EUROPEAN
COMMISSION

HIGH REPRESENTATIVE
OF THE UNION FOR
FOREIGN AFFAIRS AND
SECURITY POLICY

Brussels, 10.10.2024
SWD(2024) 233 final

JOINT STAFF WORKING DOCUMENT

Eighth progress report on the implementation of the 2016 Joint framework on countering hybrid threats and the 2018 Joint communication on increasing resilience and bolstering capabilities to address hybrid threats

Eighth progress report on the implementation of the 2016 Joint framework on countering hybrid threats and the 2018 Joint communication on increasing resilience and bolstering capabilities to address hybrid threats

INTRODUCTION

A growing variety of harmful actions targeting the European Union (EU), its Member States and partners, pose a serious and complex threat to our democracy and shared European values. Russia's unprovoked and unjustified war of aggression against Ukraine, a gross violation of international law, poses a serious threat to European security, and conflicts in the European neighbourhood have underlined the need to continue supporting our partners in defending democracy and the importance of enhancing our own resilience to different types of hybrid threats and the cascading effects caused by nearby conflicts.

A multitude of elections took place in the EU and its partner countries in 2024, which was an important development during the reporting period. Several work streams focused on electoral and democratic resilience. In December 2023, the Commission adopted its **Defence of Democracy Package**[1], which deepens the measures taken under the European Democracy Action Plan[2]. Under the Code of Practice on Disinformation and European Digital Monitoring Observatory (EDMO), dedicated taskforces were established to focus on the European elections. In April 2024, the Belgian Presidency activated the **Integrated Political Crisis Response** (IPCR) arrangements in information sharing mode to pay special attention to foreign interference in the European elections.

In the context of the implementation of the **EU Strategic Compass for Security and Defence**[3] ("Strategic Compass"), , the Council validated the Guiding framework for the practical establishment of the EU Hybrid Rapid Response Teams in May 2024. The teams will be a key tool in the **EU Hybrid Toolbox**, deployable to provide short-term and tailored assistance to Member States, partner countries, or Common Security and Defence Policy (CSDP) missions and operations in countering hybrid threats. With the approval of the Guiding framework, the EU is strengthening its capabilities to counter hybrid threats.

Another significant achievement was the work of the **EU Partnership Mission to Moldova** to support Moldova in strengthening its resilience to hybrid, cyber, and foreign information manipulation and interference (FIMI) threats. The mission is in many ways a test case for supporting EU's partners in countering hybrid threats within the context of CSDP.

This annual progress report summarises the main developments in countering hybrid threats from July 2023 to June 2024. The report should be read in conjunction with the annual progress reports on the implementation of the EU Security Union Strategy, Strategic Compass and on the implementation of the common set of proposals endorsed by EU and North Atlantic Treaty Organization (NATO) Councils.[4]

[1] COM(2023) 630 final.
[2] COM(2020) 790 final.
[3] Council document 7371/22.
[4] COM(2024) 198 final; Report of the High Representative of the Union for Foreign Affairs and Security Policy to the Council, March 2024, HR(2024) 41; EEAS(2024) 691.

IMPLEMENTATION STATUS OF THE 2016 JOINT FRAMEWORK AND THE 2018 JOINT COMMUNICATION ON COUNTERING HYBRID THREATS

EU Intelligence and Situation Centre Hybrid Fusion Cell (HFC)

The HFC has continued to support policy preparation and decision-making at all levels by providing all-source intelligence-based strategic analysis on hybrid threats to the EU, its Member States and neighbourhood countries and interests. The HFC has also briefed various Council bodies.

In accordance with the priorities of the rotating Presidencies and requests by EU institutions, bodies and agencies (EUIBAs) and various entities within the Member States, the HFC has regularly analysed hybrid threats stemming from Russia's war of aggression against Ukraine, malicious use of new technologies, hostile intelligence activities and election interference, among others. A key focus area has been potential interference in the European elections in June 2024. The HFC organised a dedicated workshop with Member States' intelligence services in April 2024 and covered the topic in its intelligence reporting and verbal briefings.

In cooperation with the rotating Presidency of the Council of the EU, the HFC held bi-annual meetings of the **national points of contact for countering hybrid threats** (national POCs). It continued to cooperate with the Intelligence Production Unit within NATO's Joint Intelligence and Security Division. The HFC continued to provide support to the Commission's work on the resilience of critical infrastructure in the energy sector. In 2024, the HFC was involved in the analysis of the results of the stress tests conducted by Member States and provided input to the final report on the exercise.

Together with the EU Intelligence and Situation Centre (Intcen) counter-terrorism section, the HFC issued the second iteration of an intelligence assessment on threats to the EUIBAs, covering terrorism, cyber threats, espionage and malicious activities in the information domain.

The HFC-led annual **Hybrid Trends Analysis** covering 2023 was issued in April 2024 and included contributions from all Member States, EUIBAs and CSDP missions and operations.

Providing an exchange platform on cyber topics, the HFC organised classified workshops with Member States' intelligence and security services which resulted in issuing comprehensive cyber-threat landscape reports on the main threat actors targeting Member States in 2023. The HFC also contributed to the **Cyber Diplomacy Toolbox** by providing situational awareness and by participating in dedicated exercises. A dedicated team intensified cooperation with relevant EUIBAs, such as the European Union Agency for Cybersecurity (ENISA), the Cybersecurity Services for the Union institutions, bodies, offices and agencies (CERT-EU) and the European Police Office (Europol).

The HFC was actively involved in exercises, such as the **Space Threat Response Architecture 2024 exercise** (STRA-X-24) and the table-top exercise on electoral resilience initiated by the Belgian Presidency.

Strengthening institutional resilience

On 13 December 2023, a Regulation laying down measures for a high common level of cybersecurity at the institutions, bodies, offices and agencies of the Union[5] was adopted and entered into force on 7 January 2024. The Regulation focuses on internal cybersecurity risk

[5] OJ L, 2023/2847, 18 December 2023.

management, governance and control framework for each Union entity, it sets up a new Interinstitutional Cybersecurity Board (IICB) to monitor and support its implementation by Union institutions, bodies, offices and agencies, and it provides an extended mandate for the CERT-EU. If taken together with the parallel proposal on information security[6], that remains pending in negotiations, the new cybersecurity and information security rules will provide a stable ground for a secure European administration, allowing the EU to play a strategic role on the international stage.

The EU Security Union Strategy[7] and the **Strategic Compass[8]** announced the work on sectoral hybrid resilience baselines. Building on the 2022 Joint staff working document (JSWD)[9], the Commission's Joint Research Centre (JRC), assisted by the European Centre of Excellence for Countering Hybrid Threats (HCOE), published a Staff Working Document (SWD)[10] in January 2024, detailing essential gaps and needs within the existing resilience baseline elements at EU level by comparing them to the Comprehensive Resilient Ecosystem (CORE) model[11]. Moreover, the SWD highlights key areas for improvement and offers a set of recommendations to address the challenges identified.

Defending our democracies: elections, foreign information manipulation and interference (FIMI) and disinformation

Strategic communication, FIMI and disinformation

The EEAS continued to denounce Russia's full-scale invasion of Ukraine, to reinforce the EU's messages of support to Ukraine, and to raise public awareness on the Russian FIMI activities, including on the attacks against the EU and its Member States. In 2023, EUvsDisinfo, EEAS' flagship initiative for raising awareness on FIMI, reached around 20 million people. Efforts have been reinforced to reach out to the African continent and build resilience against FIMI by creating a dedicated Sub-Saharan Africa StratCom Task Force, adding to existing stratcom task forces covering the EU's western and southern neighbourhoods and the Western Balkans. As one of its first deliverables, the Task Force developed and delivered a pilot campaign around the 2nd Russia-Africa Summit held in July 2023 to expose the discrepancy between Russia's deceptive promises to African nations and actual delivery. The awareness raising campaign reached more than 6 million people across different channels and languages.

The **EU's FIMI Toolbox**, endorsed by the European Council in December 2023, was further developed through the establishment of the **FIMI Information Sharing and Analysis Centre** (FIMI-ISAC), which is a significant step towards building a whole-of-society approach, a network of relevant stakeholders to form a defender community, and a shared methodology to better detect, understand and respond to FIMI. In the context of the toolbox, work continued to better equip CSDP missions and operations to counter FIMI threats.

In January 2024, the EEAS published its **Second Report on FIMI Threats[12]**, proposing a *FIMI Response Framework* for practitioners and Member States with the aim of better linking

[6] COM(2022) 119 final.
[7] COM(2022) 252 final.
[8] Council document 7371/22.
[9] SWD(2022) 21 final.
[10] SWD(2024) 12 final.
[11] Aho A., Alonso Villota M., Giannopoulos G., Jungwirth R., Lebrun M., Savolainen J., Smith H., Willkomm E., Hybrid threats: A comprehensive resilience ecosystem, Publications Office of the European Union, Luxembourg, 2023, doi:10.2760/37899, JRC129019.
[12] https://www.eeas.europa.eu/eeas/2nd-eeas-report-foreign-information-manipulation-and-interference-threats_en

analysis and insights with timely and effective responses to FIMI. Additionally, in 2023, the EEAS published the **first report on FIMI targeting the LGBTIQ+** persons to help the defender community better understand and respond to the Tactics, Techniques and Procedures (TTPs) used to target LGBTIQ+.

In the run-up to the **2024 European Elections**, the EEAS further solidified its collaboration with the European Parliament and European Commission. The EEAS' contribution to the integrity of the European Elections rested on four pillars: increased situational awareness (e.g. via reports on Operation False Façade[13] and Doppelgänger[14]), increased awareness raising and resilience building (e.g. via EUvsDisinfo's elections-focused public-facing products[15]), stronger inter-institutional cooperation (e.g. via a dedicated tripartite working group), and preparedness and increased cooperation with EU Member States (e.g. via the Rapid Alert System).

The EEAS continued strengthening its **cooperation with international partners** both bilaterally (e.g. with the US, CA, the UK, among others) and multilaterally (e.g. via the G7 Rapid Response Mechanism (RRM)). Via the EU-US Trade and Technology Council, the two partners have agreed to use the same methodology to better detect, understand, and respond to FIMI. In the G7 RRM, the EEAS is chairing the working group that is responsible for developing the G7 Collective Response Framework that the G7 Leaders tasked the RRM to deliver by the end of 2024.

The **EU Code of Practice on Disinformation** signatory base continued to grow steadily, from 34 to 44 signatories. In March 2024, signatories submitted their reports under the new Code. The reports are available to the public through the new online Transparency Centre[16]. Through the **Code of Practice Task Force**, chaired by the Commission, signatories are working on topics like challenges related to generative AI, elections and FIMI campaigns, and the disinformation surrounding Russia's war of aggression against Ukraine. The Task Force also prepared indicators for measuring prevalence and sources of disinformation across major online platforms in the EU[17]. The Task Force set up a dedicated work-stream focused on elections to the European Parliament, and published reports in March 2024 on how signatories were preparing and putting in place measures to reduce the spread of disinformation prior to the 2024 European Parliament elections. It is foreseen that the Code of Practice will swiftly become part of the co-regulatory regime for very large online platforms provided for in the Digital Services Act (DSA), linking it to the DSA's enforcement mechanisms.

Six new national and regional **European Digital Media Observatory (**EDMO) hubs became operational in 2023, complementing the existing eight hubs to extend EDMO's reach and geographical coverage to the whole of EU. Their work is crucial to debunk and expose false claims and manipulated content, providing insight regarding disinformation, and supporting media literacy initiatives. The work by EDMO and the hubs has been instrumental in analysing disinformation on Russia's war of aggression against Ukraine and in the context of the Israel-Hamas conflict.

In 2024 EDMO set up a Taskforce on 2024 European elections, which provides comprehensive geographic coverage of the European Union through its national and regional hubs and builds upon the multi-disciplinary approach of EDMO. It brings together experts from different

[13] https://www.newtral.es/wp-content/uploads/2024/05/EEAS-DataTeam-TechnicalReport-FINAL.pdf?x95607
[14] https://euvsdisinfo.eu/uploads/2024/06/EEAS-TechnicalReport-DoppelgangerEE24_June2024.pdf
[15] https://euvsdisinfo.eu/european-elections/
[16] Transparency Centre: https://disinfocode.eu/reports-archive/?years=2024.
[17] https://www.trustlab.com/codeofpractice-disinformation.

professional backgrounds in academia, media ecosystem, fact-checking and media and information literacy (MIL).[18]

Five dedicated **EU research & innovation (R&I) projects** were launched, supporting the fight against disinformation, with a budget of EUR 28 million for 2022-2027. The projects aim notably at creating AI-based tools to detect deep-fakes and tampered content, in the form of videos, images and voice.

The Commission continued developing the **Network against Disinformation**, which coordinates Commission services on response to disinformation with a focus on thematic areas. In January 2024, the Commission invested further in this work with the creation of a strategic communications task force which will continue to operationalise the Network as well as further develop responses to disinformation and other strategic communications challenges.

As part of the **Digital Education Action Plan (2021-2027)[19]**, the Commission continued the targeted promotion of the Guidelines for teachers and educators on tackling disinformation and promoting digital literacy through education and training as to ensure that young people are equipped with skills and competences to engage critically with the online world and build resilience in relation to disinformation. In addition, teacher training and curriculum development in the field of digital literacy and tackling disinformation were among the priorities of the **Erasmus+ Forward Looking Projects** call, which looked for large-scale projects in the field, with the participation of national authorities. Six projects were awarded with a total budget of EUR 8 million.

During the 2024 European Parliament elections, the European Commission offered a data and fact-checking service[20] where journalists and fact-checkers could obtain data and statistics on the EU within one hour. The objective of this service was to provide factually correct information and resources to citizens and to contribute to fighting misinformation in the EU.

Securing free and fair elections and protecting democratic processes

Securing free and fair elections and protecting democratic processes is a priority for the Commission and is of critical significance in the work on hybrid threats this year. In March 2024, a Regulation on the **transparency and targeting of political advertising[21]** was adopted, entering into force in April 2024, while most provisions will enter into application in October 2025. It provides a common high standard of transparency for the provision of political advertising services in all media in the internal market and stronger protection for the use of personal data in the targeting and ad delivery of online political advertising. It supports oversight and empowers citizens to make informed choices and deters the misuse of political advertising as a vector of disinformation and FIMI. Concretely, it prohibits the provision of advertising services to third country sponsors three months before an election or referendum.

[18] EDMO's latest report on disinformation narratives during 2023 elections in Europe analysed over 1.000 fact-checking articles published in the context of thirteen elections in twelve different European countries: https://edmo.eu/publications/second-edition-march-2024-disinformation-narratives-during-the-2023-elections-in-europe/.

[19] COM(2020) 624 final.

[20] https://ec.europa.eu/eurostat/web/products-eurostat-news/w/wdn-20240510-1

[21] OJ L, 2024/900, 20.3.2024, p.1-44, part of the Commission's package of measures to reinforce democracy and protect the integrity of elections from November 2021.

On 12 December 2023, the Commission adopted its **Defence of Democracy Package**[22], which deepens measures taken under the European Democracy Action Plan[23]. The package includes measures to develop civic space and citizen participation to bolster democratic resilience from within. It includes a proposal for a Directive on transparency of interest representation for third countries. It also includes a Recommendation on inclusive and resilient electoral processes in the European Union and enhancing the European nature and efficient conduct of the elections to the European Parliament, to ensure that elections in the EU follow the highest democratic standards[24]. The Recommendation supports high voter turnout and inclusive participation, and makes it easier to exercise one's electoral rights. It also addresses the protection of election-related information and infrastructure, including cybersecurity, and promotes measures minimising the risk of interference from third countries as well as election observation, including by citizens.

The Commission has been following up on the Recommendation, by working with Member States especially in the framework of the European Cooperation Network on Elections (ECNE) to support preparedness and exchange information on issues affecting elections, including by jointly identifying threats and gaps and by sharing findings and expertise, in relation to foreign interference, among others. In that context, the Commission also organised joint sessions of ECNE with the Rapid Alert System (RAS) and the Network and Information Security (NIS) Cooperation Group. The main operational tool that the Commission uses to support Member States' authorities to prepare for and react to incidents affecting elections is the joint election resilience mechanism, which has been rolled out as of 2022.

On 26 March 2024, the Commission also published the **Digital Services Act Guidelines**[25] on recommended measures to providers of very large online platforms and search engines to mitigate systemic risks online that may impact the integrity of elections, with specific guidance for the European Parliament elections in June 2024. The guidelines also reflect several commitments and measures to reduce the spread of online disinformation contained in the Code of Practice on Disinformation.

As mentioned previously, the **EDMO** set up a taskforce to monitor the EU information ecosystem ahead of the 2024 European Parliament elections, and to facilitate communications and dissemination of research, MIL and fact-checking initiatives within the EDMO community and across the EU.

The European Centre of Excellence for Countering Hybrid Threats (Hybrid CoE)

The EUIBAs have intensified work with the Hybrid CoE on research, training, exercises and exchanges at different levels. In 2023, the Hybrid CoE organised various **events and seminars,** including the fourth EU-NATO High-Level Retreat for high-ranking civil servants from both organisations, along with several Hybrid 101 trainings to European Commission and EEAS officials. The Hybrid CoE also continued its dialogue with the European Parliament staff aimed at providing briefings on hybrid threats in 2024. A tailor-made workshop for EU and NATO policy planners took place in April 2024.

The Hybrid CoE cooperates with the rotating Presidencies of the Council of the EU based on their requests. In 2023-2024, the Hybrid CoE provided several briefings to the Council

[22] COM(2023) 630 final.
[23] COM(2020) 790 final.
[24] OJ L, 2023/2829, 20.12.2023, p. 1-18.
[25] https://ec.europa.eu/commission/presscorner/detail/en/ip_24_1707.

Horizontal Working Party on Enhancing Resilience and Countering Hybrid Threats (HWP ERCHT) and facilitated an exercise related to the EU elections and election interference.

The Hybrid CoE and the JRC continued to cooperate on many initiatives, including the CORE model, the Early Warning Indicators Playbook and the upcoming EU Science for Policy Report.

Protection of critical infrastructure

Member States are currently transposing the Directive on the **resilience of critical entities** (CER Directive)[26] that puts forward a clear set of obligations for Member States and critical entities, as well as mechanisms for cooperation and support at EU level. The transposition of the Directive by Member States should be done by 17 October 2024.

Moreover, Member States, Commission services and relevant EU agencies are participating in exercises that aim to improve the resilience of critical infrastructure, also in cooperation with strategic partners, such as NATO. In November 2023, the CORE23-B table-top exercise, organised by the JRC and NATO Energy Security Centre of Excellence, focused on the resilience of maritime critical energy infrastructure in the Baltic Sea region. In May 2024, Spain organised a live Maritime Security Exercise (MARSEC EU 24) which focused on the protection of critical underwater infrastructure. There was participation from EU institutions and agencies (EMSA, EFCA, Frontex), and from the navies and coast guards of seven EU member states (Belgium, France, Greece, Italy, Malta, Netherlands, Spain). Spain and France contributed with assets, while EMSA supported the activity with satellite imagery. The exchange of information via the Common Information Sharing Environment (CISE) network was also successfully tested, more specifically for the illegal, unreported, unregulated/IUU fishing scenario of the exercise.

The Commission stepped up the **cooperation on the protection of critical infrastructure with the authorities of Ukraine**. The joint work aims to support Ukraine in protecting its critical infrastructure, while at the same time allowing the EU and its Member States to benefit from the experience of Ukraine's services and to increase preparedness for possible attempts to disrupt critical infrastructure. In February 2024, a delegation of the Special State Service for Communications and Information Protection of Ukraine joined the Critical Entities Resilience Group and held a series of meetings with Commission services and the EEAS. The meetings further expanded ongoing cooperation in the operational, legal and research domains.

In October 2023, the Spanish Presidency set up a meeting of directors and authorities of Member States' agencies responsible for critical infrastructure protection and resilience. The aim was to expand the critical infrastructure community network as well as exchange best practices and challenges between Member States, including on implementation of the CER Directive, as well as discussions on experiences, threat landscape, policy measures and future perspectives.

In November 2023, the **Critical Entities Resilience Group (CERG) and the Network and Information Security (NIS) Cooperation Group** came together for a joint meeting in Madrid, the first such event organised to facilitate complementarity, coherence and coordination of cyber and physical (non-cyber) measures for the purpose of critical infrastructure resilience.

By the end of 2023, Member States finalised stress testing of critical infrastructure in the energy sector as a key action under the **Council recommendation on a Union-wide coordinated approach to strengthen the resilience of critical infrastructure**[27]. The stress test was based

[26] OJ L 333, 27.23.2022, p. 164.
[27] OJ C 20, 20.1.2023, p.1-11.

on common principles and scenarios developed at EU level and designed to enhance preparedness for sabotage and other hybrid threats. It was conducted by many operators in the energy sector under the guidance of Member States' authorities. Reporting by Member States to the Commission was completed in the first quarter of 2024, based on which an assessment report[28] with recommendations on how to further increase resilience was produced.

The EU-funded security research project EU-CIP[29] and European Knowledge Hub and Policy Testbed for Critical Infrastructure Protection are playing an important role in the identification of gaps and to increase the security and resilience of critical infrastructure in the EU.

In the defence sector, with the approval of the new **Capability Development Plan on 14 November 2023**[30], the protection of critical infrastructure officially became a capability development priority agreed by the Member States. The European Defence Agency (EDA) has conducted and scheduled some initiatives, specifically dedicated to the protection of maritime and seabed critical infrastructure, in line with the maritime domain priority Underwater and Seabed Warfare.

In March 2024, EDA hosted the first workshop for the PESCO project on **Critical Seabed Infrastructure Protection** (PESCO CSIP), which aims at delivering operationally relevant capabilities that will boost underwater situational awareness and enhance the protection of critical seabed infrastructure.

Furthermore, EDA, in cooperation with the Centre of Excellence for Operations in Confined and Shallow Waters (CoE CSW), organised a table-top exercise RUBIKON on critical maritime infrastructure protection on 28-29 May 2024. The exercise addressed the challenges to national and cross-border governance at operational level, involving three neighbouring coastal Member States in the North Sea, as a concrete step to enable Member States to respond in a coordinated manner to incidents targeting critical maritime infrastructure and their direct and indirect consequences.

Energy security of supply and energy infrastructure

The EU has adopted a number of new legislative acts to combat the energy crisis, strengthen preparedness and secure energy supplies, namely the REPowerEU plan, the Gas Storage Regulation, and the Temporary Emergency Regulation enhancing solidarity regulation **and the Critical Raw Materials Act**[31]. Additionally, **new electricity market design rules** were adopted on 21 May 2024 and the **Net-Zero Industry Act**[32] entered into force on 29 June 2024**.** With respect to gas, supplies have shifted from a high level of dependence on Russian pipeline to other suppliers. The transit agreement between Gazprom and Naftogaz through Ukraine is due to expire on 31 December 2024 and the Commission and the concerned Member States are jointly reviewing the preparedness for the end of Russian gas transit. The EU has made significant progress **towards the REPowerEU objective of phasing out Russian gas by 2027**. Since the amended Recovery and Resilience Framework Regulation[33] entered into force in March 2023, 23 REPowerEU chapters have been included in the national recovery and resilience plans. Those reforms and investments complement existing measures and provide

[28] Classified document, no reference available.
[29] https://cordis.europa.eu/project/id/101073878 - European Knowledge Hub and Policy Testbed for Critical Infrastructure Protection / EU-COP / Project / Factsheet / HORIZON / CORDIS / European Commission (Europa.eu).
[30] https://eda.europa.eu/publications-and-data/factsheets/factsheet-the-2023-eu-capability-development-priorities.
[31] OJ L, 2024/1252.
[32] OJ L, 2024/1735.
[33] OJ L 63, 28.2.2023, p. 1–27.

additional EUR 60 billion which are dedicated to increase energy savings, accelerate the clean energy transition, and diversify energy supplies in particular away from Russian fossil fuels.

On 21 May 2024, the Council and the Parliament adopted a regulation and a directive establishing **common internal market rules for renewable and natural gases and hydrogen** that will contain provisions allowing Member States to adopt restrictions to the supply of natural gas, including liquefied natural gas (LNG), from Russia or Belarus, with the aim of protecting the essential security interests of the Member States or of the EU, while taking account of security of supply and diversification objectives. Regarding storage, the Regulation adopted on 20 November 2023[34] sets the intermediate fillings targets that need to be met in 2024 to reach 90% of gas storage by 1 November 2024. On 4 March 2024, the Council reached a political agreement on a recommendation to encourage Member States to continue reducing their gas consumption until 31 March 2025, by at least 15% compared to their average gas consumption in the period from 1 April 2017 to 31 March 2022.

Specifically for the electricity sub-sector, the Network Code on sector specific rules for cybersecurity aspects of cross-border electricity flows[35] entered into force 13 June 2024. This Network Code builds upon the existing EU cybersecurity horizontal framework and includes rules on common minimum requirements, planning, monitoring, reporting and crisis management.

Resilience of energy infrastructure was addressed through the aforementioned stress tests and exercises.

Securing strategic domains

There has been an increasing need to adapt the transport sector to emerging hybrid threats. In this context, the main challenge for the Commission is to reconcile the safety of persons and goods with the openness and efficiency of the transport system and the specific business models of the different transport modes.

In the **aviation sector**, the Commission continued to regularly monitor emerging threats, including hybrid threats, to adapt the aviation security baseline.

As laid down in the **Drone 2.0 Strategy**[36], with a view to supporting a possible revision of existing aviation rules to enhance resilience against Unmanned Aerial (UA) threats, the Commission, in cooperation with the European Union Aviation Safety Agency (EASA) and Member States, conducted **a risk assessment on the threat posed by uncooperative UAs** to civil aviation and airport facilities in the first half of 2024.

Moreover, throughout the period under review, the Commission, in cooperation with the EEAS, EASA and Member States, **continued to regularly monitor and assess the security risk to civil aviation from conflict zones**, notably in relation to the Hamas-Israel conflict and its spill-over effects in neighbouring countries.

On **maritime security**, the Commission and the EEAS continued monitoring conflict events or situations that could impact maritime security. On 13 September 2023, the European Maritime Safety Agency (EMSA) and the Commission issued an **update to the Interim Guidance on Maritime Security for Member States' Competent Authorities**. The update reflects the experience gained from the Commission's maritime security inspections and shares best practices among Member States. Towards the end of 2023, the Commission prepared the fourth

[34] OJ L, 2023/2633, 23.11.2023.
[35] OJ L, 2024/1366.
[36] COM (2022) 652 final.

five-year report assessing the **implementation of the Directive on Enhancing Port Security**[37]. The report, which was launched for adoption in March 2024, covered the years 2019-2023 and showed some significant progress in a number of areas, as compared to previous years.

In the Red Sea, the Indian Ocean and the Gulf, a resurgence of a series of piracy incidents occurred at the end of 2023. Sabotage attacks off the coast of Yemen also started to quickly escalate at the end of 2023, with missile and drone attacks against merchant ships. In light of this, on 19 February 2024, the EU launched a new **EU CSDP operation EU NAVFOR ASPIDES** to secure freedom of navigation in the Red Sea and the Gulf of Aden.

The revised **EU Maritime Security Strategy (EUMSS) for evolving maritime threats and its Action Plan** were adopted on 24 October 2023. The actions described within this progress report are, to a great extent, included in the revised EUMSS and its action plan.

On maritime surveillance, the EDA continued to develop the technology supporting the MARSUR Networking project. The new generation technology, MARSUR III, is expected to be delivered by the end of the first semester of 2024, with an operational demonstration foreseen at the end of the year within a CSDP operation (Atalanta or Irini). Furthermore, participating Member States are developing the necessary capabilities and processes for the exchange of classified information, a crucial step in information sharing that will improve addressing hybrid threats in cross-border scenarios.

The maritime surveillance and situational awareness community has also worked towards improved connectivity and deeper synergies between existing systems. In March 2024, a bilateral agreement between EDA, on behalf of MARSUR III contributing members, and the European Union Satellite Centre (Satcen) was concluded, which was a key milestone that will boost MARSUR's awareness capabilities. Furthermore, there is increased civilian-military cooperation, with the revised EUMSS highlighting the MARSUR-CISE adaptor as a core priority for the EU's maritime security.

Border and supply chain security

The **EU Migration Preparedness and Crisis Blueprint Network**[38] provides a permanent operational framework for monitoring and early detection of migration flows in the EU. Thanks to the continuous cooperation and information sharing among the Commission services, the EEAS, the agencies and Member States, the Network enables a joint situational awareness on migration, including on potential hybrid threats, such as instrumentalisation of irregular migration. The regular monitoring of the situation and its analysis allows for early warning, anticipation of crisis and is the basis for swift decision-making and coordinated operational response.

The instrumentalisation of migration and other government-sponsored threats of a hybrid nature are an essential part of the risks at the external borders. Several Member States, especially at the Eastern land border of the Schengen area, have experienced this. Consequently, tackling hybrid threats is a top priority in the Union's policy actions.

The **2024-2026 Strategic Risk Analysis** (SRA) by Frontex is a strategic foresight exercise for the European Border and Coast Guard. The SRA 2024 focuses on the European integrated

[37] OJ L 310, 25.11.2005, p. 28–39.
[38] OJ L 317, 1.10.2020, p. 26–38.

border management across the four-tier access control model and the main challenges the European Integrated Border Management (EIBM) might focus during the forthcoming 10 years.

In order to implement the multiannual strategic policy for European integrated border management, on 20 September 2023, Frontex adopted **the Technical and Operational Strategy for European Integrated Border Management 2023-2027**[39]. In addition, Member States are expected to establish their national strategies for European integrated border management through close cooperation between all national authorities responsible for the management of external borders and return.

On the basis of the overview of the national capability development plans, and taking into account, inter alia, the results of the risk analysis and vulnerability assessments, and the Agency's own multiannual plans, Frontex adopted a capability roadmap on 26-27 March 2024, which has the objective of converging the capability development plans of Member States and the multiannual planning of the Agency's resources to optimise long-term investment to best protect the external borders.

In February 2024, a provisional agreement was reached by the Council and the European Parliament on the **Internal Market Emergency and Resilience Act**[40] (IMERA, formerly known as the Single Market Emergency Instrument). This agreement will provide a general framework for anticipating, preparing, mitigating and minimising the negative impacts which any crisis may cause on the functioning of the Single Market and its supply chains. This will help mitigate the harmful impact on the Single Market, safeguard the free movement of persons, goods and services and maximise the availability of products needed in the crisis response.

The **Customs Control Equipment Instrument (CCEI) programme**[41] is funding the transparent purchase, maintenance and upgrading of relevant, state-of-the-art equipment to support customs authorities in their related risk management and controls activities. The Second CCEI call 2023-2024 with a total budget of 284 million euro was completed in June 2024 and Member States will launch their procurements. These continuous investments in customs detection and control equipment will strengthen the capacity of customs in ensuring the security of the EU in general.

Space

The implementation of the **Union secure connectivity programme for the period 2023-2027** is ongoing with a view to providing secure, high-quality and reliable communications services to Member States and EU institutions from 2027. This involves prospective deployment of an autonomous and multi-orbital satellite connectivity infrastructure, IRIS² Infrastructure for Resilience, Interconnectivity and Security by Satellite. The new space constellation will support protection of critical infrastructure across the EU, contribute to situation awareness and external action policies, crisis management and other applications for the benefit of EU economy as well as security and defence. The geographical coverage will extend to areas of EU strategic interest, such as in particular Africa and the Arctic. The **GOVSATCOM component of the EU Space Programme is also being implemented,** with the objective of providing satellite communication for EU and national public authorities based on existing national satellite providers. A ground infrastructure to pool together the satellite resources is being developed, and initial services will start to be provided to users at the end of 2024.

[39] https://www.frontex.europa.eu/assets/Key_Documents/IBM/EU_IBM_Brochure_EN.pdf.
[40] https://single-market-economy.ec.europa.eu/news/commission-welcomes-agreement-crisis-proofing-single-market-2024-02-02_en.
[41] OJ L 234, 2.7.2021, p. 1–17.

The 2023 revision of the Capability Development Priorities has prioritised separately Space Services and Space Operations, to emphasize the growing concerns in the space domain with respect to security and defence, as expressed in the EU Space Strategy for Security and Defence. Space Operation capabilities are aimed at monitoring, with the development of a Space Situational Awareness (SSA) capability, at protecting space assets, including via on-orbit operations, and at ensuring a responsive access to space. The resilience and responsiveness of Space Operation capabilities crucially depend on Space Situational Awareness capabilities, as does a reliable and unconstrained access to space. Space capabilities are also indispensable enablers for both civilian services and space activities while also supporting military operations in all operational domains. Continuous focus on Space Services and development of space-based technologies enabling Earth Observation, Satellite Communication, and Positioning, Navigation and Timing, will further enhance their performance and resilience, thus responding to growing operational needs.

Defence capabilities

On 5 March 2024, the Commission and the High Representative adopted a Joint Communication on a new **European Defence Industrial Strategy (EDIS)**[42] to strengthen the competitiveness and readiness of the European Defence Technological and Industrial Base (EDTIB). On the same day, the Commission also adopted a proposal for a Regulation to start implementing concrete measures identified in the EDIS, known as the **European Defence Industry Programme (EDIP)**[43]. The Strategy had been announced by Commission President von der Leyen during her 2023 State of the Union Speech. Following Russia's unprovoked war of aggression against Ukraine, the EU needs to continue toprovide military support to Ukraine and enhance its own defence readiness. EDIS proposes a number of actions, namely to strengthen the European Defence Technological and Industrial Base (EDTIB) through increased and more collaborative European investment from Member States; improve the responsiveness of the European defence industry under any circumstances and time horizon; mainstream a defence readiness culture; and team up with strategic, like-minded and international partners.

With respect to space and defence, the Observatory of Critical Technologies (OCT) will identify dependencies and criticalities of supply chains for space missions and key defence capabilities. At the end of 2023, a first classified report on microelectronic components was delivered to Member States in view of the OCT Experts Group meeting in February 2024. The OCT will look into new technologies on a regular basis and will monitor the identified criticalities.

After consultation with Member States and relevant industrial actors, the OCT will present roadmaps for mitigation measures on how to deal with the dependencies and criticalities in the relevant fields covered by the OCT.

The revised **EU Capability Development Priorities** approved by Ministers of Defence in November 2023 reflect the changes in the EU's strategic environment, political guidance provided by the Strategic Compass as well as lessons observed from Russia's war of aggression against Ukraine. The revised Capability Development Priorities will serve as the central reference for defence planning and the baseline for all EU-wide defence-related initiatives and instruments, such as the Coordinated Annual Review on Defence (CARD), the Permanent Structured Cooperation (PESCO), the European Defence Fund (EDF) and any future defence-related frameworks.

[42] JOIN(2024) 10 final.
[43] COM(2024) 150 final.

Upon participating Member States' request, EDA facilitates management of PESCO projects. In the area of countering hybrid threats, EDA is currently engaged in supporting the implementation of the PESCO projects on the Cyber Rapid Response Teams and the Cyber and Information Domain Coordination Centre.

Protecting public health and food security

The Commission convenes the European Food Security Crisis Preparedness and Response Mechanism expert group (EFSCM) in case of emergency or crisis without delay and as often as needed, to contribute to the response. This expert group also meets periodically to increase the EU's degree of preparedness for food security. To enhance preparedness, on 23 July 2024, the EFSCM published recommendations on ways to address or mitigate risks and vulnerabilities in the EU food supply chain[44], based on a 2023 Joint Research Centre mapping study[45]. The Commission also convenes the Health Security Committee which coordinates prevention, preparedness and response planning, risk/crisis communication and national responses of EU/EEA countries in response to the serious cross-border threat to health.

Chemical, biological, radiological and nuclear (CBRN) risks

The findings of a study on the feasibility of restricting access to dangerous chemicals that can be used for terrorist attacks paved the way for a robust **impact assessment on regulating the marketing and use of high-risk chemicals that can be used for terrorist attacks,** which was completed in January 2024. The impact assessment concluded that high-risk chemicals should be regulated in a similar manner to explosives precursors in the EU. The legislative proposal will be tabled subject to the political approval of the new Commission under the new mandate.

CBRN Defence has also been designated as an **EU Capability Development Priority** reflecting the need for the upgrade and development of advanced individual and collective protection methods and systems against evolving CBRN hazards.

Cybersecurity

Member States are currently adopting the **Directive on measures for a high common level of cyber security across the Union** (NIS 2 Directive). Similar to the transposition of the CER Directive, this process should be completed by 17 October 2024. The Directive strengthens security requirements with a list of focused measures, including incident handling and crisis management, supply chain security, vulnerability handling and disclosure, cybersecurity testing, the use of cryptography, and, where appropriate, encryption.

In September 2023, a pilot course *The Contribution of Cyber in Hybrid Conflict* was organised for the second time by EDA in cooperation with the European Security and Defence College (ESDC) and Hybrid CoE in Helsinki. The aim of the course was to explain the key elements of cyber defence and hybrid threats, and to provide the audience with the necessary practice, via a decision-making exercise, in understanding and addressing the implications of the intersection of cyber and hybrid threats, attacks and campaigns.

In November 2023, a table-top exercise funded through the joint election resilience mechanism, was organised by the Commission to enhance resilience for the upcoming European elections.

[44] https://agriculture.ec.europa.eu/news/proofing-eu-food-supply-chain-against-crises-new-set-recommendations-published-2024-07-23_en

[45] https://publicaFtions.jrc.ec.europa.eu/repository/handle/JRC135290.

The exercise simulated a realistic cyber incident targeting the European elections and was attended by cyber and electoral experts from 25 Member States.

With regard to the **European elections**, the Commission has taken a number of actions to safeguard the elections' integrity. In December 2023, the Commission published a **Compendium of e-voting and other information and communication technology practices**[46] which also address protection against cyber risks. In March 2024, the NIS Cooperation Group, with the support of the Commission and ENISA, published the **Compendium on the Cybersecurity of Election Technology**[47]. This new edition of the Compendium lays out recommendations to Member States, steps to take and useful guidance in managing potential cyber incidents at each stage of the electoral process. It includes an update of the elections threat landscape, new and revised case studies, cybersecurity best practices and an examination of the potential threats deriving from emerging technologies that could affect elections' resilience, namely FIMI, disinformation on social media, AI and deep fakes.

Cybersecurity in the energy sector

On 11 March 2024, the **Commission adopted a Network Code on Sector Specific Rules for Cybersecurity Aspects of Cross-Border Electricity Flows**[48]. The network code aims to establish a recurrent process of cybersecurity risk assessments in the electricity sector. The assessments will aim to systematically identify the entities that perform digitalised processes with a critical or high impact on cross-border electricity flows, their cybersecurity risks and the necessary mitigating measures that they need to implement. Multiple methodologies and standards exist today in the cybersecurity industry. The network code promotes the use and alignment with existing mechanisms established in the horizontal legislation, like the NIS 2 Directive.

Cybersecurity in the financial services sector

In the financial sector, on 22 February 2024, the Commission adopted two delegated regulations supplementing Regulation (EU) 2022/2554 (DORA) on further specifying certain designation criteria and the fees to be paid by the critical ICT third-party service providers[49]. On 13 March 2024, the Commission also adopted three delegated regulations supplementing Regulation (EU) 2022/2554 (DORA) with regards to regulatory technical standards on ICT-related incidents and cyber threats, the ICT risk management framework and the policy on contractual arrangements for the use of ICT services by ICT third party service providers[50]. All these policy products contribute to further strengthening the digital operational resilience of the EU financial sector.

Cybersecurity in the transport sector

Within the scope of the existing EU regulatory framework for cybersecurity in **civil aviation,** work on aligning aviation cybersecurity requirements has continued in the Aviation Cybersecurity Working Group, intensifying efforts in 2024 through a new sub-group involving competent authorities for aviation safety, aviation security and NIS 2. International activities have allowed for regular exchanges on aviation cybersecurity with key partner states, such as

[46] https://commission.europa.eu/document/download/b0898ba3-c7ad-4af5-8467-5e23a0469a78_en?filename=compendium.pdf
[47] https://ec.europa.eu/information_society/newsroom/image/document/2018-30/election_security_compendium_00BE09F9-D2BE-5D69-9E39C5A9C81C290F_53645.pdf.
[48] C(2024) 1383 final.
[49] C(2024) 902 and C(2024) 896.
[50] C(2024) 1519 final, C(2024) 1532 final and C(2024) 1531 final.

the United States, Brazil and international organisations (International Civil Aviation Organization, European Civil Aviation Conference and Eurocontrol). Since 2023, EASA is also working with all EASA States Civil Aviation Authorities to achieve a timely and harmonised implementation of the Part-IS Regulatory Framework for cyber-resilient aviation[51].

The Second Transport Cybersecurity Conference was organised on 2 May 2024 by the Commission as a dynamic platform to bring together stakeholders from the transport sector and cybersecurity.[52]

The revised Regulation for the trans-European transport network[53], which entered into force on 18 July 2024, explicitly acknowledges the importance and potential impacts of foreign investments on the trans-European transport network (TEN-T) and even includes a specific article on 'risks to security or public order'. Through the implementation of this Regulation, Member States should ensure that particular attentions is paid to foreign investments into transport infrastructure and assets with a cross-border impact, or those that are crucial for enabling military mobility in Europe.

In the rail sector, the Working Party on Rail Security, under the Commission Expert Group on Land Transport Security, has continued to focus on cybersecurity as one of the priority areas, with ENISA regularly updating on the cyber threat landscape. The rail sector also falls under the scope of the **Cyber Resilience Act**.

With respect to the **maritime sector**, on 22 November 2023, the Commission and EMSA published a **guidance document on how to address cybersecurity onboard ships during audits, controls, verifications and inspections[54].** The purpose of this document is to offer guidance to Member States' administrations and national inspectors/auditors/surveyors on how to address cybersecurity-related elements during audits, controls, verifications, and inspections of ships. The Commission also worked with EU Member States and third countries (e.g. United States, UK, Singapore) to strengthen guidelines[55] on maritime cybersecurity at the International Maritime Organization (IMO), and to propose other future steps to enhance maritime cybersecurity internationally.

EMSA also organised a Maritime Cybersecurity Conference on 26 October 2023, with the participation of more than 100 EU maritime cybersecurity stakeholders coming from the European Commission, ENISA, Member States, port authorities, industry and academia. Moreover, the EMSA Academy developed and delivered a Maritime Cyber Security (MCS) training course specifically designed for national administration officers having a role in developing or enforcing cybersecurity regulations in the maritime domain. The course was delivered in a blended mode from 30 October to 10 November 2023.[56]

Cyber defence

Through the **EU Policy on Cyber Defence[57],** the EU is investing in its resilience, including through the development and lawful deployment of full spectrum defensive cyber capabilities. Member States, the EEAS, the Commission services and the EDA reported on their respective

[51] OJ L 248, 26.9.2022, p. 18 and OJ L 31, 2.2.2023, p. 1.
[52] https://transport.ec.europa.eu/news-events/main-events/2nd-transport-cybersecurity-conference_en.
[53] OJ L 2024/169, 28.6.2024, p. 1.
[54] European Commission MARSEC Doc. 9209.
[55] Submission MSC 108/6, "Proposed revision of the 2017 Guidelines on Maritime Cyber Risk Management (MSC--FAL.1/Circ.3/Rev.2)", submitted to IMO on 13 February 2024.
[56] https://www.emsa.europa.eu/newsroom/latest-news/item/5068-part-time-course-on-maritime-cybersecurity-now-completed.html.
[57] JOIN (2022) 49 final.

actions and commitments in the Annual Progress Report of the EU Cyber Defence Policy, called the EU Cyber Census. Work will continue to reinforce coordination and cooperation mechanisms among national and EU cyber defence players, invest in cyber defence capabilities and strengthen security and defence partnerships in the area of cyber defence.

Framework for a joint EU diplomatic response to malicious cyber activities (Cyber Diplomacy Toolbox)

In line with the 2023 revision of the Implementing Guidelines of the Cyber Diplomacy Toolbox, aiming at developing of sustained and tailored approach towards persistent cyber threat actors, the Cyber Diplomacy Toolbox was used on multiple occasions to deter and respond to malicious cyber activities targeting the EU and its partners. On 24 June 2024, the Council approved additional restrictive measures against six persons involved in cyber-attacks affecting the EU and Member States.

International cooperation on cybersecurity

The EU continues to promote a global, open, stable and secure cyberspace, grounded in the United Nations framework for responsible state behaviour in cyberspace[58]. To this end, the EU and Member States continued to promote the establishment of a United Nations Programme of Action[59] as a single permanent platform to implement and advance responsible state behaviour in cyberspace.

The EU holds regular cyber dialogues with many partner countries, tackling all cyber issues, including cybersecurity, cybercrime, cyber diplomacy and cyber capacity building as well as increasingly cyber defence. Cybersecurity and cyber defence were discussed during several security and defence dialogues. During the period under review, the EU held **Cyber Dialogues** with a number of third countries, namely Ukraine, India, Japan, the United States and the UK. In June 2024, an informal EU-Africa dialogue on cyber and digital policy took place under the Belgium Presidency.

The EU and Ukraine continue to work together to enable Ukraine to prevent, deter and respond to cyber threats, including through increased information sharing and capacity building efforts. In November 2023, the ENISA and Ukrainian counterparts signed a **working arrangement to further strengthen cooperation on capacity-building**, best practices exchange and to boost situational awareness.

The ASEAN-EU Joint Ministerial Statement of February 2024 highlighted the exploration of joint activities with the ASEAN-Singapore Cybersecurity Centre for Excellence and the ASEAN-Japan Cybersecurity Capacity Building Centre to step up cooperation[60].

The EU also continued its **cyber capacity building projects** in the neighbourhood, including in the Western Balkans, Ukraine, Georgia and Moldova, as well as other partner countries experiencing a rapid digital development. Increased demand for cyber capacity building is emerging also from the Indo-Pacific, Africa and Latin America.

The EU will maintain its engagement for the development and implementation of **confidence building measures (CBMs)**, notably in the Organisation for Security and Cooperation in Europe (OSCE), the Organization of American States (OAS) and the ASEAN Regional Forum.

[58] https://disarmament.unoda.org/ict-security/
[59] https://documents.un.org/doc/undoc/ltd/n23/317/97/pdf/n2331797.pdf
[60] https://asean.org/wp-content/uploads/2024/02/FINAL-Joint-Ministerial-Statement-24th-ASEAN-EU-Ministerial-Meeting.pdf.

In this context in June 2024, the EU and Singapore have organised a workshop on the protection of critical infrastructure.

Economic security

The Commission and Member States continued their cooperation on FDI transactions likely to affect security or public order. This cooperation mechanism was set up by Regulation (EU) 2019/452[61] and has been fully applicable since 11 October 2020. The Commission published its **third annual report[62]** on the implementation of the Regulation in October 2023. The report's findings demonstrate a clear commitment by the Commission and Member States to safeguarding European security and public order in times of increased geopolitical tensions. Between July 2023 and June 2024, **five more Member States started fully implementing a national FDI screening mechanism.**

Implementation of European Economic Security Strategy continued throughout the reporting period. On 3 October 2023, the Commission adopted a Recommendation on critical technology areas for the EU's economic security for further risk assessment with Member States.[63] In the Recommendation, the Commission identified a list of 10 critical technology areas for the EU's economic security, with four technology areas (advanced semiconductor technologies, artificial intelligence technologies, quantum technologies and biotechnologies) highly likely to present the most sensitive and immediate risks related to technology security and technology leakage and recommended for joint risk assessments with EU Member States. The first risk assessment reports[64] on these four critical technology areas were transmitted to the Council on 27 March 2024. The Commission and the Member States are continuing their assessment on selected deep dive high risk scenarios.

The economic security package also included a White Paper on Export Controls proposing both short and medium-term actions to improve the coordination of export controls on items with both civil and defence uses, in full respect of the existing rules at EU and multilateral level. The Commission proposed to introduce uniform EU controls on those items that were not adopted by the multilateral export control regimes due to the blockage by certain members. This would avoid a patchwork of national approaches. The White Paper also provides for a senior level forum for political coordination and announces a Commission Recommendation in the summer 2024 for an improved coordination of National Control lists prior to the planned adoption of national controls. The evaluation of the EU Dual-Use Regulation is advanced to 2025.

On 24 January 2024, the Commission adopted five initiatives to strengthen the EU's economic security, including a **legislative proposal to revise Regulation (EU) 2019/452[65]** to further strengthen the protection of EU security and public order by proposing improved screening of foreign investment into the EU. This legislative proposal builds on the experience gained by the Commission and Member States with reviewing over 1,200 FDI transactions notified by Member States over the previous three years under the existing FDI Screening Regulation. It aims to address existing shortcomings and improve the efficiency of the system by ensuring that all Member States have a screening mechanism in place, with better harmonised national rules; identifying minimum sectoral scope where all Member States must screen foreign

[61] OJ L 79I, 21.3.2019, p. 1.
[62] COM(2023) 590 final.
[63] C(2023) 6689 final.
[64] Classified as RESTREINT EU/EU RESTRICTED
[65] COM/2024/23 final.

investments; and extending EU screening to investments by EU investors that are ultimately controlled by individuals or businesses from a non-EU country.

Another initiative in the economic security package was a proposal for a **Council recommendation on enhancing research security.** The Recommendation[66], adopted by the Council on 23 May 2024, identifies risks deriving from international cooperation in research and innovation, relating mainly to the areas of undesirable transfer of knowledge, foreign interference, and ethical or integrity violations. The recommendation is not legally binding but offers guidance for measures that could be taken by the Commission, the Member States and the research community.

The revised Financial Regulation[67] has proposed a clear horizontal framework for Union award procedures for which a protection of the security and public order of the Union and its Member States is necessary. The new provision will provide a toolbox of specific conditions for the participation sensitive Union award procedures and the rules and procedures to apply these conditions. With the entry into force of the new Financial Regulation, this new stable legal basis will improve protection of security and public order interest of the Union throughout its funding and procurement activities.

Building resilience against radicalisation and violent extremism

The Commission adopted a report on 14 February 2024, which concludes that the **Terrorist Content Online Regulation[68]**, which applies since 7 June 2022, has had a positive impact in limiting the spread of terrorist content online. Indeed, at least 349 removal orders have been issued by Member States' competent authorities between June 2022 and 31 December 2023, leading to terrorist content being taken down or access thereto blocked.

The EU is also working to **prevent foreign influence and funding fostering radical/extremist views** in the Member States. The Commission remains vigilant to prevent EU funds supporting any project incompatible with European values or pursuing an illegal agenda. The revised Financial Regulation now includes conviction for "incitement to hatred" as grounds for exclusion from EU funding. In addition, the Commission is undertaking internal awareness-raising measures and developing internal working methods to ensure increased scrutiny in the selection of projects.

The **strategic orientations on a coordinated EU approach to prevention of radicalisation for 2024 and 2025[69]** focus on several activities that contribute to increasing resilience, strengthening Member States' capacity in strategic communication and preventing radicalisation.

The **EU Internet Forum** (EUIF), chaired by the Commission, continues to provide a platform for voluntary collaboration with the technology industry to respond to emerging challenges online. In 2023, the EUIF produced several tools for technology companies to guide their content moderation efforts of violent extremist and terrorist content online[70]. The EUIF also

[66] Council document 9097/1/24.
[67] European Parliament, P9_TA(2024)0163, Financial rules applicable to the general budget of the Union.
[68] OJ L 172/79, 17.5.2021.
[69] https://home-affairs.ec.europa.eu/document/download/a4bd65f1-4987-4213-851c-df5b2d071d49_en?filename=Strategic%20Orientations%202024-2025_en.pdf%20[2]%20https://home-affairs.ec.europa.eu/system/files/2023-05/EUIF_Factsheet_May_2023.pdf.
[70] These include the knowledge package of violent right-wing extremist groups, symbols and manifestos, detecting financing activities of violent extremists, and a handbook on video-gaming to empower users detecting and identifying harmful content to build their resilience.

developed a handbook on borderline content in relation to violent extremism with the objective to raise awareness about the links between borderline content, such as disinformation and forms of hate speech, and violent extremism, and gather guidelines for companies to understand, detect, moderate and respond to borderline content better. The EUIF also revised the **EU Crisis Protocol** to prevent the spread of terrorist content online in relation to a real-life attack and tested the revised Protocol in presence of international partners in early 2024.

Recent terrorist attacks have shown an early use of generative-AI content mixing terrorist content with disinformation. The EUIF is addressing the risks and opportunities of generative AI in 2024 to prevent its exploitation and increase resilience of citizens. The EUIF will expand its membership this year to companies offering generative-AI services, internet infrastructure providers and financial technology companies to address the misuse of internet by malicious actors more holistically. The EUIF continues to provide alternative narratives to radicalised viewpoints and terrorist propaganda and supports fundamental rights and values through the Civil Society Empowerment Programme (CSEP). CSEP assists civil society, grass roots organisations and credible voices in their work on alternative narrative. The first iteration of CSEP came to end in 2023, but a new call for proposals is foreseen in 2025, which aims to build on the lessons learned from the previous programme.

There is often a continuum between radicalisation and violent extremism and manifestations of hate speech online and hate crimes. In December 2023, the Commission and the High Representative adopted a Joint Communication 'No place for hate: a Europe united against hatred'[71]. It aims to step up EU efforts to fight hatred in all its forms, by reinforcing action across a variety of policies. These include stepping up the work on combating hate speech online through an upgrade of the Code of conduct agreed with major online platforms and measures to enhance the protection of places of worship via an increased budget of the Internal Security Fund.

Increasing cooperation with partner countries

The European Commission continued to support the **Western Balkans** on cyber resilience through its regional programmes on cybersecurity and critical infrastructure protection (CIP) and since November 2023 also via the Growth Plan, with increasing engagement by ENISA. The latter includes cybersecurity as one of the priorities, emphasising the importance of integration with the European Union's Digital Single Market. The Rapid Response action funded by the Neighbourhood, Development and International Cooperation Instrument (NDICI) was renewed to increase the resilience of the Western Balkan countries to hybrid threats resulting from Russia's war of aggression against Ukraine. The cybersecurity crisis response support measure for the aligned Common Foreign and Security Policy (CFSP) countries was also renewed, aiming to empower partner countries to respond to cyber incidents. The Commission also continued to support the region through its five ongoing programmes aiming at tackling disinformation and radicalisation, supporting independent media, and promoting digital and media literacy in the region, as well as the Western Balkans regional communication programme WeBalkans (2024-2027) and through TAIEX and Twinning instruments.

In 2023, responding to the continued high-risk environment due to Russian large-scale cyber-attacks, the first phase of the regional cyber programme managed by the Commission, "Cybersecurity East", provided important capacity-building support to the countries in the **Eastern Neighbourhood** with particular focus on **Ukraine, Moldova and Georgia**. The

[71] https://commission.europa.eu/document/download/c60c451c-ccd2-406a-be3a-ef65123f2bb6_en?filename=JOIN_2023_51_1_EN_ACT_part1_v8.pdf.

cybersecurity component of the project helped to develop technical and cooperation mechanisms that increase cybersecurity and preparedness against cyber-attacks. A cybercrime component of the project provided capacity-building support to countries to implement the Budapest Convention, including stepping up the work in the area of collection of electronic evidence that can be used in prosecuting war crimes. In this context, the Commission launched a second phase of the cybercrime component of the CyberEast+ programme in the second quarter of 2024, with the expected launch of the cybersecurity component in the third quarter of 2024. In addition, the Rapid Response Pillar under the NDICI was also extended, with the aim of supporting resilience against diverse hybrid threats, including in the information and cyber domains. The Commission continued to support the region through its four ongoing programmes and various grants aiming at assisting independent media and civil society, its TAIEX and Twinning instruments, as well as its regional communication programme EU NEIGHBOURS East.

In **Moldova,** the Hybrid Risk Survey recommendations were adopted in July 2023 and are being addressed jointly, drawing on appropriate funding mechanisms. The recommendations are especially pertinent as Moldova has entered a prolonged election period, including the EU referendum which will take place alongside presidential elections in October 2024, characterised by the use of hybrid methods. A tailored seminar addressing hybrid threats with the participation of EUPM and a strategic TAIEX assistance on cyber resilience are scheduled prior to the elections. Under the NDICI Rapid Response Pillar, support focuses on strengthening the resilience of the Republic of Moldova to foreign interference, the consequences of the energy crisis and the Russian war of aggression against Ukraine. A project on cybersecurity that aims to enhance the cyber resilience of Moldovan beneficiaries in compliance with the EU acquis and best practices is now in its second phase. It provides assistance to Moldovan key public authorities in strengthening cybersecurity capacities, protecting critical information systems from cyber threats, and supporting the implementation of cybersecurity-related normative framework **Georgia** was granted candidate status in December 2023, on the understanding that the relevant steps set out in the Commission recommendation of 8 November 2023 are taken. The first step requires Georgia to actively fight FIMI, including disinformation, against the EU and its values. New assistance measures to combat disinformation and tackle hybrid threats were adopted in December 2023 to support Georgia in this endeavour. However, due to the recent adoption by the Georgian Government of the Law on transparency of foreign influence and other decisions, and following discussions in the Foreign Affairs Council of 24 June and the European Council of 27 June, implementation of the project has been halted pending further developments. In the **Southern Neighbourhood**, the Commission conducted a needs assessment on media support in the region, focusing also on the challenge of FIMI, including disinformation. The outcomes and recommendations will feed the overall support in media and freedom of expression. At the same time, continued support to the region was registered through its four ongoing programmes aiming at assisting independent media and civil society, as well as its regional communication programme EU NEIGHBOURS South.

The Commission also launched a new phase of its regional programme on cybercrime "CyberSouth", starting in 2024 and potentially extending to new countries. A new regional action is also being designed, with the aim to support the development of digital skills and increase the cybersecurity capacities of national agencies of partner countries.

In addition, the Enhancing Security Cooperation in and with Asia (ESIWA) is an EU flagship project on security cooperation in the **Indo-Pacific**. It acts as an 'umbrella programme' strategically underpinning EU security dialogues and covering key security themes to position the EU as a smart security enabler. The new phase of the ESIWA+ programme, for which the EU contributes EUR 6 million during 2024-2027, will support cooperation with partners in Asia

and the Indo-Pacific in a number of areas, including hybrid threats, cybersecurity and foreign information manipulation and interference and disinformation.

The first EU-**Australia** Hybrid Threats Capabilities Exchange Programme workshop took place in Brussels on 19-20 March 2024, attended by representatives from the EU institutions, the Australian government, the Hybrid CoE and the Australian Strategic Policy Institute (ASPI). The purpose of this workshop was to support a collective understanding of hybrid threats and the strategies and policies developed in response to them.

EU-NATO cooperation

EU and NATO staff-to-staff interactions on countering hybrid threats and enhancing resilience have been frequent and regular, and cross-briefings to respective committees and working groups continued. In December 2023, the two staffs shared the latest developments on the respective policy initiatives and exchanged views on future work. The Structured Dialogue on Resilience continued to ensure coherence and coordination of efforts between relevant work strands, including by implementing the recommendations of the EU-NATO Task Force on the resilience of critical infrastructure. In particular, progress has been made in the areas of civil-military cooperation, security research, critical undersea infrastructure, engagement with the private sector, and exercises. In February 2024, the Head of NATO's Cyber and Hybrid Policy Section briefed the Politico-Military Group (PMG) and the Horizontal Working Party on Enhancing Resilience and Countering Hybrid Threats on NATO`s responses to hybrid threats, particularly regarding those stemming from Russia and China. Based on reciprocity, in the same month, the EEAS Hybrid Threats and Cyber Division provided an update to Operations Policy Committee (Hybrid) on the EU Hybrid Toolbox and other relevant mechanisms in countering hybrid threats.

EU and NATO staffs continued to engage in and promote **activities organised and facilitated by the Hybrid CoE in Helsinki**. In October 2023, the Hybrid CoE facilitated the 4th EU-NATO High-Level Retreat, where senior officials exchanged views on China as a hybrid threat actor and the implications of China's evolving hybrid threat activities for the security of the Euro-Atlantic region. In April 2024, Hybrid CoE facilitated a foresight seminar on resilience of critical infrastructure for the EU and NATO policy planners. On 24 October 2023, EU and NATO representatives addressed a NATO Defence College Senior Course by delivering a joint lecture on collective resilience. On 29 May 2024, NATO representatives spoke in a conference on hybrid and technological threats to democracy co-organised by the Belgian Presidency, Defend Democracy and the EEAS.

The Technical Arrangement concerning cooperation on Cyber Defence between NATO Cyber Security Centre (NCSC) and CERT-EU continued to be implemented in line with existing provisions. Exchanges on best practices and coordination continued in the context of regular meetings at working level, a coordination meeting of the heads of the two organisations as well as targeted thematic workshops on technical issues of mutual interest. In addition, CERT-EU and NATO continued to exchange technical information on relevant cyber threats.

CSDP operations and missions

Since the deployment of the **EU Partnership Mission to the Republic of Moldova** in May 2023, the mission has provided advice on strengthening Moldova's crisis management structures and on enhancing resilience to hybrid threats, including cybersecurity, and countering FIMI. During the first year of operation, the mission has, for instance, supported the operationalisation of the Centre for Strategic Communication and Countering Disinformation and the Agency for Cyber Security, provided advice on the drafting of the National Security

Strategy, and worked with the Ministry of the Interior on the development of a comprehensive crisis management system. In addition, the mission's project cell has implemented projects within the mandate of the mission and in close cooperation with like-minded partners.

CONCLUSION

The reporting period for this progress report was marked by Russia's continued aggression against Ukraine and the new conflict between Hamas and Israel. Both of these wars have several direct and indirect cross-border effects, and they are linked to state and non-state use of hybrid means, such as FIMI, cyberattacks, damaging of critical infrastructure, instrumentalizing migration flows, with the aim of targeting the EU, its Member States and partners.

In view of the elections in Europe, efforts were undertaken during the reporting period to strengthen democratic and electoral resilience. Assessing the effectiveness of the measures implemented and evaluating the lessons-learned from the election year will take place in the next reporting period. Specific measures addressing foreign interference in elections will also be reflected in the post-election report that will be issued by the Commission, at the latest within one year after the 2024 elections to the European Parliament.

In 2023 and 2024, first cases of hybrid threats were addressed in the framework of the EU Hybrid Toolbox with the support of the Commission services and the EEAS. The toolbox offers a framework for coordinated and common responses to hybrid threats and campaigns. In May 2024, Member States made significant progress towards establishing EU Hybrid Rapid Response Teams, by validating the Guiding framework[72].

The reporting period was also marked by more extensive exchanges with NATO. New structured dialogues on space, climate and security, and emerging and disruptive technologies were launched, all being relevant for countering hybrid threats. EU's support to partners was enhanced by the activities of the EU Partnership Mission to Moldova, which is an important test case for using CSDP for countering hybrid threats.

Building on clear advances in many areas, and the prospects of the increased use of the EU Hybrid Toolbox, the work on developing EU policies on countering hybrid threats needs to continue. In a time of "permanent crisis", where crises have increasingly complex cross-border impacts, it is important to step up work to strengthen EU's policies and preparedness for all types of hazards, from man-made hybrid attacks to natural disasters.

[72] Council document 10125/24.