU law enforcement culture**. Joint training, centres of excellence and mobility programmes are essential in achieving this goal. The Commission will explore how the EU can best support training for Member State authorities, relying on **CEPOL** as the EU agency for law enforcement training.

Strengthening border security

Strengthening the resilience and security of external borders is crucial to counter hybrid threats, such as the weaponisation of migration, to prevent threat actors and goods from entering the EU, and to combat cross-border crime and terrorism effectively. **The Schengen Information System (SIS) is planned to be enhanced** in 2026 to enable Member States to enter alerts about third-country nationals involved in terrorism, including foreign terrorist fighters, and in other serious crimes, based on data shared by third countries with Europol.

Improved **interoperability** of the large-scale EU information systems will provide Member States with essential information on individuals from third countries crossing or intending to cross external borders, helping authorities to assess the conditions to authorise entry into territory of Member States[22]. The Commission will continue to work closely with Member States and eu-LISA for the swift implementation of these systems, notably the **Entry-Exit System (EES), the European Travel Authorisation System (ETIAS) and the revised Visa Information System (VIS)**, to ensure their smooth operation and security benefits.

To further enhance border security and strengthen EU cooperation in the face of evolving threats, **the Commission will propose to reinforce Frontex.** The European Border and Coast Guards should triple to 30 000 over time. The Agency should be equipped with advanced technology for surveillance and situational awareness, including intelligence relevant for European Integrated Border Management and access to robust EU Earth-Observation governmental services for border control to be deployed by 2027. This should further enhance the ability to detect, prevent, and combat cross-border crime at the external borders as well as

[19] Regulation (EU) 2024/982 of the European Parliament and of the Council of 13 March 2024 on the automated search and exchange of data for police cooperation and amending Council Decisions 2008/615/JHA and 2008/616/JHA and Regulations (EU) 2018/1726, (EU) No 2019/817 and (EU) 2019/818 of the European Parliament and of the Council (the Prüm II Regulation), OJ L, 2024/982, 5.4.2024.

[20] Directive (EU) 2023/977 of the European Parliament and of the Council of 10 May 2023 on the exchange of information between the law enforcement authorities of Member States and repealing Council Framework Decision 2006/960/JHA, OJ L 134, 22.5.2023, p. 1–24.

[21] Secure Information Exchange Network Application.

[22] Notably, the Entry/Exit System (EES) will enable Member States to identify third-country nationals at the external borders of the Schengen area and record their entries and exits, allowing for a systematic identification of overstayers. Prior to arrival of a third-country national at the external borders, the European Travel Information and Authorisation System (ETIAS) and Visa Information System (VIS) will allow Member States to pre-assess whether the presence of a third-country national in the EU territory would pose a security risk.

reinforcing its support to the Member States with the implementation of returns, in particular in relation to third-country nationals posing a security risk.

Document and identity fraud facilitates migrant smuggling, trafficking in human beings, clandestine criminal movements, and trafficking of illicit goods. The **multiple identity detector (MID)**[23], once operational, will improve national authorities' ability to identify individuals using multiple identities and counter identity fraud. The Commission will explore ways to enhance the security of travel and residence documents issued to EU citizens and third-country nationals. Additionally, the Commission will assess how EU Digital Identity Wallets, to be introduced under the European Digital Identity Framework by the end of 2026, can contribute to enhancing travel document security and improve identity verification. This will complement the proposals on digital travel credentials and the EU Digital Travel Application[24].

Travel information is crucial for authorities to identify and investigate movements of criminals, terrorists, and others posing security threats. While an EU framework exists for commercial air travel information[25], the processing of data from other transport modes for law enforcement purposes is fragmented. Consequently, criminals and terrorists can exploit different transport modes for illegal activities undetected. The Commission will work with Member States and the transport industry to **strengthen the travel information framework** by exploring a Union scheme requiring operators of private flights to collect and transfer passenger data, evaluating Passenger Name Records processing rules, and assessing ways to streamline maritime travel information processing. For road transport, the Commission will assess an expanded use of **Automatic Number Plate Recognition (ANPR)** systems and increase possibilities for synergies with the SIS.

Foresight, innovation and capability-driven approach

The Commission will develop **a comprehensive foresight approach on internal security at EU level**, relying on best practices identified at national level. This approach will support policymaking and guide investments in relevant EU-funded security research and innovation.

Research and innovation play a crucial role in internal security by creating solutions to counter emerging threats, including from technology misuse[26]. The EU must continue to invest, through EU-funded security research and innovation[27], in the development of innovative tools and solutions to address security threats while adhering to EU rules and fundamental rights. The Commission should support the transition from research to deployment, to ensure the effective uptake of those modern capabilities, with a priority on **modern technologies** like AI. This approach should include training to improve the use of AI systems and other technical capabilities by law enforcement and judicial authorities. Moreover, where relevant, the dual-use potential of technologies should be exploited in both directions (from civil to defence, and from defence to civil)[28].

The **EU Innovation Hub for Internal Security**[29], a network of innovation labs providing the latest innovation updates and effective solutions to support the work of internal security actors

[23] The MID is one of the interoperability components introduced by Regulation (EU) 2019/818 and Regulation 2019/817.
[24] https://ec.europa.eu/commission/presscorner/detail/en/ip_24_5047.
[25] Passenger Name Record (PNR) and Advance Passenger Information (API) framework established by Directive (EU) 2016/681 ('PNR Directive') and Regulation (EU) 2025/12, Regulation (EU) 2025/13 ('API Regulations').
[26] See the Commission Joint Research Centre report "Emerging risks and opportunities for EU internal security stemming from new technologies" https://publications.jrc.ec.europa.eu/repository/handle/JRC139674.
[27] Study on strengthening EU-funded security research and innovation – 20 years of EU-Funded Civil Security Research and Innovation – 2025, https://data.europa.eu/doi/10.2837/0004501.
[28] As laid down in the Niinistö report.
[29] EU Innovation Hub for Internal Security | Europol.

in the EU and the Member States, will help integrate research into practice and policy. Enhancing Europol's effectiveness requires strengthening the Europol Tool Repository (ETR), enabling it to identify, develop, jointly procure, and apply advanced technologies operationally. Additionally, the Commission will establish a **Security Research & Innovation Campus** at its Joint Research Centre, bringing together researchers to shorten the cycle from research results to innovation, development and successful implementation, while decreasing costs for development, testing and validation.

Our **European Research Area** is by its very nature collaborative, and therefore permeable to foreign interference and disinformation. Following the adoption of the Council recommendation on research security[30], the Commission and the Member States are taking measures to empower relevant actors, inter alia by setting up a Centre of Expertise on research security.

Key actions

The Commission will adopt:

- **a legislative proposal to transform Europol into a truly operational law enforcement agency in 2026**
- **a legislative proposal to strengthen Eurojust in 2026**
- **a legislative proposal to reinforce Frontex's role and tasks in 2026**
- **a legislative proposal to establish a European Critical Communications System in 2026**

The Commission will:

- **present a Roadmap setting out the way forward on lawful and effective access to data for law enforcement in 2025**
- **prepare an impact assessment in 2025 with a view to updating rules on data retention at EU level, as appropriate**
- **present a Technology Roadmap on encryption to identify and assess technological solutions to enable lawful access to data by law enforcement authorities in 2026**
- **work towards creating a High-Level Group to strengthen operational law enforcement cooperation**
- **create a Security Research & Innovation Campus at its Joint Research Centre in 2026**

The Commission, in cooperation with the Member States and relevant EU agencies, will:

- **strengthen the EMPACT architecture**
- **work towards the swift rollout of the interoperability architecture and implementation of the Prüm II Regulation**
- **strengthen the travel information framework**

Member States are urged to:

- **transpose and fully implement the Information Exchange Directive**

[30] OJ C/2024/3510, 30.5.2024.

4. Resilience against hybrid threats and other hostile acts

We will build resilience against hybrid threats by enhancing the protection of critical infrastructure, reinforcing cybersecurity, securing transport hubs and ports and combatting online threats.

The frequency and sophistication of hostile acts undermining the security of the EU have increased, with malicious actors expanding their arsenal significantly. Hybrid campaigns targeting the EU, its Member States and partners, have intensified, featuring acts of sabotage targeting critical infrastructure, arson, cyberattacks, election interference, foreign interference and manipulation of information (FIMI), including disinformation, and weaponisation of migration. Due to their political and operational role, and the nature of the information they handle, Union institutions, bodies, offices and agencies ("Union entities") are not spared.

The EU must **enhance its resilience**, utilise current tools effectively, and develop new ways to confront these evolving threats stemming from state and non-state actors, both now and in the future.

Critical infrastructure

Threats to **critical infrastructure**, including hybrid threats like sabotage and malicious cyber activity, are a major concern, notably for the infrastructure that connects Member States – be it energy interconnectors or cross-border communication cables, and transport. Since Russia's war of aggression against Ukraine, acts of sabotage targeting critical infrastructure have increased, particularly in 2024, affecting numerous Member States. Cooperation between law enforcement, security and cybersecurity services, military and civil protection, and private operators is essential to anticipate, detect, prevent and respond to such acts effectively.

Reducing vulnerabilities and strengthening the resilience of critical entities is imperative to ensure the uninterrupted provision of essential services vital for the economy and society. Timely transposition and the correct implementation by all Member States of the **Critical Entities Resilience (CER) Directive**[31] and the **Directive on measures for a high common level of cybersecurity across the Union (NIS2)**[32] are therefore crucial in that regard.

To ensure swift progress, the Commission will support Member States in identifying critical entities[33] and exchanging good practices on national strategies and on risk assessments as regards essential services, in cooperation with the **Critical Entities Resilience Group and NIS Cooperation Group**. Should critical infrastructure disruptions occur with significant cross-border impact, the **EU Critical Infrastructure Blueprint** will coordinate EU-level responses. The Commission encourages the Council to quickly adopt the **EU Cyber Blueprint,** which will further bolster coordination in the crisis management context, facilitating closer collaboration between authorities on physical and digital resilience. Following successful energy sector stress tests in 2023, the Commission will promote **voluntary stress tests** in other key sectors for internal security. Additionally, the Commission will provide a **Union-level overview of cross-border and cross-sectoral risks** to essential services to support Member

[31] 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.

[32] Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive).

[33] The sectors covered by the Directive are energy, transport, banking, financial market infrastructure, health, drinking water, wastewater, digital infrastructure, public administration, space, food production, processing and distribution.

States' risk assessments and inform a comprehensive EU-level risk assessment. In line with the Preparedness Union Strategy, the Commission will engage with Member States to identify further sectors and services not covered by the current legislation for which there might be a need to act.

The **EU-NATO Task Force on the resilience of critical infrastructure** has fostered excellent cooperation in sharing best practices and enhancing resilience in energy, transport, digital infrastructure, and space sectors. This work will continue within the **EU-NATO Structured Dialogue on Resilience**. The **EU Hybrid Toolbox** offers robust support to Member States and partners in preparing for and countering hybrid threats. **Hybrid Rapid Response Teams**[34] provide tailored short-term assistance upon request to Member States, various EU missions and partners. Furthermore, the Commission will take forward EU cooperation on combating sabotage through expert activities[35], including a **dedicated joint work programme** for the experts to streamline information exchange and map out countermeasures.

Incidents affecting **submarine cables** in Europe highlight the need for stronger measures and clearer responses. As outlined in the **EU Cable Security Action Plan**[36], the Commission, alongside the High Representative, will collaborate with Member States, EU agencies, and partners like NATO to prevent, detect, respond to, and deter threats to submarine cables. To develop an integrated situational picture of threats, the Commission will work with Member States to develop and deploy, on a voluntary basis, integrated surveillance mechanism for submarine cable per sea basin, starting with a Nordic/Baltic regional hub.

Cybersecurity

The persistent nature of **malicious cyber activity**, which often forms part of a wider range of multi-dimensional and hybrid threats, requires continued attention and action at European level. In recent years, the Union has adopted a range of cybersecurity laws which strengthen the cyber resilience of NIS2 entities operating in EU critical sectors as well as Union entities[37], improve the security of digital products (Cyber Resilience Act) and establish a framework for preparedness and incident response support (Cyber Solidarity Act). In January 2025, the Commission adopted the **European action plan on the cybersecurity of hospitals and healthcare providers**[38] to improve threat detection, preparedness, and crisis response. Its full implementation is key. At the same time, to address novel threats and developments, we need to step up our actions in particular in the areas of information exchange, supply chain security, ransomware and cyberattacks, as well as technological sovereignty.

Furthermore, implementation requires closing the current cybersecurity skills gap of 299 000 people. The Commission will work with the Member States under the Union of Skills[39] to expand the cybersecurity work force, in particular by using the new Cybersecurity Skills Academy. The STEM Education Strategic Plan[40] contributes to improving the talent pipeline and Europe's response to cybersecurity labour market needs.

---

[34] EU Strategic Compass for Security and Defence 2022, p.22

[35] The EU Protective Security Advisors, European Explosive Ordnance Disposal Network (EEODN), ATLAS Network, EU High Risk Security Network (EU HRSN), CBRN Security Advisory Group, Critical Entities Resilience Group (CERG).

[36] JOIN (2025) 9 final.

[37] Regulation (EU, Euratom) 2023/2841 of the European Parliament and of the Council of 13 December 2023 laying down measures for a high common level of cybersecurity at the institutions, bodies, offices and agencies of the Union, OJ L, 2023/2841, 18.12.2023.

[38] https://digital-strategy.ec.europa.eu/en/library/european-action-plan-cybersecurity-hospitals-and-healthcare-providers.

[39] COM (2025) 90 final.

[40] COM (2025) 89 final.

In parallel to enhancing its resilience, the EU will continue to make full use of the Framework for a Joint EU Diplomatic Response to Malicious Cyber Activities (**The Cyber Diplomacy Toolbox)** to prevent, deter and respond to cyber threats stemming from state and non-state actors.

Security of ICT supply chains

The **5G Cybersecurity Toolbox** provides the relevant framework to protect 5G networks, but currently is insufficiently implemented by Member States. Unacceptable security risks remain, specifically regarding the substitution of high-risk providers. A harmonised approach to the security of the ICT supply chain can address the current fragmentation of the internal market caused by different approaches at national level, avoid critical dependencies and de-risk our ICT supply chains from high-risk suppliers, in this way securing our critical infrastructure.

In line with this approach, in the upcoming **revision of the Cybersecurity Act**, the Commission will look more broadly at the security and resilience of ICT supply chains and infrastructure. In addition, the Commission will propose to improve the **European Cybersecurity Certification Framework**, to ensure that future certification schemes can be adopted in a timely manner and respond to policy needs.

Building on existing or ongoing sectoral assessments[41], the Commission will develop, together with the Member States, a **strategic planning for coordinated cybersecurity risk assessments.**

Cloud and telecom services have become a staple in the supply chains of critical infrastructures, businesses and public authorities. The Commission will take action to encourage critical entities to choose **cloud and telecom services which offer an appropriate level of cybersecurity**, taking into account not only technical risks but also strategic risks and dependencies.

Ransomware and cyberattacks

A persistent major challenge in the EU and globally is **ransomware**, with one report estimating a global annual cost of more than EUR 250 billion by 2031[42]. Both the **NIS2 Directive** and the **Cyber Resilience Act** will significantly improve the security posture of entities, making it more costly for ransomware networks to carry out their attacks. In addition, the Commission will work closely with Member States to ensure that more ransomware attacks, in particular advanced persistent threats, and ransom payments are reported to law enforcement, facilitating investigations.

To prevent and stop cyberattacks, the EU needs to strengthen the information exchange between law enforcement authorities, cybersecurity authorities and entities, as well as private parties, under the aegis of Europol and the EU Agency for Cybersecurity (ENISA).

Europol and Eurojust should continue to build on the achievements they have made in taking down ransomware operations, supporting law enforcement cooperation. To this end, law enforcement should maximise the use of cooperation mechanisms, including **Europol's International Ransomware Response Model** and the **International Counter Ransomware Initiative (CRI)**[43], and ENISA and Europol should cooperate to expand the repository of decryption tools for ransomware strains[44].

[41] Such as on 5G networks, telecommunications, electricity, renewable energy and connected vehicles.
[42] https://cybersecurityventures.com/global-ransomware-damage-costs-predicted-to-reach-250-billion-usd-by-2031/.
[43] https://counter-ransomware.org/.
[44] Available through the No More Ransom project, https://www.nomoreransom.org/en/index.html.

Technological sovereignty

Cybersecurity and technological sovereignty are closely interlinked, and technological dependencies need to be addressed as a matter of priority. The Union must **steer the development and deployment of new technologies**, with the Commission working to **enhance capabilities in strategic technologies** such as AI, quantum, advanced connectivity, cloud, edge, and Internet-of-Things[45], via forthcoming initiatives such as the AI Continent Action Plan, the Quantum Strategy, and others[46]. The Commission will continue supporting timely deployment of the latest available internationally agreed **Internet protocols** which are essential to maintain a scalable and efficient Internet with an enhanced level of cybersecurity. Further actions are also needed to address **radio spectrum related challenges** such as in relation to GNSS spoofing, jamming, supply chain risks and dependencies, such as the use of quantum sensing technologies and exploring the development of Radio Frequency monitoring capacity.

Deploying **post-quantum cryptography** (PQC) solutions will be crucial to safeguard sensitive communications, data at rest and to protecting digital identities in the new quantum era. On the basis of the 2024 Recommendation on a Coordinated Implementation Roadmap for the transition to PQC[47], the Commission is working with Member States to foster that transition. In this regard, Member States should identify high-risk cases in critical entities and ensure quantum-safe encryption for these high-risk cases as soon as possible and no later than by the end of 2030. The Commission is also working with the Member States and the European Space Agency (ESA) to develop and deploy the **European quantum communication infrastructure (EuroQCI)**[48], based on Quantum Key Distribution (QKD), as part of **IRIS²**, the EU Secure Connectivity Programme. Both initiatives will ultimately enable entities to transmit data and store information securely.

Quantum technologies will also play a key role in security applications: a **roadmap for quantum sensing in security applications** will be developed as part of the **Quantum Strategy**. In the same vein, the Commission is working to quantum-proof its corporate security-critical systems, including its classified IT systems.

A business-friendly cybersecurity framework

The upcoming revision of the Cybersecurity Act is an opportunity to **simplify EU cybersecurity legislation,** in line with the Competitiveness Compass. The Commission will work closely with Member States to ensure a swift, coherent and business-friendly implementation of the horizontal cybersecurity framework set out in the NIS2 Directive, Cyber Resilience Act and the Cyber Solidarity Act, promoting simplicity and coherence and avoiding fragmentation or duplication of cybersecurity rules in EU and national laws.

To enable secure access to online services and strengthen digital security across the EU, the **European Digital Identity Framework** will offer all EU citizens and residents trustworthy Digital Identity Wallets before the end of 2026. The upcoming **European Business Wallet** will facilitate secure cross-border interactions between businesses and public administrations. Both are prerequisites for the secure and more efficient functioning of the data-driven Single Market

[45] https://strategic-technologies.europa.eu/about_en#step-scope.

[46] e.g. EuropHPC JU https://eurohpc-ju.europa.eu/index_en, the Quantum Flagship Homepage of Quantum Flagship | Quantum Flagship, the 3C networks (COM(2024) 81 final) and the EU Cable Action Security Plan (JOIN(2025) 9 final).

[47] Recommendation on a Coordinated Implementation Roadmap for the transition to Post-Quantum Cryptography | Shaping Europe's digital future.

[48] https://digital-strategy.ec.europa.eu/en/policies/european-quantum-communication-infrastructure-euroqci.

with tools such as the Single Digital Gateway, e-Invoicing, e-Procurement and the Digital Product Passport.

Online security

Some of the most serious hybrid threats jeopardising the security and safety of people in Europe and targeting the EU's democratic sphere take place online. These threats include illegal activities and illegal content online, information manipulation involving artificial amplification, misleading information and FIMI.

The rigorous enforcement of the **Digital Services Act (DSA)** is paramount to ensure a safe and accessible online environment with accountable actors that is resilient also to hybrid threats. The DSA obliges providers of very large online platforms (VLOPs) and of very large online search engines (VLOSEs) to conduct risk assessments and put in place mitigation measures for systemic risks stemming from the design, functioning or use of their services. Such risks may include negative effects on civic discourse and electoral processes, as well as on public security, such as far-reaching interference of malicious foreign state actors, for example in electoral processes. Training of Member States' competent authorities on the use of legal tools to promptly remove illegal content online is important, particularly with regard to gender-based cyber violence. The DSA provides for a crisis response mechanism, which can be activated where extraordinary circumstances lead to a serious threat to public security or public health in the Union or in significant parts of it. To complement this mechanism, the Commission and the national competent authorities designated as Digital Services Coordinators have also developed a voluntary **DSA Incident Response Framework**. Digital Services Coordinators have also undertaken action to help protect the integrity of elections, by for example organising election roundtables and stress tests[49]. The DSA, together with the Regulation on political advertising[50], provides one of several strands linked to safeguarding democracy and the integrity of democratic processes, which are vulnerable to being targeted by hostile actors, including by means of digital tools and on social media.

The implementation of the **FIMI** toolbox is another important component offering key support at EU level. Supporting digital and media literacy and critical thinking are also central to these efforts[51].

Countering weaponisation of migration

Russia, with the aid and decisive support of Belarus, has purposefully weaponised migration, and illegally facilitated migration flows towards the EU's external borders with the aim to destabilise our societies and undermine the unity of the European Union. This jeopardises not only the national security and sovereignty of Member States, but also the safety and integrity of the Schengen area and the security of the Union as a whole. In its conclusions of October 2024, the European Council emphasised that Russia and Belarus, or any other country, cannot be allowed to abuse our values, including the right to asylum, and to undermine our democracy.

As stated in the 2024 Commission Communication on weaponisation of migration, in addition to strong political support, the Union has undertaken financial, operational and diplomatic measures, including cooperation with countries of origin and transit, to effectively address these

[49] DSA Elections Toolkit for Digital Services Coordinators 2025 https://digital-strategy.ec.europa.eu/en/library/dsa-elections-toolkit-digital-services-coordinators.
[50] Regulation (EU) 2024/900 of the European Parliament and of the Council of 13 March 2024 on the transparency and targeting of political advertising, OJ L, 2024/900, 20.3.2024.
[51] Digital Education Action Plan (2021-2027) - European Education Area.

threats[52]. This response involves using the new framework established by the Council to sanction individuals and organisations involved in actions and policies like Russia's weaponisation of migration, by imposing asset freezes and travel bans[53]. The EU will continue to use this framework, when necessary, and support Member States in countering this threat.

Transport security

Maritime ports, airports and land infrastructure are crucial entry and exit points. They play a vital role in the EU's economy and society and are essential for military mobility. However, these transport hubs and means are also prime targets for external threats and criminal activity. Recent incidents, including aviation cargo security breaches and attacks on rail infrastructure, highlight the serious risks. **Transport operators** can be both targets and instruments for malicious actors. Existing EU legal instruments have enhanced aviation security[54], yet the high threat level to civil aviation calls for a means of foreseeing incidents and rapidly consulting relevant Member States. The Commission will collaborate with Member States to amend existing implementing legislation in the field of Aviation Security for sharing classified information on **aviation security occurrences**. Additionally, the Commission will consider **regulatory measures** to address new threats such as **air cargo incidents** and to reinforce aviation security standards. This will also involve strengthening the **aviation security legislation (AVSEC)** to enable immediate response measures while maintaining the one-stop security area in EU airports.

In developing the upcoming **EU Ports Strategy**, building on the **EU Ports Alliance**, the Commission will explore ways to further strengthen maritime security legislation to effectively address emerging threats, secure ports, and enhance EU supply chain security. To this end, the Commission will ensure its robust implementation, and work on harmonising national practices and reinforcing background checks at ports. Further to security protocols established for air cargo, the Commission will work with Member States and the private sector on expanding these protocols to secure the maritime transport chains.

The proposed EU Customs Authority will analyse and assess risks based on **customs information** related to goods entering, exiting and transiting the EU to support Member States in preventing the exploitation of international supply chains by malicious actors. In line with the EU Maritime Security Strategy[55], the upcoming **European Ocean Pact** will play a key role in stepping up maritime security in the sea basins around the EU and beyond, including through encouraging the scaling up of multi-purpose maritime operations and exercises.

Resilience of supply chains

Europe must reduce its reliance on third-country technologies, which can lead to dependency and security risks. The Commission aims to mitigate dependencies on single foreign suppliers, de-risk our supply chains from high-risk suppliers, and secure critical infrastructure and industrial capacity on EU soil, as specified in the **Competitiveness Compass**[56]and the **Clean Industrial Deal**[57]. The Commission will promote an **industrial policy for internal security** by collaborating with EU industries in key sectors (e.g. transport hubs, critical infrastructures)

[52] COM (2024) 570 final.
[53] Council Regulation (EU) 2024/2642 of 8 October 2024 concerning restrictive measures in view of Russia's destabilising activities, ST/8744/2024/INIT, OJ L, 2024/2642, 9.10.2024.
[54] Regulation (EC) No 300/2008 of the European Parliament and of the Council of 11 March 2008 on common rules in the field of civil aviation security, OJ L 97, 9.4.2008, p. 72–84.
[55] JOIN (2023) 8 final.
[56] COM (2025) 30 final.
[57] COM (2025) 85 final.

to produce security solutions like detection equipment, biometric technologies, and drones, incorporating security by design features. In **revisiting EU procurement rules**, the Commission will assess whether the security considerations in the 2009 Defence and Security Procurement Directive[58] are sufficient to address law enforcement and critical entity resilience needs.

The Commission will support Member States in **screening Foreign Direct Investment (FDI)** and equipment procurement for logistics hubs, ensuring critical infrastructure and technology remain secure.

Once entered into application, the **Internal Market Emergency and Resilience Act (IMERA)** will help the EU manage crises that disrupt critical supply chains and the free movement of goods, services, and people. It will enable swift crisis coordination, identification of crisis-relevant goods and services, and provide a toolbox to ensure their availability. Furthermore, in close cooperation with Member States, the Commission will propose to establish **a multi-agency transport and supply chain security alert mechanism** to guarantee secure and timely sharing of relevant information necessary to anticipate and counter threats.

Moreover, with the implementation of the Critical Raw Materials Act and of the Net-Zero Industry Act, increased use of sustainability, resilience and European preference criteria in EU public procurement will foster the development of lead markets. Strengthened trade ties, for instance through Raw Materials Partnerships and Clean Trade and Investment Partnerships, will help diversify supply chains.

Resilience and preparedness for chemical, biological, radiological and nuclear threats

The Russian war of aggression against Ukraine has heightened the risk of **chemical, biological, radiological and nuclear (CBRN) threats**. To address the potential acquisition and weaponisation of CBRN materials, the Commission will support Member States and partner countries through dedicated training and exercises. The Commission will also boost CBRN preparedness and response capabilities, with threat prioritisation, innovation funding for countermeasures, rescEU capacities and stockpiling of medical countermeasures, under the umbrella of a new **CBRN Preparedness and Response Action Plan**. In addition, the **EU Strategy on Medical Countermeasures** will support the development of medical countermeasures from research to manufacturing and distribution to protect the EU from pandemics and CBRN threats.

Building on the COVID-19 pandemic experience, the EU has strengthened the health security framework[59]. The Commission is designating EU Reference Laboratories in public health to strengthen EU and national surveillance and rapid detection capacities. A Union Plan on preparedness, prevention and response in health security will be published in 2025.

Key actions

The Commission will:

- **review and revise the Cybersecurity Act in 2025**
- **develop measures to ensure cybersecure use of Cloud services**
- **propose an EU Ports Strategy in 2025**
- **revise EU procurement rules for defence and security in 2026**

[58] Directive 2009/81/EC on the coordination of procedures for the award of certain works contracts, supply contracts and service contracts by contracting authorities or entities in the fields of defence and security, OJ L 216, 20.8.2009

[59] Most notably through Regulation (EU) 2022/2371 on serious cross-border health threats.

- **present a new CBRN Preparedness and Response Action Plan in 2026**

The Commission, in cooperation with Member States, will:

- **develop and deploy the European quantum communication infrastructure (EuroQCI)**
- **ensure effective enforcement of the Digital Services Act**
- **work to counter the weaponisation of migration**
- **establish an aviation security occurrence system**
- **work to establish a multi-agency transport and supply chain security alert mechanism**

The Council is urged to:

- **adopt the Council recommendation on the EU Cyber Blueprint**

Member States are urged to:

- **transpose and fully implement the CER and NIS2 Directives**

5. Tightening the net on serious and organised crime

We will help to root out organised crime by proposing stronger rules to tackle organised crime networks, including on investigations, make youth in the EU less vulnerable to recruitment into crime, and step up measures to cut off access to criminal tools and assets.

Organised crime is exploiting an evolving landscape and proliferating exponentially. It benefits from advanced technologies, is active across multiple jurisdictions, and has strong connections beyond EU borders. Given these complex, transnational threats, EU-level coordination and support is vital.

Crime prevention

The recruitment of young people into organised crime is a growing concern in the EU. Combating organised crime requires addressing its **root causes** by offering education and alternatives to a life of crime through a whole-of-society approach. The Commission will support the integration of security considerations into EU education, social, employment, and regional policies. The EU will **promote evidence-based crime prevention policies**[60] tailored to local contexts.

To protect recipients of online services, particularly minors, from inter alia child sexual abusers, human traffickers, and online recruitment for crime or violent extremism, measures under the **Digital Services Act** require providers of online platforms accessible to minors to manage risks and act upon illegal content, including hate speech. The Commission is planning to issue **guidelines on the protection of minors**, to assist providers of online platforms in ensuring a high level of privacy, safety and security of minors online. The guidelines will contain a set of recommendations for all digital services operating in the Union to enhance the protection of minors online. In 2025, the Commission is also planning to facilitate an EU **privacy-protective age verification** solution, which will fill in the gap before the EUDI Wallet is offered at the end of 2026. The Commission will also present an action plan against cyberbullying.

Furthermore, the Commission will continue to support voluntary multistakeholder engagement with online platforms and other relevant actors, including through the EU Internet Forum and targeted codes of conduct under the Digital Services Act, such as the 2025 Code of conduct on

[60] https://www.eucpn.org/.

illegal hate speech online. The objective is to raise awareness, jointly respond to current and emerging threats, and to produce and share good practice for mitigation measures.

Locally, the impact of organised crime underscores the need for regional solutions to reduce vulnerability and the appeal of illegal activities. The EU Agenda for Cities will address security challenges in cities, building on the EU Cities against Radicalisation initiative. The Commission will support Member States in enhancing urban and regional security through the European Regional Development Fund**.**

Stronger educational foundations and skills underpin resilient and cohesive societies. Through the **Union of Skills** and **Action Plan on Integration and Inclusion**, the Union will work to help people become more resilient to mis- and disinformation, radicalisation and recruitment into crime.

Protecting children from all forms of violence, including crime, physical or mental violence, online as offline, is a core EU objective. To address the specific needs of particularly vulnerable groups such as children, who are increasingly exposed to recruitment and radicalisation, grooming and child sexual abuse, cyberbullying, disinformation, and other threats, the EU will develop an **Action Plan on the Protection of Children against Crime**, encompassing the online and offline dimensions. It will set out a coherent and coordinated approach based on the available frameworks and tools, including the future EU Centre to prevent and combat child sexual abuse, and other EU bodies and agencies, and propose ways forward where gaps remain.

Dismantling the criminal networks and their enablers

The fight against high-risk criminal networks, ringleaders, and enablers must intensify. Although recent successes are notable,[61] outdated rules and inconsistent definitions of criminal networks hinder effective criminal justice response and cross-border cooperation. The Commission will review outdated legislation in this area, proposing a renewed **legal framework on organised crime** to strengthen the response.

Administrative enforcement can complement law enforcement for faster results – as shown by the EPPO and the European Anti-Fraud Office (OLAF) in addressing **cross-border fraud and crimes against the financial interests of the EU**. Subsidy fraudsters focus on sectors such as renewable energy, research programmes, and the agricultural sector[62]. The Commission will explore ways to coordinate the use of criminal and administrative tools, enhancing cooperation with Europol, Eurojust and the EPPO. The Commission will also continue to support the wider application of **the administrative approach** to empower local and other administrative authorities to disrupt criminal infiltration[63].

The EU is working on strengthening its legal framework for combating **corruption**[64]. The European Parliament and Council should swiftly conclude negotiations on the updated anti-corruption framework proposed by the Commission. The Commission will present an EU Anti-Corruption Strategy to foster integrity and to strengthen coordination among all relevant authorities and stakeholders in this area.

[61] Including recent EMPACT cases.

[62] https://www.europol.europa.eu/cms/sites/default/files/documents/EU-SOCTA-2025.pdf.

[63] https://administrativeapproach.eu/sites/default/files/page/files/eu-jha-council-9-10-june-conclusions-administrative-approach-org-crime.pdf.

[64] Proposal for a Directive of the European Parliament and of the Council on combating corruption, replacing Council Framework Decision 2003/568/JHA and the Convention on the fight against corruption involving officials of the European Communities or officials of Member States of the European Union and amending Directive (EU) 2017/1371 of the European Parliament and of the Council, COM(2023) 234 final, Brussels, 3.5.2023.

Firearms are a key enabler of the increasing violence perpetrated by organised crime groups. The Commission will propose common criminal law standards on illicit firearms trafficking. A new **EU Action Plan against firearms trafficking** will focus on safeguarding the licit market, curtailing criminal activities, based on better intelligence and strengthening of international cooperation with particular focus on Ukraine and Western Balkans.

Illegally traded pyrotechnics, used in crimes, require measures to improve prevention and traceability. The Commission is currently evaluating the Pyrotechnics Directive and will also consider **criminal sanctions on pyrotechnics trafficking**.

Following the money

Following the money is crucial in combating organised crime and terrorism, yet it remains very challenging. The link between organised crime and money flows calls for intense and combined efforts to stop access of criminal networks to sources of funding and better protect people, businesses, and public budgets.

The EU has bolstered its efforts with the new anti-money laundering rules, including the establishment of the **EU Anti-Money Laundering Authority (AMLA)**[65]. Collaboration among AMLA, OLAF, the EPPO, Eurojust, and Europol is essential to implement effective financial investigations. The Commission will support the setting up of **partnerships**, both those facilitating inter-agency cooperation, and those involving the private sector.

To dismantle the financial motives behind organised crime, seizing assets and confiscating criminal gains is essential. The recently adopted stronger rules on **asset recovery and confiscation**[66] should be transposed by Member States without delay and used to their full potential. Combating parallel financial systems circumventing the EU anti-money laundering framework, including crypto-based systems, also requires innovative actions, shared best practices among Member States and increased support by Europol and Eurojust. The Commission will explore the feasibility of a new EU-wide system to track organised crime profits and terrorist financing, and also encourage timely and expanded information flows from **Financial Intelligence Units** to law enforcement. The Commission will explore ways to close loopholes, support Member States in capacity building, and will further work on strengthening cooperation with third countries misused by criminals for underground banking operations.

Fighting serious crimes

In addition to dismantling criminal networks, tackling serious crimes requires targeted efforts. To strengthen our ability to combat **online fraud** – which is causing very significant financial harm[67] – the Commission will support prevention measures and more effective law enforcement action and will work with Member States and stakeholders to support and protect victims, including by assisting in recovering their funds. These efforts will be formalised in an **Action Plan on Online Fraud.**

Building on the 2020-2025 EU Strategy for combating **child sexual abuse**[68], the Commission will support the co-legislators in finalising the two legislative proposals[69] to prevent and combat child sexual abuse online and to make law enforcement action against child sexual abuse and exploitation more effective. With interim rules in place until April 2026, it is essential to establish a permanent legal framework, and the Commission encourages the co-legislators to

[65] https://www.amla.europa.eu/index_en.
[66] Directive (EU) 2024/1260 of the European Parliament and of the Council of 24 April 2024 on asset recovery and confiscation, OJ L, 2024/1260, 2.5.2024.
[67] Global Anti-Scam Report 2024.
[68] COM (2020) 607 final
[69] COM (2022) 209 final and COM (2024) 60 final.

enter into negotiations on the draft Regulation laying down rules to prevent and combat child sexual abuse. The co-legislators are also invited to advance towards negotiations on the Directive on combating the sexual abuse and sexual exploitation of children and child sexual abuse material, which will establish minimum rules on the definition of criminal offences and sanctions in the area of sexual exploitation of children.

Half of the EU's most dangerous criminal networks are involved in violent **drug trafficking**. Although the EU has recently bolstered its fight against this crime[70], notably by expanding the mandate of the **EU Drugs Agency**, further actions are necessary. The Commission will work in close cooperation with the Member States to propose a new **EU Drugs Strategy**. It will also revise the **legal framework on drug precursors** and propose an **EU Action Plan against drug trafficking** to disrupt routes and business models**.** The **EU Ports Alliance's public private partnership** on strengthened port protection will be extended to include smaller and inland ports and ensure maritime security rules are enforced. Recognising the severe local impacts of drug trafficking, the Commission will continue to support a balanced, evidence-based, and multidisciplinary drug policy, with readiness for sudden drug influxes, especially synthetic opioids.

To combat the exploitation of people, the EU has adopted new rules[71] and will introduce a **renewed EU Strategy on combatting trafficking in human beings** (2026-2030), covering all stages from prevention to prosecution, with a focus on victim support at both EU and international levels.

In the fight against **migrant smuggling**, the Commission will lead efforts with key partners through the new Global Alliance to Counter Migrant Smuggling, in cooperation with Europol, Eurojust, and Frontex, including in the online dimension. The Commission's proposals on counter-smuggling[72] should be adopted and implemented without delay. Furthermore, the Commission, following the adoption of the **Toolbox on transport operators**[73], has increased outreach to foreign authorities and operators, and will continue to engage with the aviation industry and civil aviation organisations[74] to raise awareness about migrant smuggling by air[75].

Environmental crime threatens the environment, public health, and economies in the long term. The Commission will support Member States in implementing the Environmental Crime Directive[76] and bolster operational networks and actions in this field[77]. Robust enforcement is essential. In addition, the recently adopted Council of Europe Convention on the protection of the environment through criminal law[78] will help to ensure strong and comparable efforts to tackle environmental crime, both in Europe and beyond.

[70] COM (2023) 641 final.
[71] Directive (EU) 2024/1712 of 13 June 2024 amending Directive 2011/36/EU on preventing and combating trafficking in human beings and protecting its victims, OJ L, 2024/1712, 24.6.2024.
[72] COM (2023) 755 final and COM (2023) 754 final.
[73] Toolbox addressing the use of commercial means of transport to facilitate irregular migration to the EU.
[74] Including the International Civil Aviation Organisation (ICAO).
[75] The Commission will also support finalising the Regulation on measures against transport operators that facilitate or engage in trafficking in persons or smuggling of migrants, COM(2021) 753 final.
[76] Directive (EU) 2024/1203 of the European Parliament and of the Council of 11 April 2024 on the protection of the environment through criminal law, OJ L, 2024/1203, 30.4.2024.
[77] EU Network for the Implementation and Enforcement of Environmental Law (IMPEL), European Network of Prosecutors for the Environment (ENPE), EnviCrimeNet and EU Forum of Judges for the Environment (EUFJE).
[78] Committee of experts on the protection of the environment through Criminal Law (PC-ENV) - European Committee on Crime Problems.

The criminal justice response

Crime and terrorism can impact everyone, making it essential to support and safeguard rights of **victims** to reduce harm and increase overall security and trust in authorities. Building on the Victims' Rights Directive, the Commission will introduce a new **EU Strategy on Victims' Rights**.

EU criminal justice systems need effective tools to address emerging threats. To achieve this, the Commission has launched a **High-Level Forum on the Future of EU Criminal Justice**. This forum brings together Member States, the European Parliament, EU agencies and bodies, and other relevant stakeholders. Its goal is to discuss ways to ensure our criminal justice systems remain effective, fair and resilient amid evolving challenges, while strengthening judicial cooperation and enhancing mutual trust, including through digitalisation[79].

Key actions

The Commission will:

- **present a legislative proposal for modernised rules on organised crime in 2026**
- **present a legislative proposal to revise the legal framework on drug precursors in 2025**
- **present a legislative proposal for common criminal law standards on illicit firearms trafficking in 2025**
- **assess the need to revise the Directives on Pyrotechnics and Civil Explosives**
- **assess the need to further strengthen the European Investigation Order and the European Arrest Warrant**
- **present a new EU Strategy on combatting trafficking in human beings in 2026**
- **present a new EU Strategy on Victims' Rights in 2026**
- **present an EU Action Plan on the Protection of Children against Crime by 2027**
- **present an EU Action Plan against drug trafficking in 2025**
- **present an EU Action Plan against firearms trafficking in 2026**
- **successively expand the EU Ports Alliance from 2025 onwards**
- **adopt DSA guidelines on the protection of minors in 2026**
- **present an EU Action Plan against cyberbullying in 2026**

Member States are urged to:

- **fully transpose the new rules on asset recovery and confiscation by end of 2026 and use them to their full potential**
- **implement the administrative approach in the fight against criminal infiltration**
- **set up public-private partnerships against money laundering**
- **transpose and fully implement the Directive to prevent and combat violence against women and domestic violence**

The European Parliament and the Council are urged to:

- **advance towards negotiations on the Regulation laying down rules to prevent and combat child sexual abuse and the Directive on combating the sexual abuse and sexual exploitation of children and child sexual abuse material**
- **conclude negotiations on the Directive on combating corruption**

[79] Notably through the establishment of the e-Justice Communication via Online Data Exchange (eCODEX) and European Criminal Records Information System - Third Country Nationals (ECRIS-TCN).

6. Combating terrorism and violent extremism

We will introduce a comprehensive counter-terrorism agenda to prevent radicalisation, secure online and public spaces, throttle financing channels and respond to attacks when they occur.

The terrorist threat level in the EU remains high. It is closely linked to the spillover effects of geopolitical events, new technologies, and new means of terrorist financing. We need to ensure that the EU is well equipped to anticipate threats, to prevent radicalisation (both offline and online), to protect citizens and public spaces from attacks, and to effectively respond to attacks when they occur. A **new EU Agenda on preventing and countering terrorism and violent extremism** will be presented in 2025 to set out the EU's future action. In line with the new Agenda, the EU and the Western Balkans will sign the new **Joint Action Plan** on preventing and countering terrorism and violent extremism in 2025.

Prevention of radicalisation and protection of people online

Similarly to the fight against organised crime, countering terrorism and violent extremism starts with **tackling its root causes**. The **EU Knowledge Hub on Prevention of Radicalisation** will step up its support to practitioners and policymakers with a new **comprehensive prevention toolbox** to allow for early identification and interventions focused on vulnerable individuals, in particular minors**.** Radicalisation often happens in prisons and to support Member States in addressing this issue, the Commission will issue new recommendations.

Terrorist and violent extremists use online platforms to spread terrorist and harmful content, gather funds and recruit. Vulnerable users, particularly minors, are being radicalised online at an alarming rate. The **Terrorist Content Online Regulation** has been instrumental in countering the spread of terrorist content online, enabling the swift removal of the most heinous and dangerous material[80]. The Commission is currently evaluating its functioning and will assess how best to strengthen this framework.

The **EU Crisis Protocol** for a joint and rapid law enforcement and tech industry response in relation to a terrorist attack will be amended to ensure scalability and flexibility to respond to the growing online dimension of terrorist attacks. The EU Internet Forum will continue to be the main avenue for voluntary cooperation with the tech industry to tackle terrorist and harmful content online. Furthermore, the Commission is engaging in international initiatives such as the Christchurch Call Foundation and the Global Internet Forum to Counter Terrorism (GIFCT).

Counter terrorism financing

Terrorists finance their activities with crowdfunding campaigns, crypto assets, neobanks or online payment platforms. Law enforcement need to detect and investigate these financial flows. This requires means, tools and expertise. The **Counter-terrorism Financial Investigators' Network** plays a key role. The Commission will explore the creation of a **new EU-wide system to track terrorist financing** covering intra-EU and SEPA transactions, crypto asset transfers, online and wire payments, complementing the EU-US Terrorist Financing Tracking Programme (TFTP) Agreement.

The EU budget must be **protected from misuse to foster radical/extremist views** in the Member States. The revised **Financial Regulation** now includes conviction for "incitement to discrimination, hatred or violence" as a ground for exclusion from EU funding. The Commission will continue to explore the best way of making full use of the toolbox, including

[80] By 31 December 2024, 1426 removal orders have been issued to take terrorist content down or block access thereto, the large majority of which targeting Jihadist terrorist content but also right-wing terrorist content.

when selecting potential beneficiaries. The protection of the EU budget also relies on strong cooperation and information sharing with national authorities, EU agencies and bodies.

Protection from attacks

Beyond investment in preventing radicalisation, an important component of protecting citizens is restricting the means for terrorists and criminals to commit attacks. Action is needed both on the tools terrorists use and to protect the targets at risk of attack.

In addition to actions on firearms, the Commission will also **review the rules** on **explosives precursors** to include high-risk chemicals. **Public spaces** remain the most common targets for terrorist attacks, particularly for lone actors. To protect citizens from harm, the **EU Protective Security Advisory programme** will be strengthened to conduct vulnerability assessments of public spaces, critical infrastructure and high-risk events, upon request by Member States and financed by the EU budget under the Internal Security Fund. The EU will seek to expand available funding for public space protection. The Commission offers support to Member States authorities and private operators through dedicated guidance and tools, such as the Knowledge Hub on the protection of public spaces[81], and EUR 70 million have already made available to support public space protection since 2020.

The Commission will also explore introducing requirements for organisations to consider or employ security measures in publicly accessible venues, through engaging with local authorities and private partners

Given manifest vulnerabilities, the **EU Strategy on combating antisemitism and fostering Jewish life (2021-2030)** will continue guiding Commission's actions on protecting the Jewish community. The Commission will equally ensure that appropriate tools are in place to support Member States in combatting **anti-Muslim hatred.**

The use of **drones** for espionage and attacks poses an increasing security challenge. The Commission will develop a **harmonised testing methodology for counter-drone systems**, set up a **counter-drone Centre of Excellence** and assess the need to harmonise Member States' laws and procedures[82].

Foreign terrorist fighters

To identify foreign terrorist fighters returning or entering at the EU's external borders, data on individuals posing a terrorist threat is needed. To this end, the Commission, together with Europol, will strengthen its **cooperation with key third countries to obtain biographic and biometric data on individuals that might pose a terrorist threat**, including foreign terrorist fighters, which can then be inserted into the Schengen Information System in full compliance with applicable EU and national legal frameworks. It is therefore crucial that Member States make use of all the existing tools. This includes inserting all relevant information into the **SIS**, enhancing biometric checks and conducting mandatory systematic checks on all persons at EU external borders[83]. Moreover, the **Common Risk Indicators (CRIs)** developed by Frontex will continue supporting Member States' border control authorities to identify and assess the risk of suspicious travel by potential foreign terrorist fighters.

Furthermore, to ensure that Member States maintain access to the **battlefield evidence** collected by the UN Investigative Team to Promote Accountability for Crimes Committed by Da'esh/ISIL (UNITAD) for the prosecution of foreign terrorist fighters, the Commission, together with Eurojust, will assess the possibility to store this evidence in Eurojust's Core

[81] Knowledge Hub on the Protection of Public Spaces.
[82] Following from the set of key actions in the 2023 Counter-drone Communication, COM(2023) 659 final.
[83] In full compliance with the Schengen Borders Code and Screening Regulation.

International Crimes Evidence Database. Moreover, the new European **Judicial Counterterrorism Register** will continue supporting Member States' judiciaries in quickly identifying cross-border links in terrorism cases.

Key actions

The Commission will:

- **adopt a new EU Agenda on preventing and countering terrorism and violent extremism in 2025**
- **sign a new Joint Action Plan on preventing and countering terrorism and violent extremism with the Western Balkans in 2025**
- **develop a new comprehensive prevention toolbox with the EU Knowledge Hub**
- **evaluate the application of the Terrorist Content Online Regulation in 2026**
- **amend the EU Crisis Protocol in 2025**
- **present a legislative proposal to revise the Regulation on the marketing and use of explosives precursors in 2026**
- **explore the feasibility of a new EU-wide system to track terrorist financing**

Member States are urged to:

- **enhance biometric checks and conduct mandatory systematic checks at EU external borders**
- **make full use of the European Judicial Counter-terrorism Register**

7. The EU as a strong global player on security

To enhance the EU's security, we will boost operational cooperation through partnerships with key regions such as our enlargement and neighbourhood partners, Latin America and the Mediterranean region. The EU's security interests will be taken into account in international cooperation, including by leveraging EU tools and instruments.

Recent years have shown the intrinsic links between the EU's external and internal security. The Russian war of aggression against Ukraine, the conflict in Gaza, the situation in Syria and emerging conflicts around the globe have had serious spillover effects on the EU's internal security. To counteract the impact of global instability on its internal security, the **EU needs to actively defend its security interests** by addressing external threats, disrupting trafficking routes, and safeguarding corridors of strategic interest such as trade routes. Simultaneously, the EU will continue to be a strong ally to partner countries, working together to enhance global security and build mutual resilience against threats.

In recent years, the EU has taken significant steps to enhance its security cooperation. It has established operational law enforcement and judicial cooperation agreements, as well as other types of arrangements with partner countries. It is actively pursuing additional international agreements, in line with Council negotiating directives, and capacity-building initiatives, facilitated by EU agencies and bodies. Global Europe-NDICI is also crucial in strengthening security with partner countries.

The **rules-based multilateral order** is a cornerstone to strengthen global security. Security dialogues, including thematic ones, are vital for strengthening these efforts. The implementation of the **Strategic Compass for Security and Defence**, along with bilateral and multilateral cooperation frameworks such as Stabilisation and Association Agreements and Association Agreements, and collaborations with organisations like the UN and NATO, are crucial for

developing effective security solutions. The EU will continue to play its part in multilateral fora[84] and will enhance its cooperation with relevant international and regional organisations and frameworks, including NATO, the United Nations, the Council of Europe, Interpol, G7, the OSCE and civil society.

Regional cooperation

As a priority, continuing the EU's unwavering support to **Ukraine**, and strengthening the security and resilience of **EU enlargement countries**, is a political and geostrategic imperative. Supporting the security of the EU should go hand in hand with the **accelerated integration of candidate countries** in the **EU's security architecture**, in parallel to the consolidation of their regional cooperation. The Commission will use the EU's enlargement policy to support EU candidate countries' and potential candidates' capacities to respond to threats, to increase operational cooperation and information exchange, and to ensure alignment with EU principles, legislation, and tools. The Instrument for Pre-accession Assistance (IPA III), as well as the Ukraine, Moldova and Western Balkans Facilities are crucial in strengthening security in both candidate countries and potential candidates.

The EU will also further integrate the **neighbourhood partners** into the EU security architecture. Through the **New Pact for the Mediterranean** and the upcoming **Strategic Approach to the Black Sea**, the Union will aim to continue building regional cooperation and bilateral Strategic Comprehensive Partnerships with a security dimension, when relevant, with regular high level security dialogues. Operational cooperation with North Africa, the **Middle East and the Gulf** will be strengthened, in particular on counterterrorism, anti-money laundering, firearms trafficking and drug production and trafficking, notably captagon**.**

To address the rise of terrorist and criminal activity and its potential spillover effects in **Sub-Sahara Africa, notably the Sahel, the Horn of Africa**, **and West Africa** the EU will reinforce support to the African Union, the Regional Economic Communities (RECs) and the countries in the region. In line with the EU Maritime Security Strategy[85] the EU will strengthen cooperation in the **Gulf of Guinea, Red Sea and Indian Ocean** to tackle trafficking and piracy, by supporting intra-Africa and regional cooperation, and with support of EU's Coordinated Maritime Presences (CMP) and the Maritime Analysis and Operations Centre (Narcotics) (MAOC-N).

With **Latin America and the Caribbean**, the EU will strengthen operational cooperation to dismantle and prosecute high-risk criminal networks and disrupt illicit activities and trafficking routes, enhancing cooperation frameworks, such as EU-CLASI (Latin American Committee on Internal Security) and the EU-CELAC Coordination and Cooperation Mechanism on Drugs. Logistic hubs' resilience and partnerships and follow-the-money approaches will be among the priorities. The EU will further support the development of the Police Community of the Americas (AMERIPOL) to become the regional equivalent of Europol and strengthen judicial cooperation between Member States and the region. The EU will also work with **South and Central Asia** on shared security challenges related to terrorism, trafficking of illicit goods, including drugs, trafficking in human beings and migrant smuggling.

In addition, the EU will support regional cooperation frameworks in third countries to further assist them in stopping illicit trafficking at the source, in line with the principle of shared responsibility for the whole criminal supply chain. Moreover, the EU will do its part to help

[84] Global Counterterrorism Forum, the Global Coalition against Da'esh, Global Internet Forum to Counter Terrorism (GIFCT), the Christchurch Call Foundation, the Global Coalition to Address Synthetic Drug Threats.
[85] JOIN (2023) 8 final.

strengthen the security of logistic hubs abroad, by coordinating **joint inspections in third country ports**.

Operational cooperation

Global Gateway will support sustainable and high-quality infrastructure projects in digital, climate and energy, transport, health, education and research sectors. The Commission will now include security considerations, where relevant, in the future Global Gateway investments. This will include initiatives critical to the strategic autonomy of the EU and its partner countries, such as infrastructure projects incorporating security assessments and risk mitigation measures.

The Commission will pursue further **agreements between the EU and third countries on cooperation with Europol and Eurojust**, notably with Latin American countries.

In addition, the proactive participation of non-EU countries in **EMPACT** is one of the most effective means of strengthening operational cooperation. The EU will further encourage the involvement of third countries, notably the Western Balkans, the Eastern Neighbourhood, Sub-Sahara Africa, North Africa, the Middle East, Latin America and the Caribbean, in the framework. Another tool to step up cooperation with third countries on combatting crime is the Operational Task Forces between Member States and coordinated by Europol, where third countries can participate. The Commission aims to also finalise negotiations for the **EU-Interpol** international agreement[86], ensuring a more unified approach to global security threats and fighting transnational crimes.

The **Union must be present on the ground in a Team Europe approach**. Specialist Union and Member State staff play a critical role in ensuring that the Union's external action is well informed, coordinated, and responsive. To elevate this approach to the next level, the Commission, supported by the High Representative for Foreign Affairs and Security Policy, will reinforce **liaison networks** and facilitate the deployment of regional **Europol and Eurojust liaison officers,** in line with the operational needs of Member States.

The EU will seek closer operational law enforcement and judicial cooperation, foster real-time information sharing and joint operations through **Joint Investigation Teams** in third countries with the support of Europol and Eurojust. The Commission will also support Member States in setting up **joint fusion centres** bringing together experts and local law enforcement in strategic third countries.

Common Foreign and Security Policy (CFSP) tools

The Common Security and Defence Policy (CSDP) missions will also be used to their full potential to better identify and tackle external threats to the EU's internal security, in line with their mandates set by the Council. To build third countries' capacities, the High Representative for Foreign Affairs and Security Policy and the Commission will support CSDP actions with dedicated funding instruments and explore all suitable avenues of funding.

EU restrictive measures are a well-established CFSP tool, also employed for the fight against terrorism. Based on suggestions from the High Representative for Foreign Affairs and Security Policy, Member States, or the Commission, the Council could assess how the EU's existing autonomous restrictive measures (EU terrorist list) could be made more effective, operational and agile. Moreover, they could consider exploring additional restrictive measures targeting criminal networks, in line with CFSP objectives.

[86] Council Decision (EU) 2021/1312 of 19 July 2021 & Council Decision (EU) 2021/1313 of 19 July 2021.

Visa policy and information exchange

The EU's visa policy is a key tool for cooperating with third countries and securing our borders by controlling entry into the EU and setting the conditions for it. The Commission will fully integrate **security considerations into the EU visa policy** through an upcoming EU Visa Policy Strategy. The Commission will work with the co-legislators to adopt the proposal to revise and streamline the Visa Suspension Mechanism, particularly for specific cases of misuse of the visa-free regime[87]. Third countries will be encouraged to share information about individuals who may pose security threats, which will be entered into EU information systems and databases.

To achieve policy coordination and upstream efforts, unlocking more efficient, swift and smooth cooperation, the Commission will work towards establishing **data flow arrangements** and explore ways to **enhance information exchange** for law enforcement and border management purposes with trusted third countries in compliance with fundamental rights and data protection rules.

Key actions

The Commission will:

- **conclude international agreements between the EU and priority third countries on cooperation with Europol and Eurojust**
- **encourage the participation of partner countries in EMPACT to fight organised crime and terrorism**
- **support EU agencies and bodies in establishing and strengthening working arrangements with partner countries**
- **further reflect security considerations in EU visa policy through the upcoming Visa Strategy**
- **strengthen information exchange with trusted third countries for law enforcement and border management purposes**

The Commission, in cooperation with the High Representative for Foreign Affairs, will:

- **make full use of civilian Common Security and Defence Policy (CSDP) missions**
- **coordinate joint inspections in third country ports by 2027**

The Commission, in cooperation with the High Representative for Foreign Affairs and the Member States, will:

- **reinforce liaison networks and cooperation in a Team Europe approach**
- **set up joint operational teams and fusion centres in third countries from 2025 onwards**

The European Parliament and the Council are urged to:

- **conclude negotiations on the revision of the Visa Suspension Mechanism**

8. Conclusion

In a world of uncertainty, the Union's capacity to anticipate, prevent and respond to security threats needs to be upgraded.

[87] COM (2023) 642.

It is not enough to only respond to crises when they occur. We need to sharpen our awareness with a full picture of the threats as they evolve. And to ensure our tools and capabilities are up to the task.

The comprehensive set of measures detailed in this Strategy will help create a stronger Union in the world: a Union that is able to anticipate, plan for, and take care of its own security needs, that can respond effectively to threats to its internal security and hold perpetrators accountable, and that protects its open, free and prosperous societies and democracies.

This demands a change in our mindset on internal security. We will work to help foster a new EU security culture, where security considerations are factored into all our legislation, policies and programmes – from inception to implementation. And where collaboration across policy areas allows us to break new ground.

This is not the task of just one institution, government or actor. It is Europe's common endeavour.